**Пиркова О.В.**
Харківський національний університет міського господарства імені О.М. Бекетова

## ТЕОРЕТИЧНІ АСПЕКТИ ЩОДО ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ФОРМУВАННЯ ТА РЕАЛІЗАЦІЇ МІСТОБУДІВНОГО МОНІТОРИНГУ ЗЕМЕЛЬ

**Анотація**
Систематизовані підходи до визначення теоретичних аспектів забезпечення містобудівного моніторингу земель. Зосереджена увага на застосуванні геоінформаційних систем для здійснення містобудівного моніторингу земель. Доведена необхідність використання плану територій для здійснення містобудівного моніторингу земель. Визначені інструменти формування містобудівного моніторингу. Охарактеризовані показники інвестиційної привабливості реалізації будівельних програм і проектів у рамках здійснення містобудівного моніторингу земель.
**Ключові слова:** містобудівний моніторинг земель, технології, план територій, інструменти, показники інвестиційної привабливості реалізації будівельних програм і проектів, ГІС.

**Пыркова О.В.**
Харьковский национальный университет городского хозяйства имени А.Н. Бекетова

## ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ПО ПРИМЕНЕНИЮ ТЕХНОЛОГИЙ ФОРМИРОВАНИЯ И РЕАЛИЗАЦИИ ГРАДОСТРОИТЕЛЬНОГО МОНИТОРИНГА ЗЕМЕЛЬ

**Аннотация**
Систематизированы подходы к определению теоретических аспектов обеспечения градостроительного мониторинга земель. Сосредоточено внимание на применении геоинформационных систем для осуществления градостроительного мониторинга земель. Доказана необходимость использования плана территорий для осуществления градостроительного мониторинга земель. Определены инструменты формирования градостроительного мониторинга. Охарактеризованы показатели инвестиционной привлекательности реализации строительных программ и проектов в рамках осуществления градостроительного мониторинга земель.
**Ключевые слова:** градостроительный мониторинг земель, технологии, план территорий, инструменты, показатели инвестиционной привлекательности реализации строительных программ и проектов, ГИС.

УДК 004.056

## ЗАХИСТ ПЕРСОНАЛЬНИХ МЕДИЧНИХ ДАНИХ В СПЕЦІАЛІЗОВАНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ

**Розломій І.О.**
Черкаський національний університет імені Богдана Хмельницького

Запропонована методика дозволяє вирішити задачу підвищення рівня захищеності медичної інформаційної системи (МІС) та її ресурсів. Основними етапами розробки системи захисту персональних медичних даних є аналіз структури та визначення особливостей МІС, виявлення можливих загроз та вразливих ресурсів, дослідження джерел загроз та визначення рівня порушення безпеки.
**Ключові слова:** медична інформаційна система, персональні дані, система захисту, аутентифікація, ідентифікація.



**Постановка проблеми.** Однією з найактуальніших проблем, які сьогодні доводиться вирішувати в медичних закладах при використанні комп'ютерів, є захист персональних медичних даних. Захищеність персональних медичних даних визначається надійністю методів та засобів, які дозволяють забезпечити доступність, конфіденційність, цілісність інформації, в умовах впливу на неї негативних чинників природного і штучного характеру.

В останні роки гостро постало питання захисту персональних даних громадян, що обробляються в інформаційних системах. Цьому сприяє бурхливий розвиток ринку самих інформаційних систем персональних даних, зростання кількості злочинів у сфері високих технологій та вимоги законодавства.

**Аналіз останніх досліджень і публікацій.** Розробкою засобів захисту інформації займалися такі вчені як, Романец Ю.В., Герасименко В.А., Молдовян А.А.

**Виділення не вирішених раніше частин загальної проблеми.** Існує досить велика кількість розроблених методик та підходів щодо створення систем захисту інформації, проте конкретно область захисту медичної інформації на даному етапі не повністю досліджена. Існує ще ряд невирішених питань в сфері захисту персональних медичних даних, на вирішенні яких варто зупинитися.

**Мета статті.** Метою роботи є створення методики захисту персональних медичних даних, на основі розробки нових і вдосконаленні наявних методів і засобів захисту інформації.

**Виклад основного матеріалу.** Особливе місце серед систем цього класу займають медичні інформаційні системи (МІС), оскільки в них обробляються

персональні медичні дані (ПМДн) – відомості про стан здоров'я громадян, які відносяться до лікарської таємниці. Сучасні інформаційні технології відіграють найважливішу роль у медичній галузі, але однією з найбільш серйозних проблем, що перешкоджають їх повсюдному впровадженні, є забезпечення захисту інформації, в тому числі захисту персональних даних громадян і відомостей, що становлять медичну таємницю, – персональних медичних даних. Актуальність проблеми захисту персональних медичних даних сьогодні не викликає сумнівів. Кібертероризм, доступ фізичних осіб до баз персональних даних посилюють ризик вторгнення в сферу приватного життя і порушення права на її недоторканність. Захист персональних медичних даних є однією з найбільш гострих проблем в інформатизації організацій медичної галузі [1, с. 9].

Захищеність інформаційної системи характеризується рівнем безпеки. Визначити стан рівня безпеки МІС можна за допомогою моделі Белла-Лападули. Нехай, $T$ – рівень конфіденційності, множина прав доступу до системи, де $r$ – доступ до читання, $w$ – доступ до запису, $n$ – послідовність прав доступу, $i$ – послідовність рівнів конфіденційності стан називається досягнутим в системі $\sum=(v_0,R,T)$, якщо існує послідовність $\{(r_0, w_0),..., (r_{n-1}, w_{n-1}), (r_n, v_n)\}$: T $(r_i, w_i)$.

Система $\sum=(v_0,R,T)$ є безпечною, якщо її початковий стан $v_0$ – безпечний, і всі стани, досягнуті з $v_0$ шляхом застосування кінцевої послідовності запитів із $R$ – безпечні.

Захист медичних інформаційних систем є необхідністю, остільки дані системи можуть значно підвищити безпеку і якість медичної допомоги, збільшити оперативність подання медичної інформації, забезпечити комфортність у роботі медичного персонал. Розробка методів і засобів захисту медичних інформаційних систем складається з сукупності етапів, наведених на рисунку 1.

Медична інформаційна система (МІС) – комплексна автоматизована інформаційна система для автоматизації діяльності лікувально-профілактичного закладу, в якій об'єднані система підтримки прийняття медичних рішень, електронні медичні записи про пацієнтів, дані медичних досліджень у цифровій формі, дані моніторингу стану пацієнта з медичних приладів, засоби спілкування між співробітниками, фінансова та адміністративна інформація. Ядро МІС – персональні медичні дані, які є конфіденційними [2, с. 34].

Конфіденційною вважається документована інформація, доступ до якої обмежується в залежності законодавства України, Закон України «Про захист персональних даних», який поширюється на всіх суб'єктів господарської діяльності в медичній сфері незалежно від форми власності та відомчого підпорядкування. Володарем інформації, що має лікарську таємницю є пацієнт (суб'єкт персональних даних). Персональні медичні дані можна класифікувати, в залежності від ступеня конфіденційності. З цього слідує, що кожна категорія потребує різної складності захисту. Відомості про стан здоров'я відносяться до найвищої категорії конфіденційності, тому їх захисту потрібно надати особливу перевагу.

Автоматизація діяльності лікувально-профілактичного закладу передбачає внесення персональних даних пацієнта до медичної інформаційної системи. В процесі зберігання дані можуть оброблятися, накопичуватися, передаватися по мережі, редагуватися, знищуватися, розповсюджуватися. Дії, які несуть негативний характер є загрозами безпеки персональних даних, тобто сукупність умов та факторів, що створюють небезпеку несанкціонованого, в тому числі випадкового, доступу до персональних даних, результатом якого може стати знищення, зміна, блокування, копіювання, поширення персональних даних, а також інших несанкціонованих дій при їх обробці в інформаційній системі персональних даних.

Джерелом загрози безпеки інформації є суб'єкт доступу, матеріальний об'єкт або фізичне явище, що є причиною виникнення загрози безпеки інформації. Джерела загроз інформаційної безпеки можуть бути технічними, програмними або антропогенними, тобто спричинені людиною. Загрози технічного характеру можуть бути викликані неправильною експлуатацією обладнання, що є причиною виходу його з ладу. Програмні загрози є наслідком дії шкідливого програмного забезпечення, програм-вірусів. Найбільш вагомою є загроза з боку людського фактору і може мати зовнішній і внутрішній вплив.

В якості зовнішнього порушника інформаційної безпеки, розглядається порушник, який не має безпосереднього доступу до технічних засобів та ресурсів системи, яка перебуває в межах контрольованої зони.

Можливості внутрішнього порушника істотно залежать від діючих в межах контрольованої зони обмежувальних факторів, з яких основним є реалізація комплексу організаційно -технічних заходів, у тому числі з підбору, розстановці і забезпеченню високої професійної підготовки кадрів, допуску фізичних осіб всередину контрольованої зони та контролю за порядком проведення робіт, спрямованих на запобігання і припинення несанкціонованих дій.

До внутрішніх порушників можуть належати:
1) адміністратори МІС;
2) користувачі МІС;

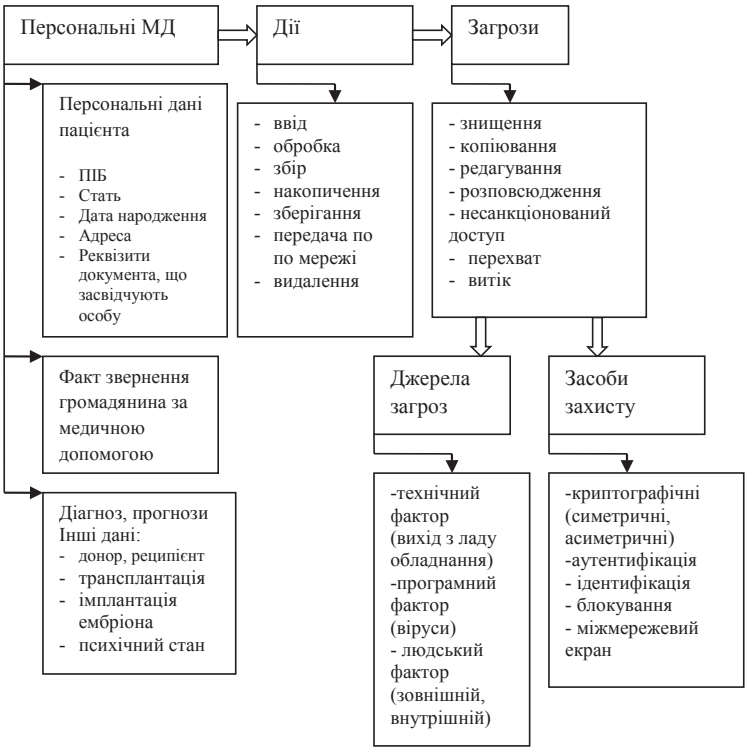


**Рис. 1. Схема персональних медичних даних**

3) особи, що володіють можливістю доступу до системи передачі даних;

4) співробітники лікувально-профілактичних закладів (ЛПЗ), що мають санкціонований доступ в службових цілях в приміщення, в яких розміщуються ресурси МІС, але не мають права доступу до ресурсів;

5) обслуговуючий персонал ЛПЗ (охорона, працівники інженерно- технічних служб);

6) уповноважений персонал розробників МІС, який на договірній основі має право на технічне обслуговування і модифікацію компонентів МІС.

Проаналізувавши загрози та їх джерела, стає явною необхідність захисту персональних медичних даних. Для захисту персональних даних в медичних закладах використовуються різні засоби і методи захисту.

Основою будь-яких систем захисту інформаційних систем є ідентифікація та аутентифікація.

Присвоєння суб'єктам та об'єктам доступу особистого ідентифікатора і порівняння його з заданим переліком називається ідентифікацією. Ідентифікація забезпечує виконання таких функцій:

1) встановлення автентичності та визначення повноважень суб'єкта при його допуску в систему;

2) контроль встановлених повноважень в процесі сеансу роботи;

3) реєстрація дій.

Аутентифікацією (встановленням достовірності) називається перевірка приналежності суб'єктові доступу пред'явленого ним ідентифікатора і підтвердження його достовірності.

Безумовно, надійними засобами захисту інформації є криптографічні методи. Криптографічні методи захисту інформації включають спеціальні методи шифрування, кодування та іншого перетворення інформації, які роблять її вміст недоступним без пред'явлення ключа криптограми і зворотного перетворення. Дані методи ефективні, перш за все тим, що забезпечують надійний захист безпосередньо самій інформації, а не доступу до неї. Даний метод захисту реалізований у вигляді програм чи пакетів програм [3, с. 114].

**Висновки і пропозиції.** Таким чином, в роботі запропоновано підхід до створення системи захисту персональних медичних даних, який ґрунтується на використанні таких засобів захисту інформації як ідентифікація, аутентифікація та криптографічних методів, що дозволить підвищити потужність роботи всієї інформаційної системи та якість надання медичних послуг. При аналізі було виявлено, що не існує єдиного, конкретного методу захисту даних. Ефективності в захисті системи можливо досягти лише в комплексному використанні засобів захисту інформації, використовуючи їх в певній послідовності, розглядаючи з точки зору конкретного об'єкту захисту.

**Список літератури:**

1. Емельянников М. Ю. Особенности защиты персональних данных в медицинской отрасли. – М.: Код безопасности, 2010. – 17 с.
2. Зыков В. Д. Структура програмного обеспечения системы защиты рабочего места обработки персональних медицынских данных // Научная сессия ТУСУР – 2007. – 156 с.
3. Нечаев В. И. Элементы криптографии (Основы теории защиты информации). – М.: Высшая школа, 1999. – 347 с.

**Розломий И.А.**
Черкасский национальный университет имени Богдана Хмельницкого

## ЗАЩИТА ПЕРСОНАЛЬНЫХ МЕДИЦИНСКИХ ДАННЫХ В СПЕЦИАЛИЗИРОВАННЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ

**Аннотация**
Предложенная методика позволяет решить задачу повышения уровня защищенности медицинской информационной системы (МИС) и ее ресурсов. Основными этапами разработки системы защиты персональных медицинских данных являются анализ структуры и определение особенностей МИС, выявления возможных угроз и уязвимых ресурсов, исследования источников угроз и определения уровня нарушения безопасности.
**Ключевые слова:** медицинская информационная система, персональные данные, система защиты, аутентификация, идентификация.

**Rozlomii I.O.**
Cherkassy B. Khmelnickiy National University

## PROTECTION OF PERSONAL MEDICAL DATA IN THE SPECIALIZED COMPUTER SYSTEMS

**Summary**
An offer methodology allows to decide the task of increase of level of security of the medical information system (MIS) and her resources. Basic design of the system of protection of the personal medical data times are an analysis of structure and determination of features of MIS, exposure of possible threats and vulnerable resources, research of sources of threats and determination of level of security breach.
**Keywords:** medical informative system, personal data, system of defense, authentification, identification.