УДК 004.056

Ю.П. ГУЛЬЧАК
Вінницький національний медичний університет ім. М.І. Пирогова
Е.Ю. ГУЛЬЧАК
ТОВ «Промавтоматика Вінниця»

НОРМАТИВНО-ПРАВОВА БАЗА ЗАХИСТУ ІНФОРМАЦІЇ В МЕДИЧНІЙ ГАЛУЗІ

Представлено систематизований огляд сучасної нормативно-правової бази України, яка регламентує функціонування автоматизованих систем з врахуванням особливостей медичної галузі. Проведений ґрунтовний аналіз існуючої законодавчої бази при практичному впровадженні комплексної системи захисту інформації в медичних інформаційних системах (МІС). Виділені особливості медичних закладів різних рівнів і подані рекомендації по впровадженню в них відповідних профілів безпеки. Розроблено концепцію правового регулювання розробки і практичного впровадження системи захисту інформаційних ресурсів МІС. Розглянуті нормативні документи визначають методологічні основи вирішення завдань захисту інформації в комп'ютеризованих медичних системах і створення прикладних нормативних і методологічних документів, які регламентують питання захисту МІС від несанкціонованого доступу; створення захищених інформаційних систем і засобів їх захисту; дозволяють оцінити рівень захищеності таких систем і їх придатність для вирішення завдань захисту інформаційних ресурсів медичного закладу і персональних даних пацієнтів. Надані рекомендації щодо необхідних рівнів послуг безпеки, які реалізують заданий функціональний профіль захищеності. Опираючись на нормативні документи визначені допустимі рівні безпеки медичних інформаційних систем, які гарантують достатній рівень захисту інформації. Детально проаналізовані рівні безпеки для загроз конфіденційності та цілісності персональних даних та подані рекомендації підсилення захисту починаючи від закладів первинного рівня до багатопрофільних медичних центрів і об'єднань. Виділені основні пункти нормативно-правових актів, важливі для розробки і впровадження політики безпеки типового медичного закладу. Обґрунтовано об'єднання базових моделей розмежування доступу для забезпечення як адміністративних, так і довірчих послуг безпеки.

Ключові слова: медична інформаційна система, захист персональних даних, профіль безпеки, конфіденційність, цілісність, доступність.

IU. P. GULCHAK
Vinnytsya National Pirogov Memorial Medical University
E. IU. HULCHAK
Company "Promautomatika Vinnitsa", Vinnytsia, Ukraine

REGULATORY-LEGAL BASIS FOR INFORMATION PROTECTION IN THE MEDICAL SECTOR

The systematic review of the modern legal and regulatory framework of Ukraine, which regulates the functioning of automated systems taking into account the peculiarities of the medical sector, is presented. A thorough analysis of the existing legislative framework was carried out at the practical introduction of a comprehensive information security system in medical information systems (MIS). The peculiarities of medical institutions of different levels are highlighted and recommendations for the implementation of their respective security profiles are given. The concept of legal regulation of development and practical implementation of the system of protection of information resources of the MIS has been developed. The reviewed normative documents determine the methodological basis for solving the problems of information security in computerized medical systems and the creation of applied normative and methodological documents regulating the protection of the MIS from unauthorized access; creation of secure information systems and means of their protection; allow to estimate the level of protection of such systems and their suitability for solving the problems of protecting the information resources of the medical institution and personal data of patients. The recommendations for the required levels of security services that implement a given functional security profile are given. Based on normative documents, acceptable levels of safety of medical information systems are determined which guarantee an adequate level of information security. The security levels are carefully analyzed for threats to the confidentiality and integrity of personal data, and recommendations for strengthening protection from the primary level institutions to the multidisciplinary medical centers and associations are presented. The main points of normative legal acts are important, which are important for the development and implementation of the security policy of a typical medical institution. The reason for combining the basic models of differentiation of access is to provide both administrative and trust security services.

Keywords: medical information system, personal data protection, security profile, confidentiality, integrity.

Вступ. Інформатизація медицини передбачає цілий комплекс складних для вирішення проблем. Серед них особливе місце займає комп'ютерна безпека. Інформація – стратегічний товар, за допомогою якого зловмисник може досягти своїх корисливих цілей. Нанести людині непоправну шкоду, зруйнувати бізнес, кар'єру, особисте життя. Інформація про здоров'я людини прекрасний інструмент для психологічного впливу, маніпулювання, шантажу. Тому збереження лікарської таємниці є надзвичайно важливим, а для деяких категорій людей життєво необхідним і вони готові вкладати серйозні кошти для її збереження на високому рівні. Крім того і держава зобов'язана зберігати конфіденційність персональних даних пацієнтів.

Мета дослідження. На жаль, в Україні на державному рівні приділяється недостатньо уваги законодавству з інформатизації медицини і інформаційної безпеки зокрема. Існуючі законодавчі акти в галузі захисту інформації не враховують специфіку і особливості медичних інформаційних систем (МІС), а тому потребують конкретизації і додаткових пояснень. В роботі проаналізовані ключові закони та підзаконні актив галузі інформатизації, якими потрібно керуватись при практичному впровадженні систем комп'ютерної безпеки в медичних закладах різного рівня. Надані рекомендації щодо вибору оптимальних рівнів захищеності (профілів безпеки) медичної інформації в закладах первинного, вторинного та

третинного рівнів.

Основна частина. Сформулюємо основні вимоги до захисту інформаційних ресурсів при практичному впровадженні систем комп'ютерної безпеки в МІС закладів охорони здоров'я різних рівнів надання медичної допомоги.

Одним з перших законів, який був прийнятий в незалежній Україні є закон України «Про інформацію» [1]. Даний документ чітко визначає поняття захисту інформації: «Захист інформації – це комплекс правових, організаційних, інформаційно–телекомунікаційних засобів і заходів, спрямованих на запобігання неправомірним діянням щодо інформації». Звідси випливає, що будь-які заходи по захисту інформації в МІС повинні носити комплексний характер і включати три складові: правову, організаційну (політика інформаційної безпеки) та технічну (інженерні та програмно-апаратні засоби захисту).

Правові аспекти захисту інформації (ЗІ) призвані забезпечити виконання норм і положень державної політики України в галузі інформаційної безпеки, здійснювати контроль за захищеністю інформації, що є власністю державних і недержавних організацій і, зокрема, за захист персональних даних (ПД) громадян (пацієнтів). Приватні медичні заклади зобов'язані згідно нормативно-правового законодавства виконувати вимоги щодо нерозголошення конфіденційної інформації нарівні з державними і нести однакову відповідальність за порушення цих вимог.

Згідно статті 18 [1] до основних даних про особу, які підлягають захисту, відноситься інформація про її здоров'я. Всяка інформація про стан здоров'я людини є конфіденційною з відповідними вимогами до її використання. «Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежений фізичною або юридичною особою, крім суб'єктів владних повноважень»[1, ст.21].

Захист інформації на державному рівні є однією з умов функціонування державних інституцій. Тому важливим з точки зору інформаційної безпеки є Закон України «Про захист інформації в інформаційних телекомунікаційних системах» [2], прийнятий у 1994 році. Виділимо основні його положення стосовно захисту інформаційних ресурсів МІС:

– державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системах з застосуванням комплексної системи захисту інформації (КСЗІ) з підтвердженою відповідністю [2, ст.8];

– несертифіковані відповідним чином системи чи їх окремі елементи не можуть використовуватися в автоматизованих системах обробки конфіденційної інформації і медичної зокрема;

– засоби захисту інформації, які використовуються для створення КСЗІ, також повинні бути обов'язково сертифіковані;

– відповідальність за забезпечення захисту інформації в системі покладається на власника системи [2, ст.9]. Тобто лікарняний заклад несе повну відповідальність за забезпечення конфіденційності ввіреної йому інформації. Коли захист інформації делегований сторонній організації наступає колективна відповідальність обох суб'єктів.

Особливе місце серед нормативно-правових актів, що мають відношення до збереження лікарської таємниці, захисту персональних даних пацієнта та інформації про стан його здоров'я посідає Закон України «Про захист персональних даних» [3], прийнятий у 2010 році. Основні положення закону, важливі для розробки, впровадження та функціонування МІС.

1.Термін персональні дані [3, п.2] визначає, що персональними даними є відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Для медицини важливо вказати перелік відомостей про пацієнта, які є персональними даними і які потрібно захищати в тому чи іншому випадку.

2. Під терміном база персональних даних [3, п.2] мається на увазі поіменована сукупність упорядкованих персональних даних електронній формі та/або картотек персональних даних. Для медичного закладу характерним є формування і супроводження трьох взаємопов'язаних, але відносно самостійних баз даних (БД)–БД медичного закладу, БД пацієнтів, БД сторонніх організацій-партнерів, захист інформації в яких повинен реалізовуватись за різними принципами.

3. Володілець персональних даних – фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначене законом. Зазвичай в якості володільця ПД виступає заклад охорони здоров'я або фізична особа – підприємець.

4. Розпорядник персональних даних – фізична чи юридична особа, якій володільцем бази ПД або законом надано право обробляти ці дані [3, ст.2]. Між володільцем і розпорядником ПД є суттєва різниця. Володільцю ПД право на обробку ПД надано або законом або самим суб'єктом ПД; розпоряднику ж таке право надається володільцем ПД або законом. Володілець ПД затверджує мету обробки персональних даних, встановлює їх склад і процедури обробки. Розпорядник обробляє персональні дані в інтересах володільця ПД у складі і з метою, визначеною володільцем.

Всі лікувально-профілактичні заклади незалежно від відомчого підпорядкування і форм власності, а також приватно практикуючі медичні працівники є власниками бази ПД. Розпорядником ПД в медичному закладі є працівник, на якого покладені обов'язки по обробці ПД, їх формування в бази, оновлення внесених даних тощо. Це може бути працівник відділу кадрів (БД працівників), працівник реєстратури при зверненні пацієнта до лікарні, медичний персонал відділень і кабінетів (БД пацієнтів), приватно практикуючий лікар.

5. Забороняється обробка ПД «… що стосуються здоров'я, статевого життя, біометричних або генетичних даних [3, ст.7,п.1] крім випадків, коли вона (обробка) необхідна в цілях охорони здоров'я, встановлення медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг, функціонування електронної системи охорони здоров'я за умови, що такі дані обробляються медичним працівником або іншою особою закладу охорони здоров'я чи фізичною особою-підприємцем, яка одержала ліцензію на провадження господарської діяльності з медичної практики, та її працівниками, на яких покладено обов'язки щодо забезпечення захисту персональних даних та на яких поширюється дія законодавства про лікарську таємницю, працівниками центрального органу виконавчої влади, що реалізує державну політику у сфері державних фінансових гарантій медичного обслуговування населення, на яких покладено обов'язки щодо забезпечення захисту персональних даних» [3, ст.7,п.6]. Тобто технічний працівник з комп'ютерної безпеки не повинен мати доступу до обробки ПД у ввіреній йому базі ПД.

6. Використання персональних даних працівниками суб'єктів відносин, пов'язаних з персональними даними, повинно здійснюватися лише відповідно до їхніх професійних чи службових або трудових обов'язків. Ці працівники зобов'язані не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, крім випадків, передбачених законом. Використання персональних даних володільцем здійснюється у разі створення ним умов для захисту цих даних [3, ст.10, п.1-2].Підставами для обробки персональних даних є захист життєво важливих інтересів суб'єкта персональних даних[3, ст.11, п.4].

Закон регулює принципи збору, накопичення, зберігання, поширення, видалення або знищення ПД [3, ст.12-15], але не конкретизує правила внесення змін і доповнень до ПД. Вказано лише, що «володільці чи розпорядники персональних даних зобов'язані вносити зміни до персональних даних на підставі вмотивованої письмової вимоги суб'єкта персональних даних»[3, ст.20, п.1]. Але не зрозуміло, як повинен вчинити лікар, коли пацієнт подає відомості про захворювання із стороннього закладу (наприклад приватної клініки). В багатьох випадках неприйнятною для медичної галузі є стаття закону, яка передбачає повідомлення суб'єкта ПД про передачу даних третій особі, їх зміну або знищення протягом деякого часу [3, ст.21].

Контроль за додержанням законодавства про захист персональних даних у межах повноважень, передбачених законом, здійснюють уповноважений і суди.

З моменту прийняття закону пройшло сім років, але до цих пір не розроблено положення про обробку та захист ПД в сфері медицини, яке було заплановано ще в 2014 році [4].

При роботі з електронними медичними документами, медичними картками пацієнтів необхідно керуватись положеннями типового порядку обробки персональних даних [5], окремий розділ якого присвячений захисту ПД. Захист персональних даних передбачає заходи, спрямовані на запобігання їх випадкових втрати або знищення, незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

Забезпечення захисту персональних даних на всіх етапах їх обробки покладається на володільця, розпорядника персональних даних, який має використовувати для цього всі наявні можливості, включаючи організаційно-правові та технічні заходи.

Організаційні заходи охоплюють:

- визначення порядку доступу до персональних даних працівників володільця/розпорядника;
- визначення порядку ведення обліку операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них;
- розробку плану дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій;
- регулярне навчання співробітників, які працюють з персональними даними.

Правові заходи повинні враховувати вимоги законодавства в сфері захисту ПД, чинні на даний момент.

З метою забезпечення безпеки обробки персональних даних вживаються спеціальні технічні заходи захисту, у тому числі щодо виключення несанкціонованого доступу до персональних даних, що обробляються та роботі технічного та програмного комплексу, за допомогою якого здійснюється обробка персональних даних [5]. Технічні заходи передбачають експлуатацію виключно сертифікованого обладнання і повинні забезпечувати необхідний рівень безпеки для даного класу МІС.

Важливим керівним документом з інформатизації міг стати закон «Про основні засади розвитку інформаційного суспільства в Україні» [6], але його основні пункти так і залишились декларативними.

В документі намічені стратегічні цілі в сфері інформатизації українського суспільства, вказано, що «залучення ІКТ для … збереження і зміцнення здоров'я населення, підвищення якості та ефективності медико-санітарної допомоги, забезпечення соціальної справедливості та прав громадян на охорону здоров'я є одним з пріоритетних завдань для України».

Проаналізувавши частину, яка стосується інформатизації медицини, маємо визнати, щодо теперішнього часу не забезпечена на належному рівні підготовка медичних працівників для роботи з інформаційно-комп'ютерною технікою (ІКТ). Не задовольняє потреб сьогодення організаційний і технологічний рівень розвитку ІКТ в охороні здоров'я. Слід виділити негативні наслідки, до яких призвела невірна інформаційна політика МОЗ по формуванню і впровадженню в практику загальнодержавних

програм охорони здоров'я. Звідси і зростання рівня захворюваності населення, і епідемії, які останнім часом поширюються в Україні; хоча документ передбачав «забезпечення доступу до світових медичних знань та актуальних на місцевому рівні інформаційних ресурсів з метою підвищення ефективного виконання державних дослідницьких і профілактичних програм з охорони здоров'я».

Окремо виділені завдання в сфері інформаційної безпеки. Актуальними залишаються питання вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері.

На даний час в Україні схвалена «Стратегія розвитку інформаційного суспільства в Україні» до 2020 року [7]. Поставлено завдання інтегрувати досягнення розвитку інформаційного суспільства в загальносвітові. Передбачається розробка та впровадження загальнодержавної програми «Здоров'я-2020: український вибір», яка корелюється з програмою Європейського Союзу «Європейська стратегія здоров'я 2020».

Документ вводить поняття **е-медицини** (електронна медицина), тобто використання інформаційних технологій «… у сфері охорони здоров'я та забезпечення оперативного доступу медичних працівників та пацієнтів до них». Е-медицина повинна забезпечувати взаємодію між пацієнтами, медичними працівниками та установами за допомогою інформаційно-комунікаційних технологій.

Основними напрямами діяльності в галузі розвитку е-медицини є:

- впровадження автоматизованих інформаційних галузевих систем, які, зокрема, дають змогу перейти до ведення медичної документації в електронному вигляді;
- розвиток телемедицини;
- удосконалення розвитку системи моніторингу стану здоров'я населення;
- створення та впровадження нових комп'ютерних технологій профілактики захворювань, діагностики, забезпечення лікувальних процесів;
- створення загальнодоступних електронних медичних ресурсів.

Окремий розділ присвячено питанням захисту інформації. Виділимо основні пріоритети діяльності за напрямком «Інформаційна безпека»[7]:

- сприяння виробництву конкурентоспроможного національного інформаційного продукту;
- сприяння вітчизняному виробництву засобів захисту інформації, створенню захищених інформаційно-телекомунікаційних систем, запровадження сучасних захищених інформаційних технологій в інтересах державного управління;
- створення ефективної системи виявлення та запобігання загрозам державних електронних інформаційних ресурсів, у тому числі щодо протидії розповсюдженню комп'ютерних вірусів, програмних і апаратних закладок, а також витоку інформації технічними каналами та за рахунок несанкціонованих дій;
- забезпечення цілісності, доступності та конфіденційності інформаційних ресурсів України, які створюють умови для розвитку особи, стійкого функціонування суспільства і держави, захисту персональних даних та інформації, що перебуває у володінні фізичних, юридичних осіб та держави, від зовнішніх і внутрішніх інформаційних загроз, зокрема шляхом протидії комп'ютерним злочинам;
- удосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема кібернетичної безпеки національної критичної інфраструктури;
- впровадження захищеного механізму ідентифікації учасників електронної взаємодії;
- формування системи моніторингу безпеки інформаційних ресурсів та систем.

Крім декларативних документів державного рівня для впровадження і експлуатації МІС важливими є норми спеціалізованих документів, які спрямовані на захист інформаційних ресурсів лікувального закладу і регулюють функціонування підсистеми інформаційної безпеки.

Розглянемо базові нормативні документи, які важливі для медицини взагалі і МІС зокрема.

Типова інструкція [8] визначає порядок роботи з матеріалами для службового користування. Згідно документа в організації повинна бути створена постійно діюча комісія з питань роботи з службовою інформацією, положення про яку та її склад затверджується відповідним актом установи. Сформульовані основні завдання такої комісії. Для медичних установ це перш за все складання переліку відомостей, що становлять службову інформацію; перегляд документів з грифом "Для службового користування" з метою його підтвердження або скасування, а також на предмет встановлення в них відомостей, що містять відкриту інформацію, яка може бути використана під час опрацювання запитів на публічну інформацію [8, п.3].

Згідно п.11 забороняється використовувати для передачі службової інформації відкриті канали зв'язку. Якщо ж виникає необхідність передавати таку інформацію, то особи, які її отримують, повинні надати письмове зобов'язання щодо її нерозголошення.

Відповідальність за організацію та забезпечення дотримання в установах порядку ведення обліку, зберігання та використання документів, що містять службову інформацію, покладається на їх керівників

[8, п.6]. Окремі вимоги для працівників організацій, які мають доступ до службових матеріалів. Вони повинні бути ознайомлені з відповідними відомчими інструкціями із захисту інформації під розпис.

Співробітникам (виконавцям), допущеним до роботи з документами з грифом "Для службового користування", забороняється повідомляти усно або письмово будь-кому відомості, що містяться у цих документах, якщо це не викликано службовою потребою [8, п.8]. Для документів з грифом "Для службового

користування" встановлюються правила перегляду, користування, пересилки, формування у справи, передавання в архів та знищення.

Головний лікар, завідувач центру первинної медико-санітарної допомоги (ЦПМСД) зацікавлені у створенні і впровадженні ефективної системи захисту інформаційних ресурсів МІС. А для цього дуже потрібна типова інструкція з розробки і впровадження політики безпеки медичних закладів різного рівня, або хоч би її окремі елементи. Такі документи вже тривалий період використовуються в різних країнах (наприклад типова модель загроз і типова модель порушника для типової МІС лікувально-профілактичного закладу в Росії 2009 р.). Ефективною система захисту інформації в МІС буде лише при умові, що керівництво медичного закладу матиме достатню нормативно-правову і, зрозуміло, технічну базу для реалізації ефективної політики безпеки.

Постановою КМ України затверджені правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [9]. Документ визначає поняття ідентифікації та автентифікації користувачів, вказує, яка інформація підлягає захисту в системі. В інформаційній системі обов'язково реєструються

- результати ідентифікації та автентифікації користувачів;
- результати виконання користувачем операцій з обробки інформації;
- спроби несанкціонованих дій з інформацією;
- факти надання та позбавлення користувачів права доступу до інформації та її обробки;
- результати перевірки цілісності засобів захисту інформації.

Реєстрація здійснюється автоматичним способом, а реєстраційні дані захищаються від модифікації та знищення користувачами, які не мають повноважень адміністратора безпеки.

Доступ до службової інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися[9, п.6].

Окремим розділом в постанові виділені організаційні засади захисту інформації. Перш за все підтверджено, що ефективний захист може забезпечити лише комплексна система захисту інформації. Для МІС КСЗІ направлена на захист від витоку інформації технічними каналами, які « … утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій, несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів».

Відповідальність за забезпечення захисту інформації в системі, своєчасне розроблення необхідних для цього заходів та створення системи захисту покладається на керівника (заступника керівника) організації, яка є власником (розпорядником) системи, та керівників її структурних підрозділів, що забезпечують створення та експлуатацію системи [9, п.17].

В медичних закладах обслуговування МІС зазвичай виконує одна, рідше кілька осіб, тому логічно, враховуючи, що обсяг робіт, пов'язаних із захистом інформації, не є значним, доручити такі роботи окремій особі (адміністратор системи або інженер).

В будь-якому закладі обов'язково складається план захисту інформації в МІС, який містить [9, п.19]:

- завдання захисту, класифікацію інформації, яка обробляється в системі, опис технології обробки інформації;
- визначення моделі загроз для інформації в системі;
- основні вимоги щодо захисту інформації та правила доступу до неї в системі;
- перелік документів, згідно з якими здійснюється захист інформації в системі;
- перелік і строки виконання робіт службою захисту інформації.

Важливо підкреслити, що система захисту інформації в МІС повинна використовувати лише сертифіковані засоби захисту.

Будь-яка інформаційна система повинна мати чітко визначені границі об'єктів, на яких відбувається обробка інформації. Такі об'єкти підлягають обов'язковому категоріюванню згідно з Положенням [10]. Документ подає визначення понять категоріювання, категорія об'єкта, об'єкт інформаційної діяльності, інформація з обмеженим доступом тощо.

Відмітимо найважливіші пункти документа стосовно МІС:

1. Категоріювання здійснюється для визначення необхідного (зі встановлених нормативно-правовими актами та нормативними документами системи технічного захисту інформації рівнів) рівня захисту інформації, що обробляється технічними засобами та/або озвучується на об'єкті.

2. Об'єктами категоріювання є об'єкти інформаційної діяльності, в тому числі об'єкти ЕОТ.

3. Категоріювання здійснюється за ознакою: ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на ОІД.

Документ установлює чотири категорії об'єктів залежно від правового режиму доступу до інформації, що циркулює в них:

«… - до третьої категорії відносяться об'єкти, в яких циркулює інформація, що містить відомості, які становлять державну таємницю, для якої встановлено гриф секретності "таємно", а також інформація, що

містить відомості, які становлять іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству й державі;

- до четвертої категорії відносяться об'єкти, в яких циркулює службова та конфіденційна інформація, вимога щодо захисту якої встановлена законом»

4. Об’єктам, на яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, встановлюється четверта (IV) категорія.

5. За рішенням розпорядників (користувачів) інформації або за рішенням власників (розпорядників, користувачів) об’єктів, на яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці, об’єктам може встановлюватися ІІІ категорія.

Для медичних закладів первинного рівня характерна різнорідність об’єкт-користувачів, об’єкт-процесів та суб’єктів інформаційної взаємодії. Тому тут однозначно третя категорія. Для закладів вторинного рівня ситуація не є однозначною. Якщо це міська лікарня, багатопрофільне територіальне об’єднання, то важливим фактором виступає різнорідність як об’єкт-процесів, так і об’єкт-користувачів. І тут встановлювати категорію потрібно рішенням розпорядників інформації за згодою власників об’єктів. Інформаційним системам медичних закладів третинного рівня може бути встановлена ІІІ категорія (наприклад для закладів психоневрологічного профілю) або IV категорія з виділенням окремих об’єктів, віднесених до ІІІ категорії.

Крім категоріювання об’єктів інформаційної діяльності законодавчо закріплені і класи автоматизованих систем за рівнем захищеності від несанкціонованого доступу [11]. Виділено три класи з окремими вимогами до функціонального складу комп’ютерних засобів захисту.

Клас «1» — одномашинний однокористувацький комплекс, який обробляє інформацію однієї або кількох ступенів обмеження доступу.

«… в кожний момент часу з комплексом може працювати тільки один користувач, хоч у загальному випадку осіб, що мають доступ до комплексу, може бути декілька;користувачі можуть мати різні повноваження (права) щодо доступу до інформації, яка обробляється».

Клас «2» — локалізований багатомашинний багатокористувацький комплекс, який обробляє інформацію різних ступенів обмеження доступу.

Відміна від попереднього класу — наявність користувачів з різними повноваженнями по доступу і/або технічних засобів, які можуть одночасно здійснювати обробку інформації різних ступенів обмеження доступу.

Клас «3» — розподілений багатомашинний багатокористувацький комплекс, який обробляє інформацію різних ступенів обмеження доступу.

Істотна відміна від попереднього класу — необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки.»

Для більшості МІС характерні автоматизовані системи класів 1 та 2.

Кожен з класів характеризується окремим набором елементів захисту, так званих профілів безпеки[11] . Загальна структура класифікації має вигляд X.YYY.Z (наприклад 2.КЦД.3), де X – функціональний клас АС, Y – підклас АС, Z – функціональний профіль АС

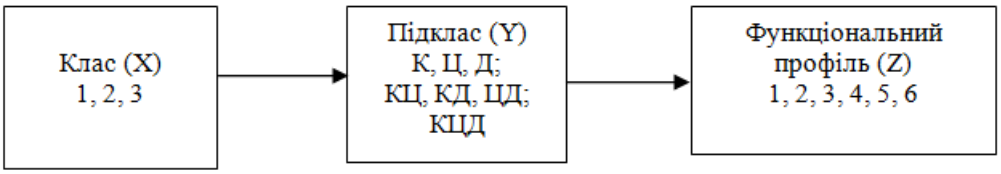

Рис. 1. Класи АС і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (К – конфіденційність, Ц – цілісність, Д – доступність)

Розглянемо більш докладно, що ж регламентує документ з точки зору забезпечення базових складових інформаційної безпеки: конфіденційності, цілісності, доступності та спостережності. Згідно з [12] під цими поняттями розуміють:

– конфіденційність інформації — властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом;

– цілісність інформації — властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом. Цілісність системи — властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки;

– доступність — властивість ресурсу системи (КС, послуги, об’єкта КС, інформації), яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний;

– спостережність — властивість КС, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії.

Врахуємо, що інформаційні ресурси лікарняного закладу є як продуктом роботи персоналу, так і готовими об'єктами МІС, з якими працюють і до яких періодично повинні мати доступ окремі категорії спеціалістів. Тому обрані стандартні функціональні профілі захищеності оброблюваної інформації повинні забезпечити недопущення несанкціонованого доступу до інформаційних ресурсів закладу, захист інформації від знищення, спотворення, копіювання, блокування тощо; захист апаратних і програмних компонентів МІС.

Для рівня первинної медичної допомоги [13] основними загрозами є порушення конфіденційності інформації і, як результат, порушення її цілісності. Тому на початковому етапі достатньо запровадити прості профілі захисту АС класу 1; від 1.К.Х до 2.КЦ.Х для амбулаторій і 2.КЦ.Х центрів первинної медико-санітарної допомоги. Будь-який профіль включає набір заходів спостережності. В подальшому завжди можливе підсилення окремих функціональних профілів і навіть заміна підкласу (наприклад КЦ.Х на КЦД.Х).

Для закладів вторинного рівня (спеціалізована допомога) [14], реформування яких почнеться у 2019 році, перш за все необхідно провести інвентаризацію і аналіз всіх комп'ютерних засобів, які використовуються на даний період, визначити їх можливості з точки зору впровадження відповідаючої сучасним вимогам комплексної системи захисту інформації. Якщо в медичному закладі вже функціонує МІС на основі локальної мережі, то необхідно переглянути наявну політику інформаційної безпеки і привести її у відповідність з існуючим нормативно-правовим законодавством згідно засад впровадження медичної реформи в Україні.

Виходячи з вищесказаного і враховуючи, що абсолютна більшість МІС закладів ІІ рівня відноситься до класу 2, можна рекомендувати рівні захищеності АС 2КЦ.Х (профілі з підвищеними вимогами до забезпечення конфіденційності і цілісності оброблюваної інформації). Щодо реалізації профілів захищеності тут потрібно керуватись можливостями технічної реалізації тих чи інших елементів захисту. Для прикладу найпростіший, доцільний для практичної реалізації профіль захищеності 2.КЦ.2 має вигляд:

2.КЦ.2 = { КД-2, КО-1, - забезпечення довірчої конфіденційності даних

ЦД-1, ЦО-1, - забезпечення довірчої цілісності даних

НР-2, НИ-2, НК-1, НО-1, НЦ-2, НТ-1 – профілі спостережності даних}.

Для закладів третинного рівня (високоспеціалізована допомога), реформа яких має початись у 2020 році [14], в загальному випадку можна використовувати ті ж рівні захищеності, що і для вторинної ланки, підсиливши їх окремі складові. Наприклад при переході від функціонального профілю 2.КЦ.2 до 2.КЦ.3 додатково реалізуються адміністративна конфіденційність даних КА-2 та адміністративна цілісність даних ЦА-2; у профілі спостережності змінюють елементи НО-1 та НТ-1 відповідно на НО-2 та НТ-2.

Заклади спеціалізованої медичної допомоги з точки зору інформаційної безпеки є найбільш вразливими, так як саме у цій ланці знаходяться найбільш інформаційно ємні бази персональних даних різнорідних категорій пацієнтів. Саме на цьому рівні зосереджена основна маса інформації, в якій зацікавлені потенційні порушники. Виходячи з цього доцільно в першу чергу забезпечити надійний захист баз персональних даних (зокрема історій хвороб) пацієнтів за напрямками конфіденційності та цілісності; захист баз даних службової медичної інформації, кадрової і бухгалтерської документації – за напрямком доступності. Крім того значно підвищуються вимоги до захисту інформації в телекомунікаційних мережах зв'язку при передачі великих масивів даних, так як телемедицина стає важливим елементом функціонування лікарні [15].

Більшість МІС відносяться до АС класу 2. Розглянемо основні вимоги до таких систем опираючись на нормативний документ [16]. Мета цього документа – надання нормативно-методологічної бази під час розроблення комплексів засобів захисту від несанкціонованого доступу (НСД) до службової інформації, яка обробляється в АС класу 2, створення КСЗІ в установі (організації), проведення аналізу та оцінки захищеності інформації від НСД в системах такого класу, а також рекомендацій для визначення необхідного функціонального профілю захищеності інформації в конкретній АС. Документ конкретизує вимоги до окремих складових АС класу 2 – обчислювальної системи, фізичного середовища, в якому функціонує АС, користувачів АС, оброблюваної службової інформації та технології її оброблення.

Забезпечення захисту службової інформації передбачає комплекс засобів і заходів, які потрібно виконати. Наведемо основні з них з огляду на їх важливість:

– організація служби захисту інформації з відповідними повноваженнями;

– створення комплексної системи захисту інформації як сукупності організаційних, правових та інженерно-технічних заходів забезпечення захисту інформації;

– перелік службової інформації, яка підлягає автоматизованій обробці;

– визначення ієрархічних рівнів повноважень користувачів та класифікаційних рівнів інформації;

– обов'язковість реєстрації в АС всіх користувачів та їхніх дій щодо службової інформації.

– заборона несанкціонованого розповсюдження, копіювання, розмноження, модифікації службової інформації в електронному вигляді та контроль СЗІ за такими діями.

– можливість однозначної ідентифікації та автентифікації кожного зареєстрованого користувача;

Перелік мінімально необхідних рівнів послуг безпеки, які реалізуються КЗЗ (функціональний профіль захищеності), вибирається залежно від технологій обробки інформації, що застосовуються, та з урахуванням типових умов функціонування АС. Для АС класу 2 визначаються такі стандартні функціональні профілі захищеності оброблюваної інформації:

- під час застосування технології, що вимагає підвищених вимог до забезпечення конфіденційності оброблюваної інформації:

2.К.3 = {КД-2, КА-2, КО-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-2, НО-2};

- під час застосування технології, що вимагає підвищених вимог до забезпечення конфіденційності та цілісності оброблюваної інформації:

2.КЦ.3 = {КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-2, НО-2};

- під час застосування технології, що вимагає підвищених вимог до забезпечення конфіденційності та доступності оброблюваної інформації:

2.КД.1а = {КД-2, КА-2, КО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-2, НО-2};

- під час застосування технології, що вимагає підвищених вимог до забезпечення конфіденційності, цілісності та доступності оброблюваної інформації:

2.КЦД.2а = {КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НК-1, НЦ-2, НТ-2, НИ-2, НО-2}.

Підсумовуючи все вище сказане для закладів охорони здоров'я можуть бути реалізовані такі базові функціональні профілі безпеки:

Для сільських амбулаторій, лікарів приватної практики, інших установ, які можна віднести до АС класу 1 мінімально достатнім слід вважати стандартний профіль 1.КЦ.Х. Нормативний документ [11] не рекомендує вибирати профіль, опираючись лише на один напрямок захисту (конфіденційність або цілісність), так як в цьому випадку практично нереально організувати дієву систему захисту інформації. Функціональний профіль 1.КЦ.2 реалізує адміністративний принцип розмежування доступу, що забезпечується послугами КА та ЦА.

1.КЦ.2 = {КА-1, КО-1; ЦА-2, ЦО-1,
НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1}

Для загроз конфіденційності рекомендується запровадити:

– мінімальний рівень КА-1. Адміністративна конфіденційність дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів;

– мінімальний рівень КО-1. Повторне використання об'єктів дозволяє забезпечити коректність повторного використання розділюваних об'єктів, тобто таких, які почергово виділяються різним користувачам та/або процесам, гарантує, що коли розділюваний об'єкт виділяється новому користувачу або процесу, він не містить інформації, яка залишилась від попереднього користувача або процесу.

Для загроз цілісності достатніми є:

– базовий рівень ЦА-2. Адміністративна цілісність дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів;

– обмежений рівень ЦО-1. Відкат забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкотити) захищений об'єкт до попереднього стану.

Профіль повинен включати базовий набір рівнів спостережності:

– базовий рівень НР-2 (реєстрація). Реєстрація дозволяє контролювати небезпечні для КС дії шляхом реєстрації і аналізу подій, що мають відношення до безпеки;

– базовий рівень НИ-2 (ідентифікація та автентифікація). Дозволяє КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС;

– мінімальний рівень НК-1. Гарантує користувачу можливість безпосередньої взаємодії з КЗЗ;

– мінімальний рівень НО-1. Розподіл обов'язків дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування;

– мінімальний рівень НЦ-1. Цілісність комплексу засобів захисту визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами;

– мінімальний рівень НТ-1. Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС.

Для закладів спеціалізованої медичної допомоги (АС класу 2) підсилюються окремі рівні захисту залежно від вирішуваних практичних задач від мінімального рівня (наприклад КД-1) послідовно до базового (КД-2), повного (КД-3). Для центрів первинної медико-санітарної допомоги і закладів вторинного рівня спробуємо сформувати профіль з параметрами, які б забезпечили прийнятний рівень захисту інформації.

2.КЦ.3 = { КД-2, КА-2, КО-1; ЦД-1, ЦА-2, ЦО-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2 }

Для загроз конфіденційності рекомендується реалізувати базовий рівень КД-2 довірча конфіденційність, яка дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Адміністративну конфіденційність підсилити до базового рівня КА-2.

Для загроз цілісності реалізувати мінімальний рівень ЦД-1 довірча цілісність, яка дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену.

Профіль підсилює мінімальний набір рівнів спостережності до базових НО-2, НЦ-2, НТ-2.

Представлені вище профілі є базовими і рекомендованими. В кожному конкретному випадку, виходячи зі специфіки лікувально-профілактичного закладу їх елементи можна змінювати, включаючи нові або змінюючи навіть підкласи захищеності оброблюваної інформації.

Основним принципом політики безпеки щодо інформаційних ресурсів медичного закладу має бути вибірковий доступ окремих об'єкт-користувачів та об'єкт-процесів до окремих суб'єктів інформаційної взаємодії. Тому в даному випадку недоцільно, а в багатьох випадках і неможливо реалізувати окремо адміністративну або довірчу модель розмежування доступу. Потрібно їх об'єднувати і забезпечувати як адміністративні послуги безпеки (КА, КЦ), так і довірчі (КД, ЦД). Для будь-якого профілю потрібно враховувати послуги спостережності (НР, НИ).

Висновки. На даний час проблема захисту інформації в медицині вимагає централізованого вирішення. Розглянуті нормативні документи визначають методологічні основи (концепцію) вирішення завдань захисту інформації в комп'ютеризованих медичних системах і створення прикладних нормативних і методологічних документів, які регламентують питання захисту МІС від несанкціонованого доступу; створення захищених інформаційних систем і засобів їх захисту; дозволяють оцінити рівень захищеності таких систем і їх придатність для вирішення завдань захисту інформаційних ресурсів медичного закладу і персональних даних пацієнтів зокрема.

Представлена нормативно-правова база, якою необхідно керуватись при проектуванні, створенні і впровадженні в практику комплексної системи захисту інформаційних ресурсів медичних інформаційних систем. В період інформатизації медичної галузі питання інформаційної безпеки повинні органічно вплітатись в канву медичної реформи; впроваджуватись на всіх рівнях функціонування автоматизованих систем обробки інформації починаючи від сільської амбулаторії і закінчуючи високотехнологічними спеціалізованими медичними об'єднаннями. Комп'ютеризація і захист інформаційних ресурсів медичної галузі неподільні. Це потрібно зрозуміти кожному керівнику медичного закладу. Подані вище нормативні документи повинні допомогти керівництву медичних закладів почати підготовку до впровадження заходів і засобів комп'ютерної безпеки, які б відповідали вимогам законодавства України і міжнародним стандартам.

Література

1. Про інформатизацію : закон України від 2 жовтня 1992 р. № 2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – ст. 650.

2. Про захист інформації в інформаційних телекомунікаційних системах : закон України від 31 травня 2005 р. № 2594-IV // Відомості Верховної Ради України. – 2005. – № 26. – ст. 347.

3. Про захист персональних даних : закон України від 1 червня 2010 р. № 2297-VI // Відомості Верховної Ради України. – 2010. – № 34. – ст. 481.

4. Захист персональних даних пацієнтів під особливою увагою Омбудсмена [Електронний ресурс]. – Режим доступу : www.med-info.net.ua/index.php?q=content – (дата звернення: 12.10.2017)

5. Типовий порядок обробки персональних даних : наказ Уповноваженого Верховної Ради з прав

6. людини № 1/02-14 від 8 січня 2014 р.

7. Про основні засади розвитку інформаційного суспільства в Україні : закон України від 9 січня 2007 р. № 537-V // Відомості Верховної Ради України. – 2007. – № 12. – ст. 102.

8. Про схвалення стратегії розвитку інформаційного суспільства в Україні : розпорядження Кабінету Міністрів України від 15 травня 2013 р. № 386.

9. Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію : постанова Кабінету Міністрів України від 19 жовтня 2016 р. № 736.

10. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : постанова Кабінету Міністрів України від 29 березня 2006 р. № 373.

11. Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці: НД ТЗІ 1.6-005-2013 : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації Служби безпеки України від 15 квітня 2013 р. № 215.

12. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.5-005-99 : наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 р. № 22.

13. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99 : наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 р. № 22.

14. Критерії класифікації закладів охорони здоров'я за рівнями подання медичної допомоги. Методичні рекомендації / Міністерство охорони здоров'я України. Український інститут стратегічних досліджень. – К., 2010. – 21 с.

15. Медична реформа: плани на 2018 рік [електронний ресурс]. – Режим доступу : http://www.medcv.gov.ua/archives/11066 – (дата звернення: 9.03.2018)

16. Захист персональних даних у сфері охорони здоров'я: алгоритм змін : науковий вісник Херсонського державного університету. – 2014. – Випуск 6-1. Том 1. – С. 216–221.

17. Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2: НД ТЗІ 2.5-008-2002 : наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13 грудня2002 р. № 84 (зі змінами від 28 грудня 2012 р. № 806).

References

1.1.1.1. Pro informatizaciyu: Zakon Ukrayini vid 2 zhovtnya 1992 r. №2657-HII// Vidomosti Verhovnoyi Radi Ukrayini.-1992.-№48.-st.650

1.1.1.2. Pro zahist informaciyi v informacijnih telekomunikacijnih sistemah: Zakon Ukrayini vid 31 travnya 2005 r. №2594-IV// Vidomosti Verhovnoyi Radi Ukrayini.-2005.-№26.-st.347

1.1.1.3. Pro zahist personalnih danih: Zakon Ukrayini vid 1 chervnya 2010 r. №2297-VI // Vidomosti Verhovnoyi Radi Ukrayini.-2010.-№34.-st.481

1.1.1.4. Zahist personalnih danih paciyentiv pid osoblivoyu uvagoyu Ombudsmena / elektronnij resurs // www.med-info.net.ua/index.php?q=content(data zvernennya: 12.10.2017)

1.1.1.5. Tipovij poryadok obrobki personalnih danih: Nakaz Upovnovazhenogo Verhovnoyi Radi z prav lyudini №1/02-14 vid 8 sichnya 2014 r.

2. Pro osnovni zasadi rozvitku informacijnogo suspilstva v Ukrayini: Zakon Ukrayini vid 9sichnya 2007 r. №537-V// Vidomosti Verhovnoyi Radi Ukrayini.-2007.-№12.-st.102

3. Pro shvalennya strategiyi rozvitku informacijnogo suspilstva v Ukrayini: Rozporyadzhennya Kabinetu Ministriv Ukrayini vid 15 travnya 2013 r. №386

4. Tipova instrukciya pro poryadok vedennya obliku, zberigannya, vikoristannya i znishennya dokumentiv ta inshih materialnih nosiyiv informaciyi, sho mistyat sluzhbovu informaciyu: Postanova Kabinetu Ministriv Ukrayini vid 19 zhovtnya 2016 r. №736

5. Pro zatverdzhennya Pravil zabezpechennya zahistu informaciyi v informacijnih, telekomunikacijnih ta informacijno-telekomunikacijnih sistemah: Postanova Kabinetu Ministriv Ukrayini vid 29 bereznya 2006 r. №373

6. Zahist informaciyi na ob'yektah informacijnoyi diyalnosti. Polozhennya pro kategoriyuvannya ob'yektiv, de cirkulyuye informaciya z obmezhenim dostupom, sho ne stanovit derzhavnoyi tayemnici: ND TZI 1.6-005-2013. Nakaz Administraciyi Derzhavnoyi sluzhbi specialnogo zv'yazku ta zahistu informaciyi Sluzhbi bezpeki Ukrayini vid 15 kvitnya 2013 r. №215

7. Klasifikaciya avtomatizovanih sistem i standartni funkcionalni profili zahishenosti obroblyuvanoyi informaciyi vid nesankcionovanogo dostupu: ND TZI 2.5-005-99. Nakaz Departamentu specialnih telekomunikacijnih sistem ta zahistu informaciyi Sluzhbi bezpeki Ukrayini vid 28 kvitnya 1999 r. №22

8. Terminologiya v galuzi zahistu informaciyi v komp'yuternih sistemah vid nesankcionovanogo dostupu:ND TZI 1.1-003-99. Nakaz Departamentu specialnih telekomunikacijnih sistem ta zahistu informaciyi Sluzhbi bezpeki Ukrayini vid 28 kvitnya 1999 r. №22

9. Kriteriyi klasifikaciyi zakladiv ohoroni zdorov'ya za rivnyami podannya medichnoyi dopomogi. Metodichni rekomendaciyi. Ministerstvo ohoroni zdorov'ya Ukrayini. Ukrayinskij institut strategichnih doslidzhen. - K., 2010. - 21s

10. Medichna reforma: plani na 2018 rik / elektronnij resurs // http://www.medcv.gov.ua/archives/11066 (data zvernennya: 9.03.2018)

11. Zahist personalnih danih u sferi ohoroni zdorov'ya: algoritm zmin Naukovij visnik Hersonskogo derzhavnogo universitetu Vipusk 6-1. Tom 1. 2014,S. 216-221.

12. Vimogi iz zahistu sluzhbovoyi informaciyi vid nesankcionovanogo dostupu pid chas obroblennya v avtomatizovanih sistemah klasu 2: ND TZI 2.5-008-2002. Nakaz Departamentu specialnih telekomunikacijnih sistem ta zahistu informaciyi Sluzhbi bezpeki Ukrayini vid 13 grudnya2002 r. №84 (zi zminami vid 28 grudnya 2012 r. №806)

Рецензія/Peer review : 4.05.2018 р. Надрукована/Printed :05.07.2018 р.
Рецензент: д.т.н., проф. А.Я. Кулик