Інтелектуальний веб-інтерфейс доступу до даних особливої важливості

Владислав Костянтинович Гуменок, Ігор Анатолійович Котов[0000-0003-2445-6259]

Криворізький національний університет,
вул. Віталія Матусевича, 11, м. Кривий Ріг, 50027, Україна
{gumenok.vladislav, rioexito}@gmail.com

Анотація. Мета роботи – розробка і дослідження інтелектуального веб-інтерфейсу доступу до даних особливої важливості. Об'єкт проектування – інтелектуальна інформаційна технологія доступу до даних особливої важливості. У теоретичній частині проведено аналіз проблем забезпечення безпеки конфіденційних даних, розглянуті існуючі способи захисту інформації, визначено актуальність та завдання дослідження. У практичній частині роботи проведено аналіз принципів побудови систем захисту інформації, розроблено структурні та функціональні моделі, розроблено інтелектуальний блок доступу до даних особливої важливості. Досліджено рівень надійності та стійкості питань системи до набору даних, зроблені висновки, що розроблений веб-інтерфейс дозволяє підвищити рівень захищеності інформації.

Ключові слова: безпека, база даних, інтерфейс, інтелектуальний, загрози, забезпечення захисту, функціональна схема, інформаційна система, автентифікація.

Intelligent web-interface for access to data of particular importance

Vladyslav K. Humenok, Igor A. Kotov[0000-0003-2445-6259]

Kryvyi Rih National University, 11, Vitalii Matusevych St., Kryvyi Rih, 50027, Ukraine
{gumenok.vladislav, rioexito}@gmail.com

Abstract. The purpose of the work is to develop and research the intellectual web-interface of access to data of particular importance. Design object – intelligence information technology access to data of particular importance. In the theoretical part the analysis of security problems of confidential data was carried out, existing methods of information protection were considered, the relevance and objectives of the research were determined. In the practical part of

the work, an analysis of the principles of construction of information security systems has been developed, structural and functional and structural models are developed, the intellectual access block of data of special importance has been developed. The level of reliability and stability of the system issues prior to the data selection is investigated, the conclusions are drawn that the developed web-interface allows to increase the level of information security.

Keywords: security, database, interface, intelligence, threats, security, functional diagram, information system, authentication.

1 Вступ

Забезпечення безпеки даних – одна з головних вимог в умовах сучасного глобалізованого світу. Серед джерел загроз безпеки інформації розрізняють стихійні – викликані впливом на інформаційне середовище об'єктивних фізичних процесів або природних явищ, технічні – зумовлені зношенням апаратних засобів, що зберігають інформацію та антропогенні, коли загроза безпеки даних походить від самої людини. В межах державних організацій різного рівня міститься інформація, що відноситься до категорії особливої важливості. Такі дані мають найвищій ступінь секретності та присвоюються суворо обмеженій групі документів. Розкриття інформації з таким грифом секретності несе в собі надзвичайну небезпеку для країни і може нанести значний збиток інтересам держави, оскільки містить інформацію, що стосується оборонної, економічної та контррозвідувальної сфер діяльності.

Найбільш розповсюдженою причиною витоку секретної інформації є саме антропогенний фактор. Його проявами можуть бути як ненавмисні дії працівників організації через необережне поводження з інформацією, так і цілеспрямовані дії з боку зловмисників, метою яких є викрадення важливих даних.

Забезпечення і підтримка інформаційної безпеки передбачає комплекс різнопланових заходів, які запобігають, відстежують та усувають можливість несанкціонованого доступу до даних. Подібні заходи включають в себе апаратні та програмні засоби захисту. Ці засоби дозволяють забезпечити механізми автентифікації, які на підставі наданих користувачем предметів автентифікації або його біометричних параметрів приймають рішення про те, чи є користувач тим, за кого себе видає.

Автентифікація є складовою частиною систем захисту інформації (СЗІ), діяльність яких спрямована на захист від несанкціонованого доступу, пошкодження, або спотворення інформації та гарантування дотримання ключових принципів захисту інформації, які полягають у забезпеченні конфіденційності, цілісності та доступності даних.

2 Мета і задачі дослідження

Метою роботи є дослідження засобів захисту інформації на основі існуючих аналогів, та розробка інтелектуального веб-інтерфейсу доступу до даних особливої важливості.

З метою досягнення поставленої мети дослідження виникає необхідність постановки та виконання наступних задач:

- розробка загальної структури інформаційної системи;
- побудова функціональної моделі інформаційної системи;
- розробка взаємодій компонентів інформаційної системи;
- розробка структури бази даних інформаційної системи.

Об'єктом дослідження є інтелектуальна інформаційна технологія забезпечення доступу до даних особливої важливості.

Предметом дослідження є комплекс організаційних заходів і програмно-технічних засобів забезпечення безпеки інформації.

Методи дослідження. У процесі дослідження застосовувалися такі наукові методи: порівняльний метод, емпіричний метод, пояснення і узагальнення. Методи аналізу та оцінки дозволили розробити програмні модулі інформаційної системи та її бази даних.

Практичне значення одержаних результатів дослідження полягає у тому, що теоретичні і методичні положення, висновки і рекомендації доведені до рівня практичних розробок, які сприяють впровадженню інноваційної продукції, ефективної системи доступу до конфіденційних даних, що дасть можливість підвищити рівень захищеності інформації та дозволить визначити ключові напрямки для подальшого удосконалення.

3 Аналіз систем захисту інформації та постановка проблеми

Система захисту інформації – сукупність організаційних і інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу [1]. Захист інформації здійснюється на всіх етапах існування інформаційних систем шляхом об'єднання відповідно до прийнятої політики безпеки в єдину систему захисту правових, організаційних, інженерно-технічних та апаратно-програмних методів, способів та засобів захисту інформації [2]. Для забезпечення належного рівня захисту інформації державними органами передбачено ведення контролю за функціональним станом СЗІ. Заходи контролю передбачають процедури атестації та ліцензування об'єктів інформації для оцінки підготовленості систем і засобів інформатизації та зв'язку до обробки інформації, що містить державну таємницю.

Безпосередній процес функціонування СЗІ передбачає розподілення між користувачами необхідних реквізитів захисту інформації (паролів, привілеїв, ключів), надання користувачам прав доступу до ресурсів системи згідно з

прийнятою політикою безпеки та їх ліквідація по закінченню потреб у доступі. Загальна схема контролю захисту інформації в межах СЗІ представлена на рис. 1.

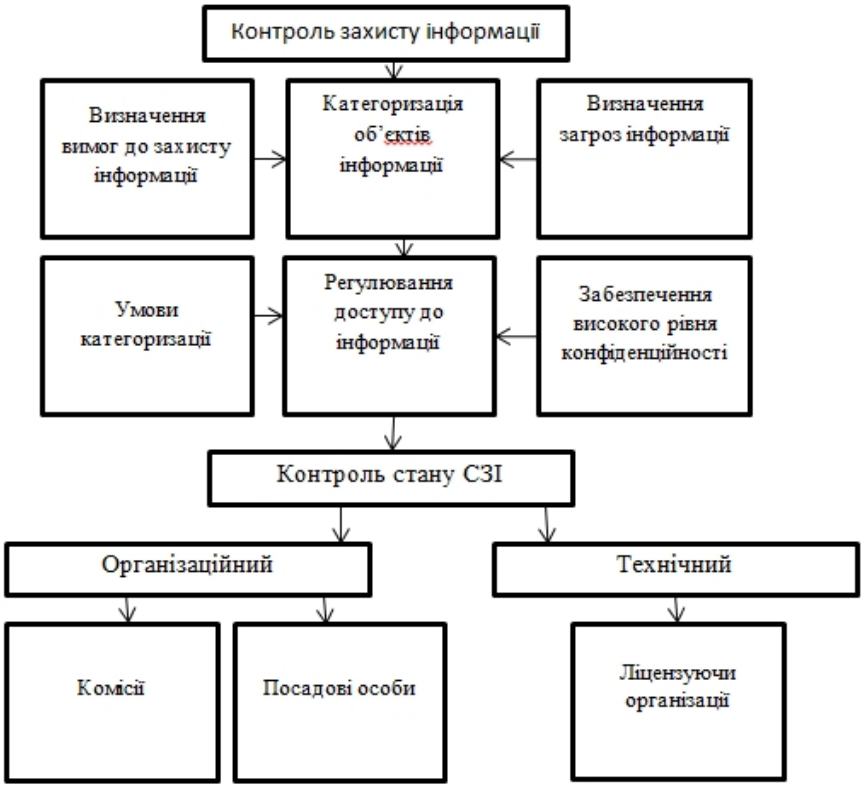

Рис. 1. Загальна схема контролю захисту інформації

Основна проблема, виявлена в процесі дослідження, полягає в тому, що забезпечення функціонування потребує використання значної кількості апаратно-технічних засобів. Це зумовлює необхідність залучення контролюючих органів та третіх осіб, що призводить до сповільнення процесу розробки та введення в експлуатацію системи захисту і підвищує ймовірність витоку конфіденційної інформації. Також виявлено, що у якості елементів автентифікації використовуються застарілі методи, такі як паролі або ключі доступу, що зберігаються на фізичних носіях та можуть бути втрачені.

4 Матеріали і методи досліджень

Система інтелектуального доступу до даних виконує ряд функцій, спрямованих на забезпечення безпеки інформації. Ключовими є автентифікація користувача та визначення його прав доступу.

Система автентифікації користувача включає в себе ряд питань, які містять особисту інформацію та забезпечують безпомилкове визначення користувача, під час отримання доступу.

Для визначення функціональних можливостей програмного продукту розробляється функціональна схема. Така схема дозволяє відобразити принципи роботи та визначити зв'язки між компонентами програми. На рис. 2 наведена функціональна схема додатку інтелектуального доступу до даних.

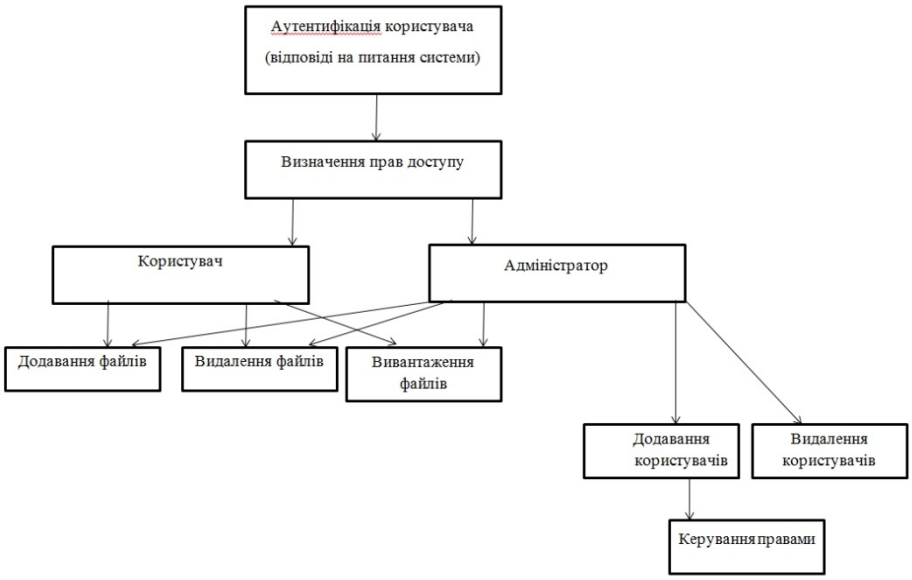

Рис. 2. Функціональна схема додатку

Функціональна схема містить інформацію про способи реалізації додатком заданих функцій. За такою схемою можна визначити, як здійснюються перетворення і які для цього необхідні функціональні елементи. Кожен функціональний елемент містить лише ті входи і виходи, які необхідні для його коректної роботи.

5 Результати

Оцінка програми інтелектуального доступу до даних особливої важливості буде здійснюватися за наступними критеріями:

- оцінка веб-інтерфейсу додатку;
- визначення характеристик додатку;
- оцінка захисту додатку;
- оцінка ефективності додатку в цілому.

При потраплянні на сторінку входу до системи користувача зустрічає форма вводу даних (рис. 3).

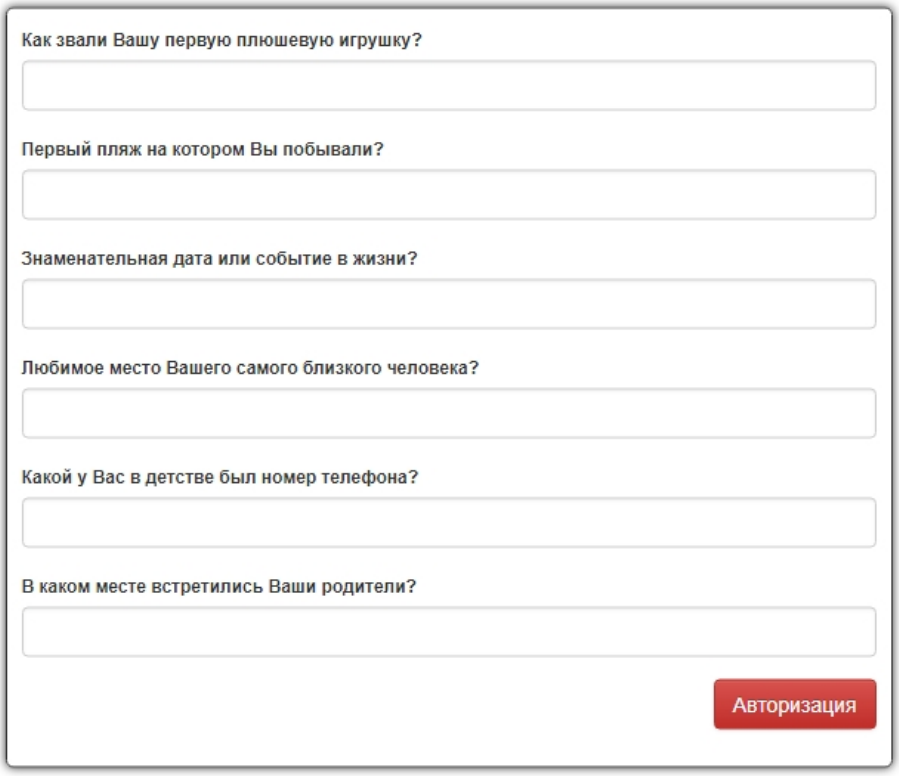

Рис. 3. Вікно входу до програми

Форма містить перелік питань, які передбачають введення особистої інформації. Після почергової відповіді на них користувач натискає кнопку авторизації. Інтелектуальний модуль доступу до інформації порівнює отриману інформацію з даними, що містяться в БД та визначає відсоткове відношення коректних відповідей. У разі, якщо даний відсоток досягає певного значення система визначає можливість отримання доступу до інформації та визначає права користувача на використання її ресурсів.

У цілому програма виконує свої функції, що полягають у забезпеченні інтелектуального доступу до інформації. Вона дозволяє здійснювати додавання та видалення інформації у разі необхідності й убезпечує інформацію від несанкціонованих дій з боку інших користувачів. Розроблений веб-ресурс забезпечує створення єдиної системи доступу до даних особливої важливості.

6 Висновки

У роботі досягнута основна мета, яка полягає у дослідженні теоретико-методичних та наукових підходів до забезпечення безпеки даних особливої важливості та на основі досліджень сучасних програмних аналогів розроблено веб-інтерфейс, що здатний надати можливість безпечного доступу до важливої інформації. На підставі цього можна зробити наступні висновки:

- розроблено загальну структури інформаційної системи;
- побудована функціональна моделі інформаційної системи;
- розроблено взаємодію компонентів інформаційної системи;
- розроблена структура бази даних інформаційної системи.

У результаті проведеного дослідження щодо формування ціни на інформаційну систему виявлено, що кінцева ціна продукту значно менше від ціни існуючих аналогів, а рентабельність її виготовлення становить 12,3 %. Таким чином, розробка та впровадження інтелектуального веб-інтерфейсу доступу до даних особливої важливості є економічно доцільними.

Список використаних джерел

1. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [Електронний ресурс] : Постанова № 373 / Кабінет Міністрів. – Київ, 29 березня 2006 р. – Режим доступу : http://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF.
2. Про інформацію [Електронний ресурс] : Закон України. – 02 жовтня 1992 р. – Режим доступу : http://zakon.rada.gov.ua/laws/main/2657-12.

References (translated and transliterated)

1. Pro zatverdzhennia Pravyl zabezpechennia zakhystu informatsii v informatsiinykh, telekomunikatsiinykh ta informatsiino-telekomunikatsiinykh systemakh (On Approval of the Rules for the protection of information in information, telecommunication and information and telecommunication systems). http://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF (2006). Accessed 13 Sep 2018
2. Zakon Ukrainy Pro informatsiiu (Law of Ukraine On information). http://zakon.rada.gov.ua/laws/main/2657-12 (1992). Accessed 13 Sep 2018