УДК 004.65

Семенюк А. М., здобувач вищої освіти;
Антонов Ю. С., канд. фіз-мат. наук, доцент,
доцент кафедри інформаційних технологій,
Донецький національний університет імені Василя Стуса

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ У КЛІЄНТ-СЕРВЕРНИХ ДОДАТКАХ НА ПРИКЛАДІ МЕДИЧНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Ключові слова: інформаційна система, конфіденційність, цілісність даних, експертиза працездатності.

Вступ. У сучасному світі інформаційні системи використовуються для автоматизації діяльності бізнес-процесів різноманітних організацій, підприємств або установ. З одного боку, це дає змогу спростити та пришвидшити певні робочі процеси, але з іншого боку, може мати певні ризики.

Актуальність. Специфіка роботи інформаційних систем різних видів передбачає роботу з різноманітними даними, частина з яких може бути конфіденційною або чутливою інформацією [1], особливо це стосується медичних інформаційних систем (МІС). До того ж, одночасно працювати з такою системою має певна кількість користувачів, а це означає, що будуть використані також і мережеві технології. У такій ситуації виникає питання комплексних заходів, що до захисту інформації на всіх рівнях [2]. До того ж у окремих ситуаціях може виникнути питання захисту системи від зовнішніх кіберзагроз. Враховуючи постійний розвиток ІТ-галузі, актуальним є аналіз та узагальнення сучасних методик і рекомендацій щодо захисту інформації.

Огляд аналогів досліджень. Один із можливих адекватних засобів управління мірою забезпечення безпеки ІТ-інфраструктури є зменшення (в ідеальному варіанті – ліквідація) потенційних вразливостей та прогалин безпеки. Оскільки інформаційні комунікаційні системи (ІКС) являють собою поєднання обладнання, програмного забезпечення та процедур, що дають змогу обробляти, зберігати, передавати та отримувати інформацію, то і підхід до їх захисту повинен бути комплексним [3, 4].

ІКС складаються з компонентів – комп’ютерів, мережевого обладнання, програмного забезпечення, баз даних тощо, – що використовуються для забезпечення функціонування організацій та інших суб’єктів і потребують захисту на кожному рівні.

Під час розробки та розгортання клієнт-серверних додатків можна виділити такі пункти, що потребують окремої уваги з погляду захисту інформації:

1. Захист мережі на основі використання, спеціального мережевого обладнання – активних інтелектуальних мережевих пристроїв, як-от керовані свічі, роутери, фаєрволи, системи виявлення вторгнень та інших [5].

2. Утворення безпечного SSH-з’єднання між клієнтом та сервером на основі ключів (без використання паролю) з одночасним задіянням фаєрволів на обох сторонах, що зменшує ризик несанкціонованих підключеннь до СУБД,

прослуховування трафіку, перехоплення й аналізу пакетів обміну на канальному рівні [6, 7].

3. Правильне адміністрування сервера, де розташована СУБД.

4. Керування правами доступу користувачів до інформації БД залежно від їх ролі на рівні таблиці, стовпчика, поля за допомогою SQL інструкцій, наприклад, Grant у MySQL [8].

5. Реалізація принципу власника для різних об’єктів у БД з наданням можливостей формування прав доступу до них для інших користувачів і з блокуванням доступу / редагування у створених програмах.

6. Недопущення зміни режимів роботи ІКС, ініціювання тестових або технологічних процесів, які здатні призвести до незворотних змін у системі.

Розглянемо у якості прикладу діяльність медичного персоналу, задіяного у роботі МСЕК, яка потребує роботи з конфіденційною (персональною) інформацією. Таку інформацію потрібно максимально захистити від несанкціонованого доступу сторонніх користувачів [10]. Це питання стає проблемним через масовий перехід до використання в медичній галузі комп’ютерної техніки, створенням великих масивів медичної інформації, недостатній рівень ІТ-підготовки медичних працівників.

Під час розробки додатку та проєктування БД для тих таблиць, де важливо розмежовувати доступ на рівні кортежів, додається атрибут owner_id та ще деякі потрібні атрибути. Надалі редагування або видалення таких записів може здійснювати лише власник, а для особливо чутливої інформації це буде стосуватись і перегляду (рис. 1).

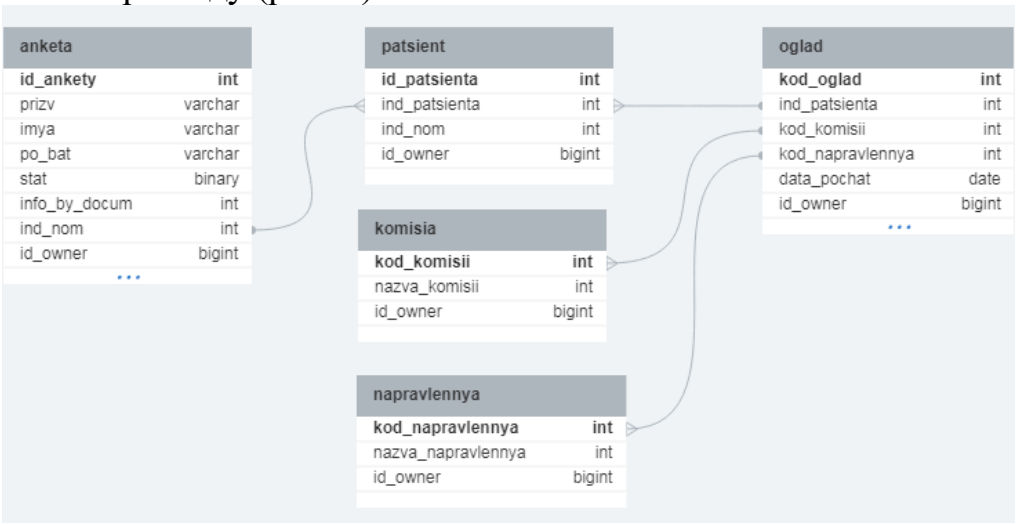

Рисунок 1 – Фрагмент реляційної моделі БД МСЕК

Після завершення розробки ПЗ необхідно вирішити питання з ролями та правами доступу до БД. Для кожної категорії користувачів на рівні СУБД створюється відповідна роль. Для кожної зі створених ролей забезпечуємо доступ лише до тих таблиць та атрибутів, які дійсно потрібні для цієї ролі. Отже, кожен користувач, що у отримає роль у системі, буде взаємодіяти лише з дозволеним набором таблиць та атрибутів відповідно до своїх повноважень:

1) реєстратори – вводять / коригують загальні дані: паспортні дані, відомості про роботу, адресу, категорію обліку (ліквідатори ЧАЕС, переселенці ЧАЕС, УБД, лікарі, та ін.); не мають доступу до медичної частини БД;

2) лікарі ЛКК – вводять медичну інформацію відповідно до наданих клінічних обстежень, висновками «вузьких» спеціалістів тощо; – частково доступна реєстраційна частина БД (професія, місце роботи, категорія, вік – !!! НЕ ДАТА НАРОДЖЕННЯ !!!), можуть коригувати дані, які ввели, – голова комісії володіє всією інформацією ЛКК; не мають доступу до обстеження МСЕК;

3) лікарі МСЕК – вводять медичну інформацію відповідно до наданих даних ЛКК, експертних обстежень, особистого огляду, висновок про наявність втрат працездатності; – обмежений доступ до реєстраційної частини (подібно ЛКК); голова МСЕК має повний доступ до БД.

На рис. 2 зображена схема взаємодії підрозділів під час проведення обстеження пацієнта. Вся інформація розміщується на захищеному сервері з контрольованим доступом та послідовно заповнюється підрозділами і стає доступною для наступного рівня.

На наступному рівні кожен користувач отримує роль, яку він буде здійснювати у системі, та для нього створюється пари RSA-ключів: приватний та відкритий. Відкритий ключ розташуємо на сервері, де міститься БД. У цьому випадку ми отримаємо доступ до віддаленого сервера по захищеному SSH-тунелю. Цей тунель буде автоматично відкриватись перед роботою фахівця, а після завершення роботи, навпаки, закриватись. Для роботи з базою даних користувач проходить аутентифікацію з використанням особистих даних.

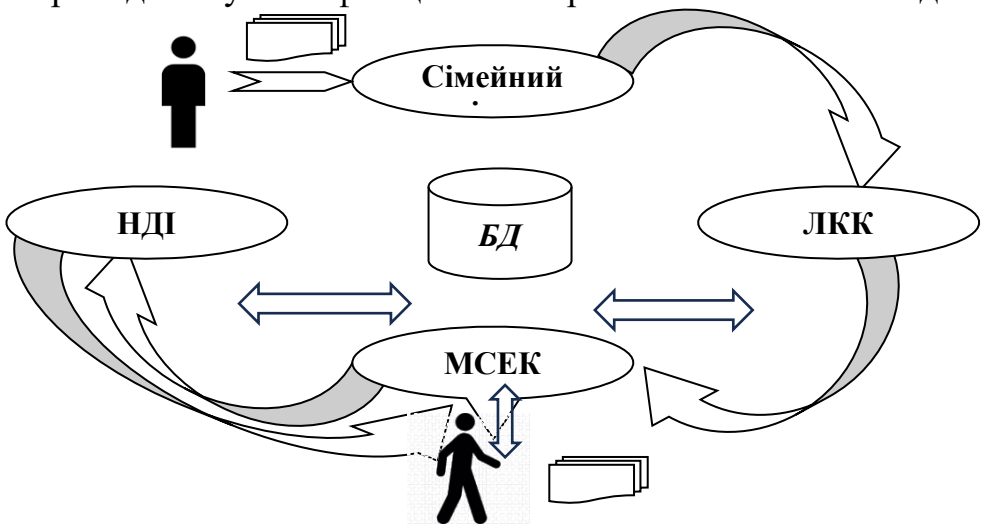

Рисунок 2 – Схема взаємодії підрозділів

Висновки

Запропонований у роботі підхід дає змогу зменшити ризики витоку конфіденційної інформації під час експлуатації інформаційних систем на базі клієнт-серверних технологій. Доступ до програмного забезпечення (АРМ МСЕК) організовано з використанням кожним спеціалістом особистих RSA-ключів, що надає додаткового захисту.

Список використаних джерел

1. Ярмакі Х. П., Музика С. С. Класифікація конфіденційної інформації, *Південноукраїнський правничий часопис*. DOI: 10.32850/sulj.2021.1.16.

2. Закон України «Про захист інформації в інформаційно-комунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

3. Інфомаційна та кібербезпека / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа. Київ: ДУТ, 2015. 288 с.

4. Вимоги до захисту інформації в інформаційних системах: роз'яснення Держспецзв'язку. URL: https://cip.gov.ua/ua/news/vimogi-do-zakhistu-informaciyi-v-informaciinikh-sistemakh-u-voyennii-chas-roz-yasnennya-derzhspeczv-yazku

5. What Is Network Security? URL: https://www.cisco.com/c/en/us/products/security/what-is-network-security.html

6. SSH Tunneling. URL: https://www.ssh.com/academy/ssh/tunneling

7. Access Your Database Remotely Through an SSH Tunnel. URL: https://support.cloud.engineyard.com/hc/en-us/articles/205408088-Access-Your-Database-Remotely-Through-an-SSH-Tunnel

8. GRANT Statement. URL: https://dev.mysql.com/doc/refman/8.0/en/grant.html

9. Семенюк А. М. Створення реєстраційної системи МСЕК. *Матеріали LII науково-технічної конференції підрозділів Вінницького національного технічного університету (НТКП ВНТУ–2023):* Вінниця, 21–23 червня 2023 р. С. 744–746.

10. Застосування арм-лікаря в структурі лікувально-профілактичного закладу / Д. Х. Штофель, С. В. Костішин, М. В. Московко, В. О. Гомолінський. *Східно-Європейський журнал передових технології.* 2011. Т. 4. № 3(52). С. 37–39.