УДК 004.021

Т. М. Хомета, УАД, м. Львів

ЗАДАЧІ ЗАХИСТУ СОЦІАЛЬНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Анотація. В статті розглянуто інформаційні соціальні системи, кожна з яких вимагає засобів захисту, а також орієнтовані на певний клас задач їх захисту, тому з кожного класу задач і вибирається інформаційна соціальна система.

Annotation The informative frames of society are considered in the article, each of which requires facilities of defence, and also oriented to the certain class of tasks of their defence, that is why from every class of tasks gets out the informative frame of society.

Аннотация: В статье рассмотрены информационные социальные системы, каждая из которых требует средств защиты, а также ориентированные на определенный класс задач их защиты, поэтому из каждого класса задач и выбирается информационная социальная система.

Ключові слова: ідентифікатор користувача, ідентифікація, аутентифікація, елімінація, транзакція.

Keywords: identifier of user, identification, authentification, elimination, transactions.

Ключевые слова: идентификатор потребителя, идентификация, аутентификация, элиминация, транзакция.

Вступ

До соціальних систем відносяться всі соціальні системи, які пов’язані з соціальними структурами, або соціальним середовищем зобов’язаннями по реєстрації осіб, майнових прав та інших факторів, що визначають різного типу правові умови визначення офіціального статусу, а також зобов’язання по наданню громадянам послуг, які передбачені відповідними юридичними нормами, системи, що реєструють офіціальні взаємовідносини між громадянами та між громадянами і державними органами.

На сьогоднішній день існує цілий ряд задач, використання яких може виявитися необхідним в найближчому майбутньому. До таких задач приводить поява та використання електронних грошових засобів, як універсальних засобів, що приймають участь в процесах торгівлі. Наступною задачею, яка буде розв’язуватися та розвиватися, є задача електронних виборів, специфіка якої полягає у тому, що засоби захисту повинні забезпечувати цілий ряд параметрів, що характеризують правові вимоги, що в сукупності визначають безпеку системи виборів.

Виклад основного матеріалу

Найбільш простими системами, з точки зору вимог до засобів захисту та системи захисту в цілому, є системи, що надають послуги громадянам держави, наприклад, надання реєстраційних документів різних типів по запиту громадян. До основних задач захисту, що виникають в цьому випадку можна віднести наступні:

- задачі захисту баз даних, що вміщують предмет, або об'єкт реєстрації;
- задачі захисту доступу до системи реєстрації, представників державних органів та клієнтів.

Задачі захисту баз даних, що вміщають інформацію про предмети, або об'єкти реєстрації, розв'язуються відомими методами, які безпосереднього відношення до клієнтів, які звертаються за послугами до організацій1, не мають.[1].

В основному задачі захисту, що характеризуються відповідними особливостями стосуються проблем захисту доступу, які можна сформулювати наступним чином:

- задача захисту доступу до автоматизованої системи видачі документів, або до автоматизованої системи, в якій зі сторони державного органу приймає участь державний службовець;
- задача ідентифікації службовця та ідентифікації клієнтів;
- задачі захисту розподілених систем доступу.

Задача доступу до системи, для випадку, коли зі сторони системи, в її роботі не приймає участь працівник, досить широко досліджена і відомі різні підходи до її розв'язку [2,3] Найбільш простий розв'язок задачі захисту доступу полягає у використанні ідентифікатора користувача та персонального паролю. В цьому випадку, довільний користувач, перш ніж зможе користуватися відповідною послугою повинен зареєструватися в системі, завдяки чому користувач може отримати відповідні атрибути. Такий спосіб захисту може використовуватися у тому випадку, коли користувач передбачає порівняно регулярно користуватися послугами відповідної установи. Прикладом такої ситуації можуть служити медичні установи. В цьому випадку користувач може реєструватися, при цьому може використовуватися третя сторона, яка користується у потенціальних користувачів довірою. Такі підходи досить поширені і глибоко досліджені.

У випадку, коли користувач планує скористатися доступом разово або користуватися рідко, то виникає задача ідентифікації разового користувача. Така ситуація є характерною для соціальних середовищ і відрізняється від попереднього випадку наступним. Однією з особливостей соціальних середовищ є відсутність певної підготовки потенціальних користувачів для того, щоб інформаційні системи, в тому вигляді, в якому прийнято їх експлуатувати, могли повноцінно ними користуватися без допомоги третіх осіб, чи третіх учасників процесу надання послуг. Наступна особливість полягає у впровадженні в середовище потенціальних користувачів сучасних

електронних засобів типу смартфонів, планшетів володіють функціями, що дають змогу користуватися останнім, як віддаленим засобом доступу. В цьому випадку, виникають наступні проблеми:

- створення пункту доступу до мережі Internet, які були б доступні для всіх потенціальних користувачів;
- створення засобів захисту різного рівня для даних, які отримує користувач в залежності від характеру цих даних та особливостей користувача;
- реалізація можливостей використання відповідної послуги користувачем з наступною елімінацією відповідного сервісу з смартфону, планшета користувача, який отримав відповідну послугу.

В рамках цих задач виникає необхідність забезпечувати наступні можливості для користувача:

- користування відповідним додатком, для отримання послуги, було доступним для не підготовленої особи;
- необхідно реалізувати можливість завантаження відповідного додатку на основі використання заданого телефонного номеру служби, що надає відповідну послугу, а також видалення відповідного додатку;
- розробити протоколи тимчасового захисту каналу зв'язку та тимчасової ідентифікації відповідного користувача даної послуги.

Очевидно, що всі ці можливості не повинні перевищувати по своїй вартості, існуючої ціни отримання послуги.

Такий підхід до розвитку систем надання електронних послуг населенню, обумовлює необхідність розв'язування цілого ряду задач, які виникають внаслідок реалізації надання послуги в електронному вигляді користувачам. Одно з таких розширень асортименту додаткових задач є наступна задача. Зрозуміло, що будь який користувач, або громадянин, потребує певну послугу від державної установи, фізичним проявом якої є той чи інший документ, який клієнт буде використовувати для розв'язку інших задач у інших державних, або приватних інституціях. Оскільки такий документ користувач отримує для того, щоб його використати при співпраці з іншою організацією, то така інша організація повинна технічно бути готова до сприйняття електронного документу від користувача. Зрозуміло, що впровадити таку систему електронних документів одночасно у всіх організаціях є неможливо. Тому, виникає задача надання можливості користувачу, у випадку необхідності дублювати отриманий документ у формі, яка є доступною можливим організаціям, які планують використовувати відповідний документ користувача. Використання електронних форм документів має сенс лише у випадку, коли забезпечується дистанційна комунікація між користувачем та організацією. У випадку необхідності використання документу на тому, чи іншому носії, паперовий носій, в даному випадку розглядати не будемо, то організація, яка не є готова до використання електронних документів користувача, може в значній мірі дискредитувати

електронну систему документів в цілому. Використання електронних документів є допустимим лише в тому випадку, коли передбачається перехід відповідних установ на використання електронних документів.

В електронних системах, серед споріднених державних, чи інших організацій, використовуються механізми виключення окремого споживача з циклу обміну необхідними документами, оскільки такий обмін фактично, потрібний відповідним організаціям. В цьому випадку, користувач, який звертається у відповідну організацію за послугою, не мусить збирати з різних установ різні документи для установи, в яку звернувся користувач. Така установа в межах окремих мереж, в які входять споріднені установи, не залежно від користувача, отримують всі дані, які ця установа потребує з інших установ, через канали електронного зв'язку, без участі користувача. В рамках такого підходу існує досить суттєвий недолік, який полягає у тому, що користувач повністю стає залежним від регіональних інформаційних систем. Тому, у будь якому випадку, в рамках системи, існує можливість формування документів на носіях паперових, або пластикових, які не потребують для початкової, або базової ідентифікації ніяких додаткових технічних засобів.

Окремим класом інформаційних систем, що орієнтовані на обслуговування громадян є системи, що пов'язані з обслуговування фінансових операцій. В цьому випадку, основною стороною, що надає послуги являється система банків. Особливістю цієї системи є те, що переважна кількість банків є структурами приватними. Це приводить до того, що банки повинні самі заробляти на забезпечення власних процесів функціонування.

Параметром заробітку, в цьому випадку, є вартість різних фінансових послуг. В багатьох випадках якість таких послуг може бути різного рівня. Вартість таких послуг не регламентується в достатньо точній мірі державними органами, що дозволяє банкам отримувати прибутки, використовуючи не завжди обґрунтовані ціни надання відповідних послуг. Іншою важливою характеристикою банківських послуг є забезпечення їх безпеки для клієнта, оскільки, будь які банківські послуги пов'язані з коштами клієнта. Характерним для банківської системи є не прозорість гарантованих банком параметрів, що характеризують безпеку для коштів клієнта. Банківський сектор, судячи з даних масової інформації, не забезпечує бажаного рівня безпеки використання послуг банків клієнтами. Крім того, цей сектор є досить специфічним, що обумовлюється його статусом комерційної структури, тому більш детально проблеми безпеки в цьому секторі розглядати не будемо, оскільки в силу об'єктивних причин, дані про стан та методи забезпечення безпеки послуг користувачів є не доступні. Між установами, в першу чергу, державними та громадянами існують взаємозв'язки, що пов'язані з коштами, які громадяни передають державі. Це стосується в першу чергу податкових зобов'язань перед державою зі сторони громадян. Хоча, для транзакцій самих коштів

використовується система банків, відповідні організації в більшості випадків, не підтверджують по відношенню до громадян, факту виконання останніми своїх зобов'язань. Така ситуація приводить до того, що громадяни вимушені самі проводити контроль та перевірки процесів платежів та інших процесів, що пов'язані з їх взаємодією з відповідними організаціями. У випадку використання автоматизованих інформаційних систем, відповідні підтвердження громадянам про те, що вони виконали свої зобов'язання повинні надходити до останніх в автоматичному режимі. В цих випадках, важливою є задача захисту процесів взаємодії громадян з відповідними організаціями, або державними структурами. В якості підтвердження наявності такого захисту можна використовувати обернені зв'язки між відповідною структурою і користувачем.

Важливою галуззю використання інформаційних систем в рамках інтересів громадян, є створення та використання Internet магазинів. Такий спосіб проведення операцій досить поширений, оскільки він має ряд явно виражених переваг. Найбільш важливою перевагою є можливість здійснювати придбання товарів без відвідування магазинів чи інших торгових об'єктів. Оскільки, в таких системах використовуються грошові кошти, то система захисту продавців і в першу чергу покупців є досить актуальною. Для вирішення цієї проблеми необхідно розв'язувати задачі захисту транзакцій, що пов'язані з оплатою, задачі ідентифікації покупців і продавців та розв'язування інших задач захисту, що виникають, при реалізації цих процесів. Задачі захисту транзакцій грошових коштів, в цьому випадку можуть перекладатися на банківську систему, якщо покупець має банківський рахунок. [4]. Можна прийняти, що у певної кількості покупців такі рахунки є. У випадку коли покупець таких рахунків не має, то Internet магазин повинен вирішувати задачу захисту покупців, або співпрацювати тільки з такими клієнтами, які мають відповідні рахунки. На сьогоднішній день досить поширеними є ситуації, коли покупці не мають банкових рахунків. В цьому випадку система Internet магазину повинна забезпечувати можливість безпечної реалізації процесів отримання коштів у покупця та процесу передачі йому відповідних товарів. Якщо забезпечити безпеку покупця порівняно легко за рахунок використання системи торгових агентів, то забезпечити безпеку функціонування Internet магазину від спроб заволодіти товарами по фальсифікованих платіжних картах, є досить складно. Для вирішення цієї проблеми необхідно розв'язувати задачу ідентифікації власника карти і, відповідно, самої карти, яка повинна розв'язуватися на кількох рівнях ідентифікації та аутентифікації. У випадку Internet магазинів ця задача ускладнюється тим, що у останнього не має бази покупців з тими чи іншими даними. В окремих випадках, для вирішення цієї задачі різні торгові мережі вводять преміальні картки покупців та інші способи оцінити базову кількість покупців та зацікавити останніх в користуванні з їх послуг. Захист самих Internet магазинів розглядати не будемо, бо цей аспект можна відокремити від аспекту захисту покупців.

Захист покупців в системі електронної торгівлі має іще один аспект, який полягає у наступному. Кожна система Internet магазинів проводить свою рекламно-торгівельну політику. В рамках цієї політики окремі Internet магазини можуть використовувати шкідливі для покупця методики рекламування своїх товарів, чи послуг. Шкідливість виникає в тих випадках, коли реалізація процесу рекламування використовує різні методи та засоби, що можуть впливати на покупця на рівні підсвідомості. Це особливо характерно для тих груп покупців, які користуються комп'ютерною технікою та користуються можливостями комп'ютерних мереж. Таке зловживання зі сторони системи Internet магазинів може полягати у наступному:

- використання персонально орієнтованої реклами;
- використання рекомендацій стосовно товарів, які пропонується покупцю придбати;
- пропозиції складних механізмів отримання знижок на окремі товари та інші методи впливу на покупців.

Використання персонально орієнтованої реклами є досить поширеним. Персоналізація реалізується з точністю до віку потенціальних покупців. Наприклад, реклама може бути орієнтована на дітей, на осіб пенсійного віку і т. д. На сьогоднішній день, засоби захисту населення від реклами, що передається по електронних мережах Internet є досить слабо розвинутими. Ця ситуація має місце з наступних причин:

- мало проектується продуктів захисту від рекламної інформації, оскільки такі продукти досить слабо продаються;
- державні організації не проводять діяльність по захисту населення від шкідливої рекламної діяльності;
- високі доходи від продаж, що збільшуються завдяки вдалої, з точки зору працівників, реклами.

Захист покупців від упередженої реклами представляє собою окрему проблему, тому, детально проводити аналіз методів захисту від неї споживачів не будемо [5].

Наступний тип соціальної інформаційної системи є система, що обслуговує медичну галузь. Така система, на відміну від інших систем повинна об'єднувати всі регіони держави, на які поширюються правила медичного обслуговування. Основними функціями такої системи є наступні:

- інформування про наявність у пацієнта медичної страховки, не залежно від місця, де пацієнт потребує медичної допомоги, очевидно, що мова йде про територіальне розміщення пацієнта;
- інформація лікарів, про стан здоров'я пацієнта у випадку, коли пацієнт попадає до іншого лікаря;
- активізація діалогу з фахівцем, коли необхідна додаткова інформація стосовно пацієнта і т. д.

Очевидно, що така система не може бути створена в повній версії

одночасно. Вона формується по етапах, наприклад, на початку така система дозволяє отримати дані про наявність медичної страховки, що дозволяє надавати пацієнтам медичну допомогу в повному об'ємі. Проблема захисту пацієнта, в цьому випадку, полягає в тому, щоб треті особи не могли не санкціоновано скористатися відповідною страховкою замість власника цієї страховки. В даному випадку, захист пацієнта ґрунтується на ідентифікації справжнього пацієнта, яка здійснюється на основі документа ідентифікаційного, яким є паспорт.

Інформаційні системи медичного характеру, які формуються в рамках держави орієнтовані на розв'язування цілого ряду задач, прикладами яких можуть бути наступні:

- проведення Internet консиліумів;
- виявлення даних про наявність тих, чи інших засобів, що необхідні для лікування;
- проведення в режимі on – line за участю фахівців, операцій, які є невідкладними та інші.

До важливих соціальних систем відносяться системи, що забезпечують реалізацію процесів різних соціальних виплат. Необхідність в такій системі обумовлюється наступними факторами, або особливостями:

- у такої системи існує досить багато користувачів;
- користувачі, такої системи, у порівнянні з іншими, досить часто змінюються у зв'язку з закінченням обслуговувань та початком обслуговувань;
- типи соціальних платежів досить різноманітні і таких платежів досить велика кількість;
- в переважній більшості випадків, коштів на реалізацію платежів є досить мало;
- основною небезпекою, для користувача, в даному випадку, є несанкціонований доступ до системи особи, яка не має уповноважень на отримання соціальної виплати.

Як виникає з приведеного вище, в основі захисту споживача, лежить захист доступу до системи. Якщо прийняти до уваги, що значна кількість споживачів, є не достатньо підготовлена до користування такою системою, то проблема захисту споживачів суттєво ускладнюється.

До важливих соціальних інформаційних систем відносяться системи дистанційного навчання. Необхідність в таких системах обумовлюється наступними факторами:

- досить часто виникає необхідність в процесі роботи, вивчати додатково деякий предмет;
- наявність людей з обмеженими фізичними можливостями обумовлює необхідність створення умов для підготовки їх до виконання певних робіт, яка передбачає навчання в рамках стандартного курсу;

- необхідність мати документальне підтвердження наявності деякої кваліфікації.

В першому випадку основною ціллю дистанційного навчання є отримання знань, що необхідні для виконання деякої роботи. Якщо така потреба виникла у дипломованого працівника, то, в такому випадку, від системи дистанційного навчання потрібна можливість такої організації навчання, при якій ефективність навчання була би максимальна. Основними компонентами довільного учбового процесу є надання теоретичної інформації для процесу навчання та організація практичного навчання. Переважно, такі послуги надає той або інший учбовий заклад, по профілю якого користувач хоче розширяти свої знання. Особливістю учбового процесу, є здатність цього процесу, крім теоретичних даних, надавати користувачу ряд практичних навиків використання відповідних теоретичних даних. В рамках учбового процесу, включаючи учбовий процес дистанційного навчання, важливою особливістю є можливість надання студенту інтерпретаційних розширень стосовно матеріалу, який представляється. Другою особливістю є можливість забезпечити ефективність отримання практичних навиків відповідних до розв'язку задач. При традиційних методах навчання така можливість забезпечується проведенням практичних занять. Очевидно, щоб забезпечити виконання всіх приведених особливостей, не достатньо відтворювати процеси навчання в дистанційному режимі аналогічно тому процесу, який реалізовується в класичному режимі. В дистанційному режимі методика навчання повинна реалізовувати всі психологічні ефекти, які присутні в методиці традиційного навчання. До таких психологічних ефектів належать наступні форми та особливості навчального процесу:

- необхідність освоювати матеріал, що подається поступово в певному часовому ритмі;
- необхідність виконувати завдання, що дозволяють отримати практичні навики незалежно від можливих фактів, що можуть обумовити зміну певного ритму навчання;
- пристосувати ту чи іншу швидкість процесу навчання до особливостей окремої особи і т. д.

Приведені вище фактори демонструють складність організації дистанційного навчання, якщо воно не реалізується у вигляді формального копіювання процесу традиційного навчання. Проблеми захисту, в даному випадку, мають наступні аспекти:

- захист доступу користувача, до системи навчання, щоб можна було запобігти несанкціонованого використання процесу навчання іншою особою;
- захист авторських прав на методику навчання, яку формує автор відповідного курсу, або предмету;

- ідентифікація особи, що проходила навчання з ціллю того, щоб на етапі підтвердження отриманих знань в процесі навчання не існувало можливості підміни особи, що навчалася, іншою особою, яка уже має відповідні знання, які отримала окремо від даного процесу.

Захист доступу користувача до дистанційної системи навчання забезпечує можливість отримати відповідну послугу особі, яка оплатила відповідну послугу. Захист авторських прав забезпечує не можливість використання розробленої методики навчання, користувачем з ціллю перепродажі відповідної послуги. Крім того такий захист реалізується по відношенню до потенціальних несанкціонованих осіб, які хотіли б відповідну послугу продавати від свого імені. Останній випадок захисту є досить важливим, оскільки, у випадку його відсутності, може дійти до дискредитації всієї системи дистанційного навчання. Справа у тому, що наявність певних знань прийнято підтверджувати відповідними документами. У випадку, коли особа, яка виявила бажання отримати певні знання не змогла, в силу різних причин, скористатися з даної послуги, а інші обставини, наприклад, продовження терміну навчання, чи кошти, що необхідні для додаткового доповнення передбачуваного курсу, не дозволили особі такі знання отримати, то не допустимою є ситуація, коли здійснюється спроба фальсифікувати процес перевірки знань, шляхом залучення до такої перевірки другої особи, яка необхідними знаннями володіє.

Висновки.

В статті розглянуто цілий ряд окремих інформаційних систем, кожна з яких орієнтована на певний клас задач. Тому з кожного класу задач вибрано інформаційну соціальну систему (*ICS*), оскільки кожна з них вимагає засобів захисту, що є типовим для цілого класу. На прикладі такої системи проведено аналіз задач захисту та аналіз основних способів розв'язку цих задач.

1. *Соколов А. В.* Защита информации в корпоративных сетях / А. В. Соколов, В. Ф. Шаньгин. — М. : ДМК Пресс, 2002.
2. *Сталлинг В.* Основы защиты сетей. Приложения и стандарты / В. Сталлинг. — М. : Издательский дом «Вильямс», 2002.
3. *Чмора А. Л.* Современная прикладная криптографія / А. Л. Чмора. — М. : Гелиос АРВ, 2002.
4. *Молдавян Н. А.* Криптография: от примитивов к синтезу алгоритмов / Н. А. Молдавян, А. А. Молдавян, М. А. Еремеев. — СПб. : БХВ Петербург, 2004.
5. *Петров А. А.* Компьютерная безопасность / А. А. Петров. Криптографические методы защиты. — М. : ДМК, 2000.
6. *Бабаш А. В.* Криптография / А. В. Бабаш, Г. П. Шанкин. — М. : СОЛОН-Р, 2002.

Поступила 26.10.2015р.