УДК 004.056.55
Підкова Ю. І.
Тернопільський національний економічний університет

МЕТОДИ ТА ЗАСОБИ ДОСЛІДЖЕННЯ НАДІЙНОСТІ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПРИ ЗДІЙСНЕННІ ІНТЕРНЕТ-ТРАНЗАКЦІЙ

Підкова Ю. І. Методи та засоби дослідження надійності та захисту персональних даних при здійсненні інтернет-транзакцій. У роботі розглянуто застосування методів та засобів дослідження надійності та захисту персональних даних при здійсненні Інтернет-транзакцій, а також запропоновано застосування методів та засобів дослідження надійності та захисту персональних даних при здійсненні Інтернет-транзакцій, до яких віднесено моніторинг, виявлення і реагування на інциденти. Показано, що при об'єднанні моніторингу, виявлення і реагування на інциденти в єдину систему, це дозволить досліджувати надійність та забезпечувати захист персональних даних при здійсненні Інтернет-транзакцій.
Ключові слова: надійність, захист, персональні дані, Інтернет-транзакції, моніторинг, виявлення інцидентів, реагування на інциденти.

Пидкова Ю. И. Методы и средства исследования надежности и защиты персональных данных при осуществлении интернет-транзакций. В работе рассмотрено применение методов и средств исследования надежности и защиты персональных данных при осуществлении Интернет-транзакций, а также предложено применение методов и средств исследования надежности и защиты персональных данных при осуществлении Интернет-транзакций, к которым отнесены мониторинг, выявление и реагирование на инциденты. Показано, что при объединении мониторинга, обнаружения и реагирования на инциденты в единую систему, это позволяет исследовать надежность и обеспечивать защиту персональных данных при осуществлении Интернет-транзакций.
Ключевые слова: надежность, защита, персональные данные, Интернет-транзакции, мониторинг, выявление инцидентов, реагирование на инциденты.

Pidkova Y. I. Methods and tools to study the reliability and protection of personal data in the implementation of internet transactions. The paper discusses the use of methods and tools to study the reliability and protection of personal data in the implementation of Internet transactions, and proposed the use of methods and tools to study the reliability and protection of personal data in the implementation of Internet transactions, which include monitoring, detection and response to incidents. It is shown that when combining monitoring, detecting and responding to incidents into a single system, this allows us to investigate the reliability and ensure the protection of personal data during the implementation of Internet transactions.
Keywords: reliability, protection, personal data, Internet transactions, monitoring, incident detection, incident response.

Вступ. Фінансовим послугам, включаючи банки, страхування і інвестиції, характерна найважливіша роль для повсякденного життя споживачів. Однак для більшості продуктів, які пропонуються традиційними фінансовими організаціями, характерна відсутність турботи про простоту реєстрації та забезпечення належного рівня захисту персональних даних при здійсненні Інтернет-транзакцій, хоча і фінансові транзакції, зазвичай, здійснюються за допомогою надійного Web-сайту [1, 2].

До найбільших ризиків, пов'язаних з віддаленою ідентифікацією об'єктів у цифровому середовищі, слід віднести сферу електронних фінансових відносин, до яких відносяться ризики, зв'язані [2-6]: з втратою особистих даних користувача електронних грошей; зі зломом електронного гаманця; з втратою даних або грошових коштів через збій обладнання системи; з викраденням даних клієнтів, яке здійснюються за допомогою хакерських атак на клієнта, банк або магазин тощо.

У зв'язку з тим, що рівень загальної комп'ютерної грамотності споживачів електронних фінансових послуг невисокий, тому кількість постраждалих користувачів збільшується паралельно зростанню популярності фінансових послуг [5, 6]. Основна проблема при здійсненні Інтернет-транзакцій полягає в спробі перехоплення даних під час транзакції або викрадення особистої інформації з бази даних.

До ключових недоліків проведення Інтернет-транзакцій слід віднести наступні [5-9]:

- недостатньо високий рівень інформаційної безпеки, тобто характерна присутність слабкої організації захисту платежів і збереження фінансових коштів клієнтів на рахунках. Цей недолік відкриває можливість для кіберзлочинців для викрадення персональних даних;
- технічні збої, пов'язані з великою кількістю користувачів, технічними роботами або оновленням програмного продукту і, відповідно, навантаженням на платіжну систему;
- недостатню інформованість клієнтів конкретного банку, які здійснюють транзакції, про нові технології та засоби захисту від шахрайських дій.

Тобто сучасний етап розвитку технологій електронних платежів, особливо при здійсненні Інтернет-транзакцій, потребує використання сучасних методів та засобів дослідження надійності та

захисту персональних даних. Хоча технології захисту інформації також стрімко розвиваються, але існує необхідність у подальшому дослідженні надійності та захисту персональних даних при здійсненні Інтернет-транзакцій.

Аналіз попередніх досліджень.

У роботі [1], автором виконано класифікацію за призначенням методів криптографічного захисту документообігу.

Автором роботи [2] розглянуто забезпечення безпеки інформації при використанні пластикових карток за допомогою технології 3-D Secure, а за допомогою цієї ж технології у роботі [3] розглянуто протокол захисту електронних платежів. Розподілену систему по виявленню шахрайських платежів розглянуто в [4].

Сучасним принципам побудови захищених інтелектуальних мереж, призначених для використання у системах забезпечення економічної безпеки з організацією процесів розробки ПО присвячені роботи [5-7].

У роботах [8, 9] приведені особливості захисту електронних платіжних систем у мережі Інтернет.

Далі, розглянемо існуючі методи та засоби дослідження надійності та захисту персональних даних при здійсненні Інтернет-транзакцій.

До відомих засобів захисту інформації в банківській організації відносяться [7, 10]: апаратні і програмні.

До апаратних засобів захисту інформації відносяться [7]: USB-токени; смарт-карти; SecretNet; «Страж NT» тощо. До програмних засобів захисту інформації відносяться: технологія 3D-Secure; ПЗ з двухфакторною аутентифікацією; Протокол HTTPS; Міжмережеві екрани тощо.

З метою забезпечення безпеки при здійсненні Інтернет-транзакцій застосовуються два методи [4, 5, 7]:

- в системі на основі особистого ідентифікаційного номера / номера транзакції (PIN / TAN) PIN-код являє собою пароль, який використовується для входу в систему, а TAN – це одноразові паролі для підтвердження транзакцій. Розподіл номерів транзакцій (TAN) може здійснюватися різними способами. Найбільш поширений – це відсилання списку номерів TAN користувачеві онлайнових банківських послуг електронною поштою. Найбільш безпечний спосіб використання номерів TAN – це їх генерація в міру необхідності за допомогою секретного ключа. В цьому випадку номера TAN генеруються за допомогою ключа в залежності від часу і унікального секретного коду, що зберігається в секретному ключі (двухфакторна аутентифікація). Надання онлайнових банківських послуг за допомогою номерів PIN / TAN зазвичай здійснюється через WEB-браузер з використанням захищених з'єднань по протоколу безпечних з'єднань (SSL), завдяки якому відсутня необхідність додаткового шифрування;

- в системі передача номерів TAN для користувача онлайнових банківських послуг здійснюється відправкою повідомлень SMS з номером TAN поточної банківської транзакції на мобільний телефон користувача, що працює за стандартом GSM. У тексті SMS, зазвичай, наводиться сума і докладна інформація про транзакції; номер TAN є чинним лише на короткий час. Послуга «TAN через SMS» використовується в банках багатьох країн, зокрема Німеччини, Австрії та Нідерландів, оскільки вважається, що даний спосіб забезпечує високий рівень безпеки.

Крім того, існує різновид онлайн-банкінгу на основі підпису, в якому всі транзакції завіряються підписом і шифруються [2, 7]. Ключі для генерації підпису та шифрування можуть зберігатися на смарт-картах або на будь-якому іншому пристрої зберігання даних в залежності від конкретної системи реалізації.

Ідентифікацію при проведенні Інтернет-транзакцій з використанням банківських облікових даних можна розділити на 2 види, в яких [3, 5]:

- використовуються електронні засоби платежу (банківська карта);
- використовуються облікові дані системи банк-клієнт.

Безпечній електронній фінансовій транзакції повинні пред'являтися такі вимоги [4, 7]:

- цілісність і авторизація;
- конфіденційність;
- готовність і надійність.

При здійсненні Інтернет-транзакцій взаємодія у системі «банк-клієнт» може здійснюватися, в тому числі, шляхом направлення клієнтові SMS на номер мобільного телефону. Для підвищення безпеки в усьому світі широко поширений спосіб двухфакторної ідентифікації, коли ідентифікація і аутентифікація клієнта здійснюється одночасно за допомогою номера мобільного оператора і

направленням одноразового пароля на вказаний номер. За допомогою такої ідентифікації виконуються транзакції в сфері банківських послуг і взаємодії клієнтів і кредитних організацій [3].

Існуючі в даний час інформаційні системи ідентифікації і аутентифікації є централізованими [2, 7]. Недоліком такої системи є її вразливість. Децентралізовані системи ідентифікації по суті представляють собою сукупність розподілених реєстрів даних. Децентралізований реєстр даних може містити інформацію будь-якого роду, однак характерною особливістю є те, що копії реєстру зберігаються одночасно у всіх його користувачів і автоматично оновлюються. Надійність системи забезпечують криптографічні алгоритми, завдяки яким внесений до реєстру запис неможливо видалити або підробити [1, 3]. Легітимність додавання нових записів досягається алгоритмами, які відрізняються від системи до системи, але виконують одну і ту ж функцію: не допустити технічної можливості спотворення даних (наприклад, через комп'ютерний збій або злий умисел). Розподілені реєстри більш захищені від кібератак, тому що замість однієї бази даних вони представляють собою безліч копій однієї і тієї ж бази даних, і таким чином, щоб бути успішною, кібератака повинна бути проведена на всі копії одночасно. Технологія також є стійкою для несанкціонованої зміни або злому, оскільки учасники мережі відразу ж виявлять зміни в одній з частин реєстру. Додатково до цього методи, використовувані для захисту і поновлення інформації, передбачають, що учасники можуть ділитися даними і бути впевненими, що всі копії реєстру збігаються один з одним в будь-який момент часу. У зв'язку з тим, що концепція розподілених реєстрів є досить новою, хоча вже використовується бізнесом, в даний час, як в зарубіжних країнах, так і в Україні, відсутня достатнє і необхідне правове регулювання ідентифікації і аутентифікації на основі децентралізованих систем.

Регулювання питань транскордонної передачі персональних даних, включаючи ідентифікаційну інформацію, на міжнародному рівні проводиться на основі Конвенції про захист осіб у відношенні автоматизованої обробки персональних даних (ETS N 108) (укладена в Страсбурзі 28.01.1981).

Слід також зазначити, що найбільш поширений варіант шахрайства при здійсненні платежів в мережі Інтернет є фішинг, спрямований на отримання доступу до конфіденційних даних користувачів – логінів і паролів [3, 7]. Таке може досягатися шляхом проведення масових розсилок електронних листів і особистих повідомлень від імені банків, великих Інтернет-магазинів. З метою мінімізації таких ризиків необхідно розробити системи дослідження надійності з управління ризиками, які пов'язані з електронними платежами, в тому числі з Інтернет-транзакціями.

Постановка проблеми. У роботі необхідно розглянути і запропонувати застосування методів та засобів дослідження надійності та захисту персональних даних при здійсненні Інтернет-транзакцій.

Результати досліджень. До основних методів дослідження і захисту персональних даних при здійсненні Інтернет-транзакцій слід віднести: моніторинг, виявлення і реагування на інциденти. Ці методи включають заходи, що вживаються для виявлення підозрілих дій, в першу чергу на підставі інформації про різні події; заходи по виявленню загроз на ранній стадії розглядаємого процесу; а також заходи, що вживаються для розпізнавання загроз при виявленні тих чи інших підозрілих дій.

Метод моніторингу являє собою комплексну систему виявлення загроз щодо захисту персональних даних при здійсненні Інтернет-транзакцій, який допомагає відстежити різні дії шляхом пошуку аномальних відхилень у поведінці і діях користувачів на прикладному рівні, а також на рівні системи, бази даних або мережі. Крім того, така комплексна система буде спостерігати за тим, що відбувається в рамках окремих рахунків і між різними рахунками, використовуючи будь-які канали, доступні користувачам. Такий метод дослідження і захисту персональних даних при здійсненні Інтернет-транзакцій також допомагає відслідковувати і аналізувати поведінку користувачів або акаунтів і пов'язані з цим транзакції, і дозволяє виявляти аномальну поведінку, використовуючи правила або статистичні моделі. Крім того, метод дослідження і захисту персональних даних при здійсненні Інтернет-транзакцій може (в оптимальним варіанті) використовувати безперервно оновлюючі профілі і облікові записи користувачів, а також тимчасових груп, порівнюючи транзакції і виявляючи серед них підозрілі. Зокрема, для ретельного відстеження внутрішніх дій щодо захисту персональних даних при здійсненні Інтернет-транзакцій необхідний моніторинг привілейованих користувачів інформаційних технологій, які можуть безпосередньо вносити зміни в файли і дані, на відміну від тих, які використовують звичайні призначені для користувача програми.

Виявлення в методі дослідження і захисту персональних даних при здійсненні Інтернет-транзакцій представляє систему виявлення випадків загроз, яка здатна обробляти, розбивати на частини і аналізувати великі обсяги даних з використанням складних взаємозв'язків і сортування за правилами, що визначаються комерційними організаціями (банками), з метою запобігання загрозам. Такий метод дослідження і захисту персональних даних при здійсненні Інтернет-транзакцій може

використовуватися для виявлення загроз з боку як внутрішніх зловмисників (наприклад, співробітників), так і зовнішніх (наприклад, клієнтів). Для підтримки функцій виявлення загроз система виявлення, дослідження і захисту персональних даних при здійсненні Інтернет-транзакцій може і повинна класифікувати різні об'єкти, такі як користувачі, облікові записи, домашні господарства, персональні комп'ютери, мобільні телефони та інтерактивні термінали, з метою виявлення аномальної поведінки даного об'єкта при виконанні транзакції. У разі виявлення загроз застосовується політика на основі правил, що базується на людських судженнях і знаннях, а також на математичних моделях прогнозування, які допомагають оцінити ймовірність дій щодо захисту персональних даних при здійсненні тієї чи іншої Інтернет-транзакції.

При дослідженні і захисту персональних даних при здійсненні Інтернет-транзакцій має бути присутнім реагування (на випадки загроз), тобто при виявленні підозрілої активності система даного методу повинна реагувати на підозрілі дії і приймати різні запобіжні заходи, такі як блокування облікового запису або обмін інформацією.

Комбінації моніторингу та аналізу при дослідженні і захисту персональних даних при здійсненні Інтернет-транзакцій повинні відповідати найбільшою мірою рівнів ризиків з визначенням можливостей по реалізації і підтримці технологій забезпечення безпеки.

Архітектура системи дослідження і захисту персональних даних при здійсненні Інтернет-транзакцій повинна включати операції і компоненти. У разі ідеального варіанту, система дослідження і захисту персональних даних при здійсненні Інтернет-транзакцій повинна запускати моніторинг всього сеансу роботи з моменту первинного входу користувача в систему. При цьому система виконує операції з протидії загроз по розкриттю персональних даних при здійсненні Інтернет-транзакцій, тобто виконує моніторинг і можливе реагування на загрози.

Під час виконання процедури введення логіна і пароля, аутентифікації і авторизації в системі захисту персональних даних при здійсненні Інтернет-транзакцій з метою перевірки в звичайній ситуації, аналізу піддається процедура першого входу в систему. Далі досліджувані облікові дані, зібрані в процесі входу в систему захисту персональних даних при здійсненні Інтернет-транзакцій, порівнюються з інформацією, що знаходиться в базі облікових даних користувачів (імена користувачів і паролі), IP-адресою, базою даних профілів поведінки користувачів тощо. У результаті такої процедури визначається кількісний показник ризику. Виконання авторизації з метою перевірки відбувається згідно з правилами аутентифікації, що визначені у базі облікових даних. В системі захисту персональних даних при здійсненні Інтернет-транзакцій така база може розширюватися шляхом додавання нових правил.

В системі дослідження та захисту персональних даних при здійсненні Інтернет-транзакцій після авторизації користувача виявляються випадки погроз і проводиться збір інформації з різних джерел (тобто мереж, служб систем і на основі аутентифікації). Виявлення загроз в системі відбувається при аналізі даних, отриманих від компонента, який відповідає за моніторинг таких випадків. При виявленні високого рівня ризику загроз захисту персональних даних при здійсненні Інтернет-транзакцій, компонент, який відповідає за протидію таким загрозам, запитує більш серйозну перевірку для користувача, який увійшов в систему. Отримані рішення з питань загроз повинні відправлятися назад до бази даних. Тобто виконується формування самонавчальної замкнутої системи по дослідженню і захисту персональних даних при здійсненні Інтернет-транзакцій, яка дозволяє поліпшити її експлуатаційні характеристики на наступному етапі роботи.

В системі дослідження та захисту персональних даних при здійсненні Інтернет-транзакцій повинен бути компонент, який відповідає за адміністрування та підготовку звітів, що дозволить більш детально вивчити загрози і більш ефективно виконувати управління. Такий компонент відкриває можливість користувачам системи виконувати безперешкодний аналіз і складати звіти за функціональними характеристиками, виявляти протиріччя в оцінці або доступі, визначати елементи системи, які можна вдосконалити, а також відстежувати дії користувачів і експлуатаційні показники системи. Крім того, за допомогою засобів підготовки звітів може бути забезпечено наочне уявлення докладної інформації про характеристики системи захисту персональних даних при здійсненні Інтернет-транзакцій для фахівців, які займаються аналізом випадків загроз.

Архітектура системи дослідження і захисту персональних даних при здійсненні Інтернет-транзакцій повинна включати види, що пов'язані: з модулями виявлення випадків погроз, які повинні бути вбудовані в сервер додатків (наприклад, WEB-сервер); з прослуховуванням і / або моніторингом онлайн-додатків; з програмними інтерфейсами для успадкованих додатків.

До найбільш важливих факторів, які визначають ефективність додатків, слід віднести правила і процеси, що відображають діяльність організації (наприклад, Інтернет-магазину). Для модуля

виявлення загроз захисту персональних даних при здійсненні Інтернет-транзакцій, який розміщений всередині сервера додатків Правила (встановлюється певною організацією), характерне застосування фільтра до всіх запитів по протоколу передачі гіпертексту (HTTPS) (наприклад, здійснення Інтернет-транзакції), перед тим як дана транзакція звернеться до додатка.

Здійснення Інтернет-транзакцій може бути зупинено або перенаправлено на процедуру верифікації транзакції в реальному часі шляхом виконання правил виявлення загроз для даного модуля. Для підозрілих Інтернет-транзакцій повинно виконуватись припинення з передачею на розгляд фахівцеві-аналітику. Для цього, за допомогою спеціально налаштованих інтерфейсів прикладного програмування (API) виконується об'єднання таким чином, що транзакції перенаправляються на процедуру перевірки типу запит / відповідь.

За допомогою інтерфейсів API для проведення транзакцій через систему виявлення загроз, їх потік контролюється, і при виявленні підозрілої транзакції користувач піддається перевірці в реальному часі. Робота таких інтерфейсів API заснована на WEB-послузі і, які ускладнюють перехід від однієї конкретної системи до іншої.

У разі застосування інтерфейсів API з метою виявлення загроз захисту персональних даних при здійсненні Інтернет-транзакцій вони дозволяють виконувати безпосередній контроль потоку таких транзакцій, але це вимагає виконання значної роботи з інтеграції. Крім того, у разі зміни базової програми – інтерфейсам необхідно постійно оновлюватися. Цей метод є кращим для серверів додатків, які не вимагають втручань в Інтернет-транзакції користувачів в реальному часі, оскільки він є простим з точки зору відмови або заміни.

Висновки. У роботі розглянуто застосування методів та засобів дослідження надійності та захисту персональних даних при здійсненні Інтернет-транзакцій. Показано, що до відомих засобів захисту персональних даних при здійсненні Інтернет-транзакцій відносяться апаратні і програмні. Забезпечення безпеки при здійсненні Інтернет-транзакцій досягається на основі двох методів: на основі особистого ідентифікаційного номера / номера транзакції (PIN / TAN) та передачі номерів TAN для користувача онлайнових банківських послуг з відправкою повідомлень SMS з номером TAN поточної банківської транзакції на мобільний телефон користувача, що працює за стандартом GSM. Послуга «TAN через SMS» використовується в банках багатьох країн, зокрема Німеччини, Австрії та Нідерландів, оскільки вважається, що даний спосіб забезпечує високий рівень безпеки. Ідентифікація при проведенні Інтернет-транзакцій з використанням банківських облікових даних відбувається з використанням електронних засобів платежу (банківської картки) і облікових даних системи банк-клієнт.

Також в роботі запропоновано застосування методів та засобів дослідження надійності та захисту персональних даних при здійсненні Інтернет-транзакцій, до яких віднесено моніторинг, виявлення і реагування на інциденти. Показано, що при об'єднанні моніторингу, виявлення і реагування на інциденти в єдину систему, це дозволить досліджувати надійність та забезпечувати захист персональних даних при здійсненні Інтернет-транзакцій.

1. Йона Л. Г. Криптографічний захист електронного документообігу / Л.Г. Йона, О.О. Йона, В.С.Терешко // Цифрові технології. – 2013. – № 13. – С. 142-146.

2. Быхно А. 3D-Secure: безопасные покупки через Интернет [Электронный ресурс] / Александр Быхно. – Режим доступа: http://credit-card.ru/articles/security/3dsecure.php

3. 3-D Secure [Электронный ресурс]. – Режим доступа: http://www.bankdbo.ru/3-d-secure

4. Фахретдинов, Р. Анализ средств подтверждения банковских транзакций [Электронный ресурс] / Руслан Фахретдинов. – Режим доступа: http://frodex.ru/article/ authentification2014

5. Гончаров В.В. Безопасность и защита интернет-платежей // Расчеты и операционная работа в коммерческом банке. – 2010. – № 4. – С. 54-58.

6. Йона О.О. Специфічні чинники активізації загроз економічній безпеці господарюючих суб'єктів / О.О. Йона // Технологічний аудит та резерви виробництва. – 2012. – № 4/6 (8). – С. 31-32.

7. Юсупова О.А. Безопасность транзакций при использовании Интернет-банкинга / О.А. Юсупова // Финансовая аналитика: проблемы и решения. – 2016. – №35. – С. 26-40.

8. Грицюк П.Ю. Електронні гроші – нове досягнення криптографії та інформаційних технологій / П.Ю. Грицюк, Ю.І. Грицюк // Науковий вісник НЛТУ України: зб. наук.-техн. праць. – Львів : РВВ НЛТУ України. – 2013. – Вип. 23.1. – С. 339-347.

9. Грицюк П.Ю., Грицюк Ю.І. Особливості захисту електронних платіжних систем у мережі Інтернет / П.Ю. Грицюк, Ю.І. Грицюк // Науковий вісник НЛТУ України: зб. наук.-техн. праць. – Львів : РВВ НЛТУ України. – 2013. – Вип. 23.10. – С. 314-331.

10. Мартынов В.Г. Электронные деньги. Интернет-платежи / В.Г. Мартынов., А.А. Андреев В.А. Кузнецов. – М. : Изд-во "Маркет ДС", ЦИПСиР, 2010. – 176 с.