УДК 004.65.056.53:61

А. С. АНДРІЙЧУК, А. А. СТРЄЛКІНА

Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», Україна

РОЗРОБЛЕННЯ МОДЕЛІ КЕРУВАННЯ ДОСТУПОМ ДО ПРИВАТНОЇ МЕДИЧНОЇ ІНФОРМАЦІЇ

Сучасна медицина виросла на нездоланний рівень за останні десятиліття. Сьогодні даний сектор людського життя є високотехнологічною галуззю, де успішно розвиваються всі сфери, які можуть врятувати життя раніше безнадійних пацієнтів. Значно вдосконалено технічне оснащення закладів охорони здоров'я, стало можливим діагностувати захворювання на ранніх стадіях та швидко відновити працездатність пацієнтів. Тим не менш, з усьома перевагами і можливостями сучасних технологій в даній сфері, виникає багато проблем. Однією з найбільш значних є забезпечення приватної медичної інформації, яка повинна роздивлятися з двох сторін як технічної, так і регламентуючої. Забезпечення приватності даних у медичних системах залежить від правильної і своєчасної організації керування доступом до медичної інформації. Найбільш поширеним і всеосяжним регламентуючим документом для забезпечення безпеки медичних даних є акт США Health Insurance Portability and Accountability Act (HIPAA). Щодо українських нормативних документів, то вони реалізують права пацієнта на отримання інформації про стан свого здоров'я, а медичні системи не мають сертифікат про відповідність комплексної системи захисту інформації згідно вимогам нормативних документів з технічного захисту інформації. В даній статті авторами розглядається проектування моделі керування доступом, яка вирішує проблему забезпечення інформаційної безпеки медичних систем і базується на керуванні доступом на основі ролей з мінімальними обмеженнями. Модель, що розроблюється, повинна визначати дії та ресурси, які доступні користувачу, а також надавати індивідуальний доступ до ресурсів. Авторами було проведено дослідження існуючих моделей керування доступом, виявлені переваги та недоліки, аналіз чого поляг в основу розроблення власної моделі. В роботі описується створення політики безпеки на основі ролей, яка визначає дозволені в системі потоки інформації, спираючись на міжнародний регламентуючий документ HIPAA. За допомогою розробленої моделі, можна по різному виконати її зберігання і в будь-якому випадку дуже просто перевести у реляційну базу даних.

Ключові слова: *приватна медична інформація, модель доступу, модель політики безпеки, HIPAA, RBAC.*

Вступ

На сьогоднішній день, медицина є однією зі сфер послуг, яка на наших очах переходить у цифровий вимір [1]. Паперові дані, що займали кілька кімнат, зараз вміщуються у кишені, а доступ можна отримати із будь-якої точки земної кулі.

Медицина – це галузь, де приватність, цілісність, доступність, знаходиться вище, ніж дизайн та інтерфейс додатку. Тому, для забезпечення безпеки даних пацієнтів у EMR (англ. Electronic Medical Record)-системах необхідно ретельно розробити модель доступу даних ґрунтуючись на міжнародний стандарт HIPAA (англ. Health Insurance Portability and Accountability Act) [2].

Процес переходу до цифрових технологій веде за собою зростання користувачів та додатків, як наслідок – зростає і об'єм даних. У купі, це призводить до проблем масштабування системи. Зростання користувачів веде до появи ролей, груп, привілеїв, а тому потребується втручання у поведінку системи.

Нездатність дотримування HIPAA піддає ризику акредитацію та репутаційні збитки, судові позови, фінансові штрафи у розмірі від 100 до 250 000 доларів США та тюремне ув'язнення в межах від одного до десяти років [2].

Таким чином, **метою** даної роботи є проектування моделі керування доступом на основі ролей, яка задовольняє усім вимогам міжнародного регламентуючого документу HIPAA та забезпечує захист персональної інформації, що використовується медичними організаціями.

1. Регламентуючі документи інформаційної безпеки в медичних системах

Розробка програмного забезпечення для галузі охорони здоров'я є однією із перспективних галузей в інформаційних технологіях [3], але в процесі ви-

никає багато труднощів та обмежень. Вони пов'язані із вимогами дотримання захисту [4] та конфіденційності інформації [5], пов'язаної із здоров'ям.

В Україні забезпечення конфіденційності інформації пацієнтів гарантується наступною нормативно-правовою базою [6]:

– Закон України «Про захист персональних даних»;

– Закон України «Про охорону здоров'я».

Нормативні гарантії дані Законом України реалізують права пацієнта на отримання інформації про стан свого здоров'я. Для отримання цієї інформації, пацієнт подає запит щодо доступу до персональних даних вказавши в запиті лише прізвище, ім'я та по батькові, місце проживання і реквізити документа, який посвідчує його особу. Водночас у запиті пацієнт вказує перелік персональних даних, які його цікавлять, заклад охорони здоров'я, до якого він звертається із запитом. Тому ця гарантія більш формальна, а на практиці пацієнт, аби отримати дані, зазначає значно більше інформації, аби можна було дати відповідь на його запит.

У вересні 2017 року відбувся запуск Електронної системи охорони здоров'я eHealth [7]. Це інформаційно-телекомунікаційна система, що забезпечує автоматизацію ведення обліку медичних послуг та управління медичною інформацією в електронному вигляді, до складу якої входять центральна база даних та електронні медичні інформаційні системи, між якими забезпечено автоматичний обмін даними через відкритий програмний інтерфейс. eHealth забезпечить електронізацію системи охорони здоров'я, сприятиме захисту прав лікарів та пацієнтів та об'єднає медичні електронні системи [8].

В основі роботи системи лежить наступна нормативно-правова база [9]:

– Закон України "Про державні фінансові гарантії надання медичних послуг та лікарських засобів";

– Наказ МОЗ "Про затвердження Порядку надання первинної медичної допомоги";

– Наказ МОЗ "Про затвердження Порядку вибору лікаря, який надає первинну медичну допомогу, та форми декларації про вибір лікаря, який надає первинну медичну допомогу";

– Постанова КМУ "Про затвердження порядку функціонування електронної системи охорони здоров'я".

Але на сьогоднішній день eHealth не має у наявності сертифікату про відповідність комплексної системи захисту інформації (КСЗІ) згідно вимогам нормативних документів з технічного захисту інформації [10], і безпечним назвати зберігання даних пацієнтів не можна. Тому при розробці програмного забезпечення найкращим буде дотримуватись вимог HIPAA, як перевіреного та налагодженого стандарту.

Основні вимоги щодо медичної інформації регламентуються федеральним законом США «Про відповідальність і перенесення даних про страхування здоров'я громадян». Під дію документів HIPAA попадають медичні організації, такі як медичні заклади, страхові компанії, центри медичних розрахунків. Основним завданням цього нормативного акту є захист персональних даних пацієнтів, заборона розголошення лікарської таємниці і покарання винних у разі умисного чи ні порушення певних правил. Цей закон спрямований на впровадження сучасних технологій в індустрію охорони здоров'я і при цьому забезпечувати захист і приватність інформації, пов'язаної зі здоров'ям. У сферу цього закону можуть входити певні організації (наприклад, лікарні, лікарські кабінети, стоматологічні клініки) і окремі особи, які взаємодіють з захищеними даними про здоров'я. Також ці закони можуть поширюватися на компанії, що працюють з подібними організаціями і від імені цих організацій взаємодіють з захищеними даними про здоров'я.

Згідно [4] правило конфіденційності забезпечує федеральний захист персональної інформації, що використовується медичними організаціями, і надає пацієнтам сукупність прав щодо цієї інформації, а також дозволяє розкривати персональну інформацію про здоров'я, необхідну для лікування пацієнтів та використання в інших важливих цілях. Предметом захисту є персональні медичні дані пацієнта, які включають в себе:

– інформацію про фізичне та психічне здоров'я пацієнта;

– історію його звернень до медичних установ;

– фінансову інформацію щодо медичних послуг;

– особисті дані пацієнта, за допомогою яких можна будь-яким чином ідентифікувати особистість пацієнта.

Таким чином, головним терміном HIPAA є захищена інформація про здоров'я (англ. PHI), яка включає в себе все, що може бути використано для ідентифікації особистості.

HIPAA дозволяє використовувати правило «Необхідного мінімуму» [11] при проектуванні систем, які задовольняють усі вимоги конфіденційності. Тобто, система повинна докласти всі необхідні зусилля, щоб використовувати, вимагати або розкривати тільки той мінімум інформації, котрій необхідний для досягнення мети.

Тому, виникає два питання:

– Кому необхідний доступ до PHI?

– Який тип доступу і які обмеження пов'язані із цим типом?

Також, із цього виникає висновок: все, що явно не дозволене, то заборонене.

Що стосується вимог до безпеки, то вони властиві будь-якій інформаційній системі:

– авторизація та автентифікація;
– автоматичне закриття сесії;
– шифрування даних.

Тобто, існує можливість визначити функціонал моделі керування доступом. Вона повинна визначати дії та ресурси, які доступні користувачу, а також надавати індивідуальний доступ до ресурсів.

2. Проектування моделі керування доступом

Згідно [12], існує три основні категорії моделей керування доступом до конфіденційної медичної інформації:

– дискреційна;
– мандатна;
– ролева.

Є і інші, але це вузькоспеціалізовані політики, які не цікаві у контексті цієї статті, або похідні від вищеназваних.

Дискреційне або довільне керування доступом ґрунтується на понятті власника ресурсу [13]. Тільки власник вирішує, хто має доступ до ресурсу і з якими привілеями. Реалізується на основі списків доступу. Недолік цієї моделі у тому, що підтримка списків дуже затратна із ростом користувачів або об'єктів, бо користувач має прямий зв'язок із привілеями, а тому повна кількість цих відношень є кількість користувачів помножене на кількість ресурсів.

Мандатне або примусове керування доступом характеризується визначенням доступу самою системою, а не власником ресурсу [14]. Наприклад, призначення користувачу або групі користувачів мітки, та порівняння цього значення з міткою ресурсу. Серед недоліків – статичність, відсутність гнучкості.

Керування доступом на основі ролей (Role Based Access Control, RBAC) є розвитком моделей доступу на основі мандатної та дискреційної моделі. На відміну від них, ролева модель надає механізм побудови політики безпеки, а не накладає певні обмеження. В порівнянні з дискреційною моделлю, система контролює доступ до ресурсу на рівень вище, ніж власник ресурсу. Також, наявність ролей дає більше гнучкості, знижує складність конфігурації системи, тому що можна розділити систему на складові частини, на кожну призначити права і прив'язати їх до ролі. А далі – користувачам призначати ролі, а не привілеї. Модель на основі ролей не дозволяє користувачам безпосередньо зв'язуватись з привілеями [12].

Потреба у RBAC виникає з мінімально необхідних правил HIPAA [11]. Тобто, медичні організації (healthcare organizations, HCO) повинні розкривати тільки мінімально необхідну інформацію для досягнення мети.

HCO повинні визначити, хто вимагає доступ до PHI, щоб виконувати свою роботу, і якої інформації вони потребують. Тобто, HIPAA вимагає, щоб охоплені суб'єкти надавали працівникам доступ до мінімальної інформації, необхідної для виконання їх роботи, враховуючи їх особливу роль в організації, і найбільш ефективним шляхом є контроль доступу на основі ролей.

RBAC складається з чотирьох пов'язаних компонентів, що показано на рис. 1:

– користувач;
– роль;
– привілей;
– ресурс.

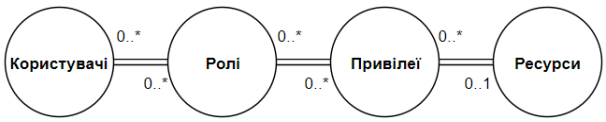

Рис. 1. Зв'язок компонентів RBAC

Користувач – це людина, або зовнішній для системи механізм, котрий взаємодіє із системою.

Роль – сукупність привілеїв. Кожен користувач може мати декілька ролей, та кожна роль може належати декільком користувачам.

Привілеї – набір прав доступу на певні ресурси. Одна роль може мати декілька привілеїв, а привілей може належати декільком ролям.

Ресурс – може бути чим завгодно, будь-який об'єкт, група об'єктів, окремі поля об'єкта, абстрактні сутності, та інше.

Отже, після визначення кожного компоненту ролевої моделі, необхідно зв'язати їх разом. Проектування зазвичай починається від моделі.

Результатом є модель відношень, яка представлена на рис. 2.

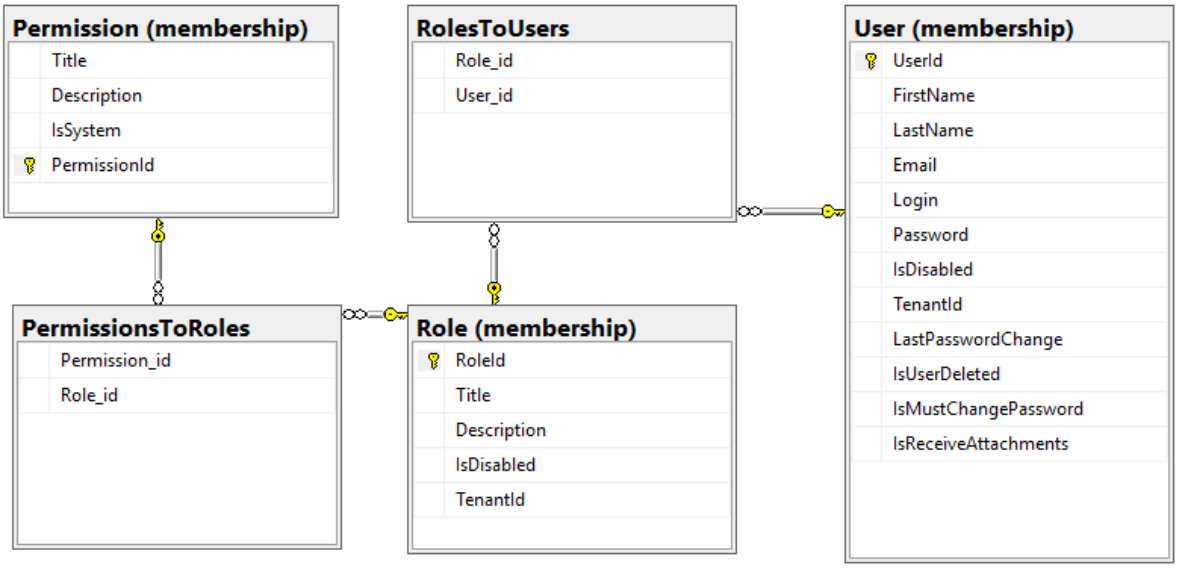

Рис. 2. Модель відношень

Згідно із схемою зв'язку компонентів RBAC, таблиця користувачів через відношення «багато до багатьох» пов'язана з таблицею ролей, це відношення реалізується через додаткову таблицю. Так само, таблиця з ролями пов'язується із привілеями.

Що стосується відношень привілею та ресурсу, то достатньо привести привілеї до перерахування, а саму сутність застосовувати як атрибут для контролера, властивості, або метода. Таким чином, контроль доступу не буде знаходитися в одній доменній області, що підвищує рівень безпеки. А реалізація логіки керування правами користувачів на стороні клієнта дозволяє не залежати від логіки фреймворку.

Однозначне іменування ролей, ресурсів і привілеїв обов'язкове, так як усі вони представлені окремими сутностями, а тому мають однозначну ідентифікацію по визначенню. У системі більше немає інших місць, де створюються ролі, ресурси або привілеї.

Маючи представлену вище модель, можна по різному виконати її зберігання, але в будь-якому випадку дуже просто перевести у реляційну базу даних. Необхідно лише правильно описати зв'язки, що доволі не складно, а деталі реалізації залежать від обраного стеку технологій.

3. Використання моделі для керування доступом у EMR-систему

У якості прикладу буде впровадження спроектованої моделі керування доступу у абстрактну міжнародну медичну організацію із існуючою EMR-системою.

Після надходження пацієнта до шпиталю, виконується запит конфіденційної інформації до державної бази даних. У такому випадку дані пацієнта – це об'єкт, а персонал лікарні, який взаємодіє із об'єктом – суб'єкт.

Оскільки модель ґрунтується на рольовій політиці безпеки, то остання складається з чотирьох пов'язаних компонентів, а саме ресурс, користувач, привілей і роль.

Першим кроком є визначення ресурсів, до яких треба обмежити доступ:

– дані пацієнта;
– запити на оновлення даних пацієнта;
– формування звітів по лікарні;
– налаштування системи.

Наступним кроком буде формування привілеїв системи, будуючись на технічний процес медичного закладу:

– керування налаштуваннями шпиталю;
– керування запитами до державної бази даних;
– керування ролями та користувачами;
– створення та перегляд запитів по лікарні;
– створення та перегляд даних пацієнта;
– створення та перегляд звітів.

Далі, дивлячись створені привілеї та враховуючи особливості кожного медичного закладу формується перелік ролей, як головний лікар, лікар, медична сестра, центр обслуговування пацієнтів і технічний спеціаліст.

Останнім кроком є проектування моделі керування доступу, базуючись на мінімальних вимогах HIPAA. В такому випадку, у користувача може бути багато ролей, а у ролі – багато користувачів. Так само, у ролі може бути багато привілеїв, а у приві-

лея – багато ролей. Спроектована ролева модель керування даних представлена у табл. 1.

На основі отриманого проекту, будується прикладна модель, реалізація якої залежить від обраного стеку технологій, але сама модель найчастіше накладається на базу даних, хоча існує можливість імплементації на стороні клієнта.

Висновки

Отже, розроблення програмного забезпечення для медичної галузі супроводжується постійним вирішенням проблем пов'язаних із захистом конфіденційної інформації користувачів. Але після появи закону США «Про відповідальність і перенесення даних про страхування здоров'я громадян», компанії, які займаються обробкою PHI, повинні дотримуватися необхідних вимог. HCO повинні запровадити необхідні рішення, щодо вимог, а це зумовлює додаткові дослідження та розробку.

Перш за все, забезпечення безпеки медичних систем залежать від правильної і своєчасної організації керування доступу до конфіденціальної інформації.

В статті описано основні мотиви початку досліджень, представлено основні регламентуючі документи, надано процес забезпечення інформаційної безпеки медичних систем, сформовані вимоги. Було спроектовано модель керування доступом на основі ролей, яка забезпечує захист персональної інформації, що використовується медичними організаціями.

Також розглянуто розробку моделі на прикладі абстрактного шпиталю і спосіб її імплементації в існуючий бізнес-процес, таким чином забезпечивши конфіденційність медичної інформації.

Напрямком подальших досліджень є доробка ролевої моделі до семантичної ролевої моделі керування доступом. Значна відмінність полягає у можливості автоматизації операцій призначення та відклику ролей.

Література

1. Tucker, D. Healthcare Goes Digital [Electronic resource] / Daniel Tucker. – Access mode: https://www.wnycstudios.org/story/243822-healthcare-goes-digital/. – 18.12.2012.

2. HIPAA Privacy Rules for the Protection of Health and Mental Health Information [Electronic resource] // U.S. Department of Health & Human Services. – Access mode: https://www.hhs.gov/hipaa/for-professionals/privacy/. – 11.10.2009.

3. Стрєлкіна, А. А. Забезпечення кібербезпеки медичних систем: виклики і рішення в контексті Інтернету речей [Текст] / А. А. Стрєлкіна, Д. Д. Узун // Радіоелектронні і комп'ютерні системи. – 2017. – № 1. – С. 44–50.

4. The HIPAA Privacy Rule [Electronic resource] // U.S. Department of Health & Human Services. – Access mode: https://www.hhs.gov/hipaa/for-professionals/privacy/. – 11.10.2009.

5. The HIPAA Security Rule [Electronic resource] // U.S. Department of Health & Human Services. – Access mode: https://www.hhs.gov/hipaa/for-professionals/security/. – 11.10.2009.

6. Право на медичну інформацію [Електронний ресурс] // Ваше здоров'я. – Режим доступу: https://www.vz.kiev.ua/pravo-na-medichnu-informaciyu/. – 14.07.2017.

Таблиця 1

Ролева модель керування даних

Привілей - Роль	Головний лікар	Лікар	Медична сестра	Центр обслуговування пацієнтів	Технічний спеціаліст
Керування налаштуваннями шпиталю	+				+
Керування запитами до державної бази даних	+	+		+	
Керування ролями та користувачами	+				+
Створення та перегляд запитів по лікарні	+			+	
Створення та перегляд даних пацієнта	+	+	+	+	
Створення та перегляд звітів	+				

7. Устінов, О. В. Електронна система охорони здоров'я відкрита для реєстрації лікарів і пацієнтів [Електронний ресурс] / О. В. Устінов // МОРІОН. – Режим доступу: https://www.umj.com.ua/article/114387/elektronna-sistema-ohoroni-zdorov-ya-vidkrita-dlya-reyestratsiyi-likariv-i-patsiyentiv. – 18.07.2017.

8. eHealth: що дасть українцям електронна система охорони здоров'я? [Електронний ресурс]. – Режим доступу: https:/uk.etcetera.media/ehealth-shho-dast-ukrayintsyam-elektronna-sistema-ohoroni-zdorov-ya.html. – 25.07.2017.

9. Яка нормативно-правова база лежить в основі роботи системи? [Електронний ресурс]. – Режим доступу: https://portal.ehealth.gov.ua/clarifications/2017-09-15-base/. – 05.04.2017.

10. К системе eHealth уже подключены около тысячи медучреждений [Електронний ресурс]. – Режим доступу: https://delo.ua/econonomyandpoliticsinukraine/k-sisteme-ehealth-uzhe-podkljucheny-okolo-1-tys-medicinskih-uchr-340771/. – 22.04.2018.

11. HIPAA Правила конфиденциальности в целях защиты информации о физическом и психическом здоровье пациентов [Електронний ресурс]. – Режим доступу: https://www.omh.ny.gov/omhweb/russian/hipaa/phi_protection.pdf. – 11.07.2009.

12. Семенова, Н. А. Семантическая ролевая модель управления доступом [Текст] / Н. А. Семенова // Прикладная дискретная математика. – 2016. – № 2(16). – С. 50–64.

13. Discretionary Access Control (DAC) [Electronic resource] // Techopedia. – Access mode: https://www.techopedia.com/definition/229/discretionary-access-control-dac/. – 10.12.2008.

14. Rouse, M. Mandatory access control (MAC) [Electronic resource] / M. Rouse. – Access mode: https://searchsecurity.techtarget.com/definition/mandatory-access-control-MAC. – 05.08.2008.

References

1. Tucker D., *Healthcare Goes Digital*. Available at: www.wnycstudios.org/story/243822-healthcare-goes-digital/ (accessed 18.12.2012).

2. U.S. Department of Health & Human Services, *HIPAA Privacy Rules for the Protection of Health and Mental Health Information.* Available at: https://www.hhs.gov/hipaa/for-professionals/privacy/ (accessed 11.10.2009).

3. Strielkina, A., Uzun, D. *Zabezpechennya kiberbezpeky medychnykh system: vyklyky i rishennya v konteksti Internetu rechey*. [Cybersecurity of medical systems: challenges and solutions in the context of the internet of things]. *Radioelektronni i komp'uterni sistemi - Radioelectronic and computer systems, 2017*, no. 1, pp. 44–50.

4. U.S. Department of Health & Human Services. *The HIPAA Privacy Rule*. Available at: https://www.hhs.gov/hipaa/for-professionals/privacy/ (accessed 11.10.2009)

5. U.S. Department of Health & Human Services. *The HIPAA Security Rule.* Available at: http://www.hhs.gov/hipaa/for-professionals/security/ (accessed 11.10.2009).

6. *Pravo na medychnu informatsiyu* [Right to healthcare information]. Available at: http://www.vz.kiev.ua/pravo-na-medichnu-informaciyu/ (accessed 14.07.2017).

7. Ustiniov, O. V. *Ukrayins'kyy medychnyy chasopys, Elektronna systema okhorony zdorov"ya* [Digital healthcare system]. Available at: https://www.umj.com.ua/article/114387/elektronna-sistema-ohoroni-zdorov-ya-vidkrita-dlya-reyestratsiyi-likariv-i-patsiyentiv (accessed 18.07.2017).

8. *eHealth: shcho dast' ukrayintsyam elektronna systema okhorony zdorov"ya* [eHealth: What will the Ukrainian health system provide to Ukrainians]? Available at: https://uk.etcetera.media/ehealth-shho-dast-ukrayintsyam-elektronna-sistema-ohoroni-zdorov-ya.html (accessed 25.07.2017)

9. *Yaka normatyvno-pravova baza lezhyt' v osnovi roboty systemy?* [What legal framework is the basis of the system?]. Available at: https://portal.ehealth.gov.ua/clarifications/2017-09-15-base/ (accessed 22.05.2018).

10. *Do systemy eHealth vzhe pidklyucheno blyz'ko tysyachi medustanov* [To the eHealth system already connected about a thousand medical institutions]. Available at: https://delo.ua/econonomyand politicsinukraine/k-sisteme-ehealth-uzhe-podkljucheny-okolo-1-tys-medicinskih-uchr-340771/ (accessed 22.04.2018).

11. U.S. Department of Health & Human Services, *HIPAA Privacy Rules for the Protection of Health and Mental Health Information.* Available at: https://www.omh.ny.gov/omhweb/russian/hipaa/phi_protection.pdf (accessed 11.07.2009).

12. Semenova, N. *Semantycheskaya rolevaya model' upravlenyya dostupom* [Semantic Role-Based Access Control Model]. *Applied Discrete Mathematics*, 2016, no. 2(16), pp. 50-64.

13. Techopedia, *Discretionary Access Control (DAC).* Available at: https://www.techopedia.com/definition/229/discretionary-access-control-dac (accessed 10.12.2008).

14. Rouse, M. *Mandatory access control (MAC).* Available at: https://searchsecurity.techtarget.com/definition/mandatory-access-control-MAC (accessed 05.08.2008).

Надійшла до редакції 24.04.2018, розглянута на редколегії 16.05.2018

РАЗРАБОТКА МОДЕЛИ УПРАВЛЕНИЯ ДОСТУПОМ К ПРИВАТНОЙ МЕДИЦИНСКОЙ ИНФОРМАЦИИ

А. С. Андрийчук, А. А. Стрелкина

Современная медицина выросла на непреодолимый уровень за последние десятилетия. Сегодня данный сектор человеческой жизни является высокотехнологичной отраслью, где успешно развиваются все сферы, которые могут спасти жизнь ранее безнадежных пациентов. Значительно усовершенствовано техническое оснащение учреждений здравоохранения, стало возможным диагностировать заболевания на ранних стадиях и быстро восстановить работоспособность пациентов. Тем не менее, со всеми преимуществами и возможностями современных технологий в данной сфере, возникает много проблем. Одной из самых значительных является обеспечение приватности медицинской информации, которая должна рассматривать с двух сторон как технической, так и регламентирующей. Обеспечение приватности данных в медицинских системах зависит от правильной и своевременной организации управления доступом к медицинской информации. Наиболее распространенным и всеобъемлющим регламентирующим документом для обеспечения безопасности медицинских данных является акт США Health Insurance Portability and Accountability Act (HIPAA). Относительно украинских нормативных документов, то они реализуют права пациента на получение информации о состоянии своего здоровья, а медицинские системы не имеют сертификат о соответствии комплексной системы защиты информации в соответствии требованиям нормативных документов по технической защите информации. В данной статье авторами рассматривается проектирования модели управления доступом, которая решает проблему обеспечения информационной безопасности медицинских систем и базируется на управлении доступом на основе ролей с минимальными ограничениями. Разрабатываемая модель должна определять действия и ресурсы, которые доступны пользователю, а также предоставлять индивидуальный доступ к ресурсам. Авторами было проведено исследование существующих моделей управления доступом, выявлены преимущества и недостатки, анализ которых лег в основу разработки собственной модели. В работе описывается создание политики безопасности на основе ролей, которая определяет разрешенные в системе потоки информации, опираясь на международный регламентирующий документ HIPAA. С помощью разработанной модели, можно по-разному выполнить ее хранения и в любом случае очень просто перевести в реляционную базу данных.

Ключевые слова: приватная медицинская информация, модель доступа, модель политики безопасности, HIPAA, RBAC.

DEVELOPMENT OF ACCESS CONTROL MODEL TO PRIVATE MEDICAL INFORMATION

A. S. Andriichuk, A. A. Strielkina

Modern medicine has grown to an insurmountable level over the past decades. Today, this sector of human life is a high-tech industry, where all areas that can save lives of previously hopeless patients are successfully developing. The technical equipment of health care facilities has been substantially improved, it has become possible to diagnose diseases at an early stage and to quickly restore the working capacity of patients. Nevertheless, with all the advantages and capabilities of modern technology in this area, there are many problems. One of the most significant is the provision of privacy of medical information, which should be considered from both sides, both technical and regulatory. Ensuring the confidentiality of data in medical systems depends on the correct and timely organization of managing access to medical information. The US Health Insurance Portability and Accountability Act (HIPAA) is the most widespread and comprehensive regulatory document for the security of medical data. Regarding the Ukrainian normative documents, they realize the rights of the patient to receive information about their state of health, and medical systems do not have a certificate on the compliance of a comprehensive system of protection of information in accordance with the requirements of normative documents on the technical protection of information. In this article, the authors are considering designing an access control model that solves the problem of providing information security for medical systems and is based on access control based on roles with minimal constraints. The model to be developed should determine the actions and resources that are available to the user, as well as provide individual access to resources. The authors examined the existing models of access control, identified the advantages and disadvantages that formed the basis of their own model. The paper describes the creation of a role-based security policy that defines the information flows permitted by the system, based on the international regulatory document HIPAA. With the help of the developed model, it is possible to execute its storage in different ways and in any case, it is very easy to convert into a relational database.

Keywords: private medical information, access model, security policy model, HIPAA, RBAC.

Андрійчук Андрій Сергійович – студент кафедри комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», Харків, Україна, e-mail: a.andriychuk@student.csn.khai.edu

Стрєлкіна Анастасія Андріївна – асистент, аспірант комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків, Україна, e-mail: a.strielkina@csn.khai.edu.

Andriichuk Andrii– student of Computer Systems, Networks and Cybersecurity department, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine, e-mail: andriychuk@student.csn.khai.edu

Strielkina Anastasiia – assistant lecturer, PhD student of Computer Systems, Networks and Cybersecurity department, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine, e-mail: a.strielkina@csn.khai.edu.