efficiency of the online store were revealed, which will increase the conversion and number of visits, as well as reduce costs.

REFERENCES:

1. Trading platforms [Electronic resource] /. - The electron. journal –Access mode: https://www.investopedia.com/terms/t/trading-platform.asp
2. Types of trading platforms [Electronic resource] /. - The electron. journal – Access mode: https://bestforexbroker.online/types-of-forex-trading-platforms/
3. Ecommerce system [Electronic resource] /. - The electron. journal - Access mode: https://www.cs-cart.com/ecommerce-system.html
4. Online store performance [Electronic resource] /. - The electron. journal - Access mode: https://www.theselfemployed.com/ecommerce/10-ways-optimize-online-store-performance/
5. Sales Conversion [Electronic resource]. - The electron. journal - Access mode: https://www.klipfolio.com/resources/kpi-examples/sales/sales-conversion-rate
6. Calculation of the effectiveness [Electronic resource]. - The electron. journal - Access mode: https://www.investopedia.com/articles/fundamental-analysis/10/strategy-performance-reports.asp
7. Dropshipping [Electronic resource]. - The electron. journal - Access mode: https://www.shopify.com/guides/dropshipping/understanding-dropshipping
8. UTM tags [Electronic resource]. - The electron. journal - Access mode: https://www.opentracker.net/article/UTM-tags

УДК 004.056.55

ЗБЕРІГАННЯ КВАЛІФІКОВАНОГО ЕЛЕКТРОННОГО ПІДПИСУ

Р.С. Алексєєв, С. І. Войцех
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

Розвиток глобальних комунікацій в діловому і повсякденному житті обумолює поширення взаємовідносин, пов’заних з електронним обміном даними. В обміні можуть приймати участь органи державної влади, комерційні і некомерційні організації, а також громадяни на офіційному та особистому рівнях.

Проблема зберігання електронних документів від копіювання, модифікації і підробки вимагає застосування спеціальних засобів і методів захисту. Важливу роль серед них відіграє електронний цифровий підпис (ЕЦП), який забезпечує підтвердження цілісності інформації документа, його реквізитів і факту підписання конкретною особою.

Цифровий підпис дозволяє здійснити:

1. Аутентифікацію особи - автора електронного документа.
2. Контроль цілісності переданого документа: при будь-якій випадковій або навмисній зміні документа підпис стане недійсним, тому що він обчислений на підставі вихідного стану документа і відповідає лише йому.

3. Захист від модифікації документа через наявність можливості контролю цілісності. Гарантія виявлення підробки при контролі цілісності робить підробку недоцільною у більшості випадків.

4. Неможливість відмови від авторства. ЕЦП створюється із використанням закритого ключа, який повинен бути відомим тільки підписанту, що не дає змоги відмовитися від свого підпису під документом.

5. Доказове підтвердження авторства документа. Створити коректний підпис можливо, лише знаючи закритий ключ, а він повинен бути відомим тільки власнику, через що власник пари ключів може довести своє авторство під документом. В документі можуть бути підписані такі поля як «автор», «внесені зміни», «мітка часу» і т.п.

На даний час порядок та організація електронного документообігу, а також правовий статус електронного цифрового підпису визначаються Законом України «Про електронні довірчі послуги» (далі – Закон). Він запроваджує поняття «кваліфікований електронний підпис»(КЕП) на зміну поняття «електронний цифровий підпис». Згідно Закону кваліфікований електронний підпис – це удосконалений електронний підпис, який створюється із використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа. Для того, щоб мати можливість підписувати електронні документи, подавати електронну звітність або електронні декларації, особа повинна отримати КЕП. Видача останнього згідно Закону є довірчою послугою, що здійснюється лише в центрах сертифікації ключів, акредитованих Центральним засвідчувальним органом (АЦСК).

Згідно Закону для кваліфікованих постачальників електронних довірчих послуг кваліфікований електронний підпис чи печатка вважається таким, що пройшов перевірку та отримав підтвердження, якщо під час перевірки за допомогою кваліфікованого сертифіката електронного підпису чи печатки отримано підтвердження того, що особистий ключ, який належить підписувачу чи створювачу електронної печатки, зберігається в засобі кваліфікованого електронного підпису чи печатки.

Це означає, що усі КЕП повинні генеруватися та зберігатися на захищеному носієві ключової інформації(НКІ).

Застосування апаратних НКІ (смарт-карт, токенів) має такі недоліки:

1. Висока ціна носіїв.
2. Необхідність завжди мати пристрій при собі (у разі утрати пристрою КЕП потрібно перевипускати)
3. Один захищений носій може зберігати лише один секретний ключ.
4. Електронний підпис неможливо використовувати на веб-ресурсах без установки на комп’ютер необхідних бібліотек (драйверів) для роботи з носієм.
5. Недостатня рівень забезпеченості носіями.

Усунення наведених недоліків може бути досягнуто шляхом створення програмно-апаратного комплексу “хмарного” КЕП на базі існуючого АЦСК. Такий підхід до надання електронних довірчих послуг також забезпечить такі переваги, як:

1. Одне централізоване сховище ключів, доступ до якого можливий лише при наявності інтернет-підключення.
2. Відповідальність за збереження і захист ключів приймає на себе АЦСК.
3. Відпадає необхідність використання бібліотек (драйверів).
4. Можливість інтеграції комплексу зі сторонніми сервісами.
5. Низька ціна аренди місця в криптомодулі.
6. Спрощення процедури отримання КЕП.

ПЕРЕЛІК ПОСИЛАНЬ:

1. https://zakon.rada.gov.ua/laws/show/2155-19#n534
2. https://www.pfu.gov.ua/kr/327258-pro-kvalifikovanyj-elektronnyj-pidpys/
3. Семь безопасных информационных технологий / под ред. А. С. Маркова. - М.: ДМК Пресс, 2017. — 224 с.: ил
4. https://medoc.ua/uk/blog/kep-na-zahishhenih-nosijah-roztlumachumo-shho-do-chogo

УДК 004.056

РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ РИЗИК-БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ

В.В. Гнатушенко, В.О. Бура, Т.М. Фененко
(Україна, Дніпро, Національна металургійна академія України)

Постановка проблеми. Створення інформаційної системи (ІС) ризик-безпеки персональних даних, яка б дозволила знизити невизначеність при виборі альтернатив, тим самим зменшити можливість прийняття неефективного рішення.

Сучасні інформаційні системи найчастіше представляють собою складні комплекси взаємопов'язаних компонентів. Завдання аналізу безпеки, оцінки ризиків у таких системах ускладнюється тим, що експерту невідомі точні значення характеристик системи яка аналізується. Більшість існуючих методик припускають завдання наближених точкових оцінок, що знижує достовірність отриманих, також точкових, результуючих показників.

При експертному оцінюванні, ми стикаємося з різними видами невизначеності, і основним завданням є її спільне моделювання. Аналогічна проблема виникає і при виборі найбільш ефективного комплексу засобів протидії загрозам інформаційної безпеки. Для її вирішення використовується методика рандомізації оцінок факторів з подальшим відбором результатів, що задовольняють вихідними даними.

В умовах реального світу інформація слабо визначена - має нечислової характер, неточна, погано структурована. Фактично, первинні дані являють собою випадкові величини. Поряд з невизначеністю оцінок можлива і