ЗАХИСТ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ШЛЯХОМ ВИКОРИСТАННЯ ЦИФРОВОГО ПІДПИСУ НА ПІДПРИЄМСТВАХ

Романенко Олена Миколаївна

Анотація

У роботі проаналізовано недоліки та переваги використання цифрового підпису в процесі електронного документообігу. Розроблено рекомендації щодо підвищення ефективності використання електронного документообігу на вітчизняних підприємствах.

Ключові слова

Електронний цифровий підпис (ЕЦП), електронний документообіг (ЕД), захист інформації, інформаційні технології.

Вступ

Широке використання інформаційних технологій у всіх сферах життя суспільства робить досить актуальною проблему захисту інформації, інформаційних ресурсів, каналів передачі даних від злочинних дій зловмисників. У міру розвитку технологій електронних платежів та документообігу є велика небезпека втручання сторонніх осіб, з метою завдання шкоди підприємству, що призведе до відчутних збитків. Тому не випадково захист даних у комп'ютерних мережах стає однією із найгостріших проблем.

Метою дослідження є розроблення рекомендацій щодо підвищення ефективності використання електронного цифрового підпису (ЕЦП) на вітчизняних підприємствах.

Результати дослідження

На сьогодні вирішення проблеми захисту інформації різного виду на підприємствах здійснюється шляхом використання електронного цифрового

підпису (ЕЦП), який дозволяє здійснювати аутентифікацію як автора електронного документа так і самого документа[5].

Технологія ЕЦП може бути не менш ефективною, ніж звичайного підпису. Але для практичного використання виникають проблеми правового визнання електронного підпису нарівні із звичайним, що в свою чергу потребує певного регулювання процедур надання засобів цифрового підпису[4].

Засоби для ЕЦП (програмне забезпечення для шифрування та коди) надають уповноважені на це установи – центри сертифікації, які засвідчують надання засобів електронного підпису особі сертифікатом. Українське законодавство передбачає два види сертифікатів: звичайний та посилений. Звичайний може видаватися будь-якою особою (центром сертифікації), яка вирішила займатися цим видом діяльності. Для видачі посиленого сертифіката центр сертифікації повинен користуватися засобами ЕЦП, які в Законі названо «надійними засобами ЕЦП» та пройти акредитацію уповноваженим на це органом – центральним засвідчувальним центром.

Не менш серйозною прогалиною закону[1-3] є недостатня увага до питання захисту інформації про особу. Закон досить широко як для такого документу говорить про те, що в сертифікаті вказуються необхідні дані про особу.

Крім того, при систематичному співробітництві підприємства з партнерами за допомогою електронних технологій, можуть виникати й інші проблеми при розв’язанні господарських конфліктів. Все це потребує доповнення законодавства, перш за все Господарського та Цивільного кодексів і відповідних процесуальних кодексів, що поки що залишається лише перспективою.

Проблеми запровадження в Україні електронного документообігу та ЕЦП стають все більш актуальними. Вони набувають значної політичної та економічної ваги у зв’язку з розширенням використання інформаційно-комунікаційних технологій у суспільних відносинах, розбудові систем електронних платежів, електронної торгівлі тощо.

Одне з проблемних питань, що потребує вирішення, – це робота центрів сертифікації ключів, які мають надавати послуги цифрового підпису. Спеціалісти вважають, що кількість бажаючих займатися такою діяльністю, можливо, буде

досить незначною. Зокрема, тому, що фінансовий бар'єр виходу на ринок таких структур за нинішніх умов буде досить високим з огляду на специфіку їх функцій.

Висновки

Отже, центр сертифікації ключів є критичним елементом в системі застосування ЕЦП. Неналежна організація надання послуг ЕЦП, незабезпечення відповідного рівня безпеки функціонування, захисту інформації або збої у роботі зазначеного суб'єкта може створити умови, що сприятимуть масовим зловживанням при застосуванні ЕЦП, в тому числі їх підробленню, компрометації та неможливість використовувати даний механізм підписувачами, що отримують послуги ЕЦП у цих суб'єктів та особами, які перевіряють ЕЦП. Але це питання можна вирішити лише за допомогою повного впровадження електронного документообігу, для цього необхідно доопрацювати відповідну законодавчу та нормативну базу, що регламентує електронне урядування в органах державної влади та органах місцевого самоврядування, в першу чергу надання послуг в електронній формі;

– потребує вирішення питання правового надання юридично значимого статусу електронним інформаційним ресурсам, які розміщуються в інформаційно-телекомунікаційних системах органами державної влади та органами місцевого самоврядування[6];

– необхідно визначити на законодавчому рівні порядок, статус та гарантії надання послуг в електронній формі, встановити регламенти і стандарти їх надання, у тому числі тих, які потребують об'єднання зусиль кількох органів виконавчої влади;

– потребує врегулювання проблема передавання та довгострокового зберігання електронних документів у державних архівах, музеях, бібліотеках, підтримки їх в актуальному стані та забезпечення доступу до них.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Конституція України від 28.061996 р. № 254 к/96-ВР // Відомості Верховної Ради України від 23.07.1996 р. – 1996. – № 30. – С. 141.
2. Цивільний кодекс України від 16.01.2003 р. № 435-IV // Відомості Верховної Ради України від 03.10.2003 р. – 2003. – № 40. – С. 356.
3. Закон України «Про електронні документи й електронний документообіг» від 22.05.2003 р. № 851-IV // Відомості Верховної Ради України. – 2003. – № 54.
4. Чирський Ю. А. Електронний цифровий підпис: правові аспекти застосування // Довідник секретаря та офіс-менеджера. – №1. – 2007. – С. 26-31
5. Азарова А. А., Ивчук Е. В., Кукуруза М. И., Электронная цифровая подпись как средство защиты информационной модели предприятия.
6. Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження): Монографія. – К.: Атака, 2007. – 304 с.