За результатами дослідження було зроблено наступні висновки:

1. Виявлено, що для алгоритму AES час шифрування зростає пропорційно до збільшення розміру ключа.

2. За результатами проведених досліджень можна стверджувати, що кібербезпека для хмарних сервісів зростає завдяки використанню алгоритму Blowfish, адже у ньому поєднується і малі затрати на час шифрування, і висока криптостійкість.

3. У наслідок комплексного порівняння досліджуваних алгоритмів шифрування за ознаками: тип шифрування, можливі набори ключів, час злому ключа методом «Повного перебору» та за загальною характеристикою безпеки; було систематизовано основні характеристики кожного з них та здійснено порівняння їх за власними обчисленнями (шифрування) за ознакою «час шифрування різного розміру файлів».

4. За результатами власних обчислень доведено, що для алгоритму Blowfish час шифрування є мінімальним незалежно від розміру файлу, проте для алгоритму AES затрати часу для шифрування є максимальними для великих файлів.

Література:

1. Yogesh Kumar, Rajiv Munjal and Harsh Sharma,"Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.

2. Chadi Riman, Pierre E. Abi-Char "Comparative Analysis of Block Cipher-Based Encryption Algorithms: A Survey" Information Security and Computer Fraud, 2015, Vol. 3, No. 1, 1-7.

3. W. Stallings, Cryptography and Network Security, 4th Edition, Pearson Prentice Hall, 2006.

4. Agrawal Monika, Mishra Pradeep, "A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, pp. 877-882.

УДК 004.415:725.513

Юрчук Б.О.
Науковий керівник: к.е.н, доцент Коляденко С.В.
Вінницький національний аграрний університет

ПОБУДОВА ІНФОРМАЦІЙНОЇ СИСТЕМИ ЛІКАРНІ

YURCHUK B.O.

CONSTRUCTION OF THE INFORMATION SYSTEM FOR A HOSPITAL

Сучасне життя неможливе без ефективного керування. Важливою категорією керування є системи обробки інформації, від яких багато в чому залежить ефективність роботи будь-якого підприємства. Дана система

повинна забезпечувати одержання загальних звітів за підсумками роботи, дозволяти легко визначати тенденції зміни найважливіших показників, забезпечувати одержання інформації, критичної за часом, без істотних затримок, виконувати точний і повний аналіз даних.

XXI – століття активного розвитку інформаційних технологій у всіх галузях народного господарства. Для сучасного стану ІС суспільства, питання медичного обслуговування є дуже важливим, особливо на теперішній час, коли хворих стає все більше. Лікарня – це та установа, яка намагається підтримати та поліпшити стан здоров’я людей, а отже їхню працездатність. В нашій державі існує багато медичних установ, але їхня робота не завжди продуктивна саме в плані автоматизації даних лікарні. В тих установах де існує ІС – вона застаріла і потребує реорганізації та реструктуризації.

Оскільки ІС автоматизації роботи лікарні є відносно небагато і переважно всі вони написані для лікарень профільного напряму, тому в даній роботі описано ІС із загальним варіантом автоматизації БД.

Спрощений алгоритм роботи поліклініки виглядає наступним чином: хворий (пацієнт) приходить на прийом до лікаря, останній проводить обстеження і ставить діагноз. Так визначається хвороба пацієнта і назначається відповідне лікування. В процес лікування входить: призначення медикаментозних препаратів, фізпроцедур, режиму лікування та багато іншого. Щодо самого медперсоналу, то у БД інформаційної системи `поліклініки` повинні міститися дані про освіту, посади, порядок чергування та відділень де працюють співробітники `поліклініки`. Все ці дані розміщено у таблицях БД.

Отже, доопрацьована ІС обліку пацієнтів та їх лікування, які надає лікарня має автоматизувати наступні задачі:

- облік призначення діагнозів;
- облік лікування пацієнтів;
- облік медперсоналу та пацієнтів.

Для автоматизації поставлених задач необхідно в СУБД створити таблиці, та з’єднати їх між собою логічними зв’язками. Графічне зображення ІС наведено на рисунку 1.

Між атрибутами кожної окремої таблиці встановлено співвідношення 1:1. Окремі атрибути інформаційних об’єктів потрапили не в одну, а в декілька таблиць, але в кожній з них вони мають різне функціональне призначення. Наприклад, *Код Співробітника* в таблиці *Медперсонал* містить унікальний внутрішній ідентифікаційний номер кожного співробітника, в таблиці *Прийом Пацієнтів* цей самий атрибут містить код того співробітника, який прийняв певного пацієнта, в таблиці *Лікування* – який лікує певного пацієнта, в таблиці *Освіта Співробітників* – який отримав освіту, в таблиці *Чергування* – який чергує по дням.

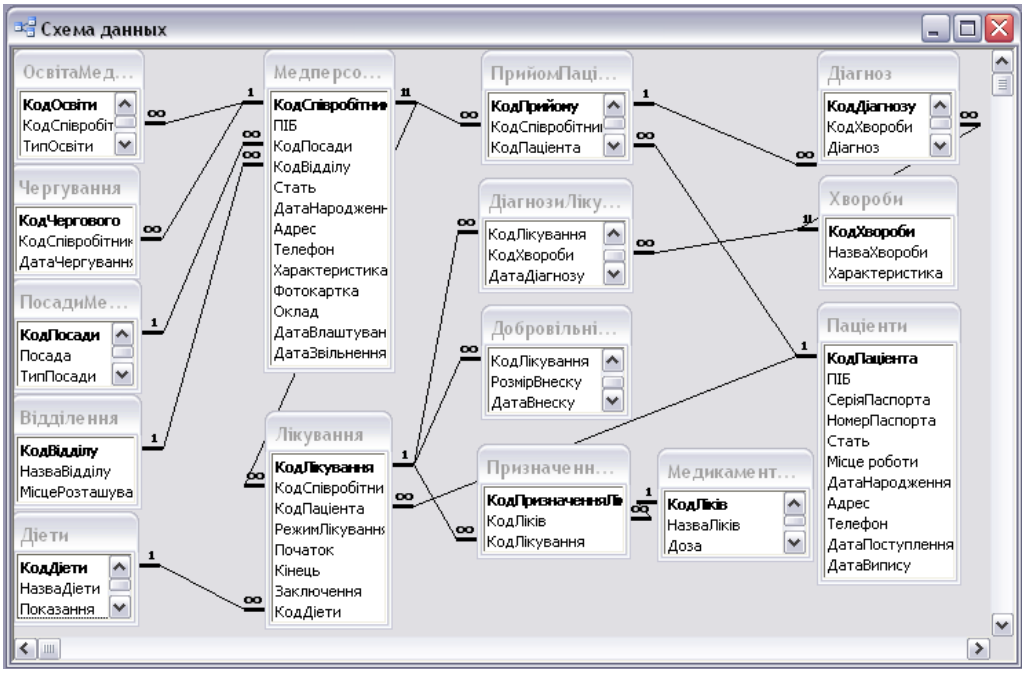

Рис. 1. Графічне зображення ІС поліклініки

Перед початком експлуатації системи необхідно розробити та затвердити єдині методи кодування інформації і неухильно дотримуватися їх при редагуванні даних. Це дозволить усунути дублювання, надлишковості та неузгодженості даних ще на етапі введення.

Література:

1. Основи створення інформаційних систем: Навчальний посібник / Береза А.М., 2-ге видання. – К.: КНЕУ – 2001р. – 156ст.

2. Проектування баз даних інформаційних систем: Методичка / Бойко В.В., Савинов В.М. – 2009р. – 246ст.

3. Практикум з інформатики та комп’ютерної техніки. Частина ІІ. Прикладна інформатика: Навч.-метод. Посібник / Шпортько О.В. – Рівне: РДГУ, 2003 –64 с.

4. Загальні відомості про типи даних і властивості полів [Електронний ресурс] : проект / Microsoft – електронні дані – Режим доступу: https://support.office.com/uk-UA/Access