КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (14), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.14.100106
УДК 004.031

Паламарчук Світлана Анатоліївна
начальник науково-дослідного відділу
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0001-7483-9165
palam_sv@ukr.net

Паламарчук Наталія Анатоліївна
начальник науково-дослідної лабораторії
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0001-8818-7794
3ndl3@ukr.net

Ткач Володимир Олександрович
старший науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0003-0013-7368
tkachwolodymyr@gmail.com

Шугалій Ольга Олександрівна
старший науковий співробітник
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID ID: 0000-0002-6587-0096
olga.shugaliy@gmail.com

ФОРМИ ЕЛЕКТРОННОГО ПІДПИСУ ТА ОСОБЛИВОСТІ ЙОГО ВИКОРИСТАННЯ В ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Анотація. «Зелене світло» широкому застосуванню електронних документів та цифрового підпису в державі, дав Закон України «Про електронні документи» та «Про електронний цифровий підпис», які набрали чинності з 28.12.2003 р. і з 01.01.2004 р. відповідно. Продовженням у запровадженні електронних документів, в тому числі, форм електронного підпису та використання їх в захищених інформаційних системах, стало прийняття в 2018 році Закону України «Про електронні довірчі послуги» (Закон України «Про електронний цифровий підпис» втратив чинність) та низки підзаконних актів щодо електронної взаємодії між двома інформаційними ресурсами (державними реєстрами/інформаційно-телекомунікаційними системами) та/або для надання адміністративних послуг. Використання новітніх технологій, спрямованих на збільшення ефективності роботи, водночас породжує нові ризики, які можуть призводити до розкриття чутливої інформації, наслідки чого можуть бути критичними. Щоб цього не трапилося, система що створюється або існуюча система повинні бути добре захищеними та відповідати *Концепції «Захищених інформаційних систем».* Дана *Концепція* включає в себе ряд законодавчих ініціатив, наукових, технічних і технологічних рішень. Також, необхідно звернутися і до визначення надійної інформаційної системи, яке надано в *«Помаранчевій книзі»*. Згідно якої, надійна інформаційна система визначається як «система, що використовує достатні апаратні і програмні засоби, щоб забезпечити одночасну достовірну обробку інформації різного ступеня секретності різними користувачами або групами користувачів без порушення прав доступу, цілісності та конфіденційності даних та інформації, і яка підтримує свою працездатність в умовах впливу на неї сукупності зовнішніх і внутрішніх загроз». На сьогодні, серед усталених методів захисту інформації особливе місце займає електронний

підпис (як для перевірки цілісності документа, підтвердження авторства так і для автентифікації користувача).

Ключові слова: електронний підпис; кваліфікований електронний підпис; особистий ключ; відкритий ключ; захищені інформаційні системи; електронна взаємодія.

ВСТУП

Електронний підпис, як механізм захисту інформації, здобув можливість повноцінної реалізації в державних установах після удосконалення нормативно-правової бази України (банківська сфера раніше інтегрувала його в свою діяльність). Не менш важлива і реалізація технічних стандартів, які в сучасних реаліях функціонування інформаційно-телекомунікаційних систем мають бути інтероперабельними для забезпечення електронної взаємодії.

Постановка проблеми. Забезпечення будь-якого механізму захисту інформації (послуги безпеки) в сучасних системах має комплексних характер, та поєднує нормативне, організаційне та матеріально-технічне забезпечення. Кожна з цих складових постійно проходить адаптацію до сучасних реалій та відповідно, має адаптуватись і їх системна зв'язність. Не є виключенням і забезпечення електронного підпису, як механізму, який крім перевірки цілісності документа і підтвердження авторства, використовується і для автентифікації користувача в системі (послуги безпеки згідно НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» [5]) та наразі має ряд неоднозначних трактувань щодо реалізації між розробниками інформаційно-телекомунікаційних систем та розробниками комплексних систем захисту інформації.

Аналіз останніх досліджень і публікацій. Порушена проблема виникла не сьогодні. Її досліджували у своїх працях вітчизняні вчені, а саме: Кукарін О. Б. Ткач Ю.М. И.Д. Горбенко, С.И. Збитнев, А.А. Поляков І.В. Двойленко, С.Ф. Левшаков, О.П. Голобуцький, О.Б. Шевчук та інш. [6] – [9]. Використання тієї чи іншої форми електронного підпису чи печатки в інформаційних системах має свої особливості, які потрібно враховувати при створенні захищеної системи.

Метою статті є аналіз форм електронного підпису та деяких особливостей їх використання в захищених інформаційно-телекомунікаційних системах.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Провідні країни світу активно використовують захищені системи обміну даними і майже зовсім відмовилися від паперового діловодства. «Захищеною системою» можна вважати таку систему, яка має включати механізм захисту для забезпечення: збереженості документів; безпечного доступу; достовірності документів та протоколювання (реєстрації) дій користувачів [2], [14]. Ці вимоги є основою безпеки для будь-якої системи, а загрози порушення цілісності інформації, при сучасних варіантах їх реалізації, можуть призводити до викрадення інформації, її знищення чи модифікації. Причини витоку інформації можуть бути різні, це і недосконалість керівних документів, недотримання їх вимог, порушення правил поводження з документами, технічними засобами та носіями інформації. До таких факторів та порушень можна віднести:

недостатнє знання користувачами основ захисту інформації й нерозуміння необхідності їх ретельного дотримання;

використання неатестованих або несертифікованих технічних засобів обробки інформації, неліцензійного програмного забезпечення тощо;

слабкий контроль за дотриманням правил обробки інформації з боку служб захисту інформації та кібернетичної безпеки, плинність кадрів.

Для власників інформаційно-телекомунікаційних систем доцільним буде дотримання наступних правил:

захист інформації повинен забезпечуватися в будь-якій системі (важливим є впорядкування та консолідація інформації, впорядкування документообігу);

розмежування прав доступу користувачів в системі здійснювати з врахуванням його функціональних обов'язків;

контроль дотримання визначеного порядку зберігання облікових записів користувачів та стандартних правил кібернетичної безпеки;

забезпечення конфіденційності інформації здійснюється за рахунок використання засобів криптографічного захисту інформації (КЗІ), тощо.

Підтвердження цілісності документу, підтвердження авторства (окрім реалізації КЗІ) можливе з використанням електронного підпису та електронної печатки з використанням електронної позначки часу, а також через використання кваліфікованого електронного підпису (КЕП) та засобу КЕП чи печатки і удосконаленого електронного підпису та засобу удосконаленого електронного підпису чи печатки (форми електронного підпису) [1], [3], [6] – [8].

Для вибору тієї чи іншої форми електронного підпису з метою використання в захищених інформаційних системах, розглянемо, що представляють собою ці форми:

1) електронний підпис – це електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис;

2) з*асіб електронного підпису чи печатки* – апаратно-програмний або апаратний пристрій чи програмне забезпечення, які використовуються для створення та/або перевірки електронного підпису чи печатки;

3) КЕП – удосконалений електронний підпис, який створюється з використанням засобу КЕП і базується на кваліфікованому сертифікаті відкритого ключа.

Термін «кваліфікований підпис» введений *AC CWA 14167-1:2004* [13] та визначений в Directive 1999/93/EC [10] як розширений електронний підпис *{advanced electronic signature),* заснований на посилених сертифікатах *(qualified certificate),* створених безпечними (надійними) засобами накладання електронних підписів *(secure signature creation device).*

4) засіб КЕП чи печатки – апаратно-програмний або апаратний пристрій чи програмне забезпечення, які реалізують криптографічні алгоритми генерації пар ключів та/або створення КЕП чи печатки, та/або перевірки КЕП чи печатки, та/або зберігання особистого ключа КЕП чи печатки.

Пара ключів – це особистий та відповідний йому відкритий ключі, що є взаємопов'язаними параметрами алгоритму асиметричного криптографічного перетворення. *Особистий ключ* – параметр алгоритму асиметричного криптографічного перетворення, який використовується як унікальні електронні дані для створення електронного підпису чи печатки, доступний тільки підписувачу чи створювачу електронної печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів. *Відкритий ключ* – параметр алгоритму асиметричного криптографічного перетворення, який використовується як електронні дані для перевірки електронного підпису чи печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів. Умови зберігання відкритого ключа

мають унеможливлювати його модифікацію або підміну, допускається його зберігання й передача у стисненому вигляді згідно *ДСТУ 4145-2002*.

Отже, захищений носій особистих ключів це і є засіб КЕП чи печатки, що призначений для зберігання особистого ключа та має вбудовані апаратно-програмні засоби, що забезпечують захист записаних на ньому даних від несанкціонованого доступу, безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання. КЕП призначений для використання фізичними та юридичними особами-суб'єктами електронного документообігу, як для підтвердження особи так і для підтвердження цілісності даних в електронній формі.

Підпис, як спосіб ідентифікації підписувача електронного документу, дозволяє однозначно визначати походження інформації (джерело інформації), що міститься у документі. Для того, щоб мати можливість підписувати електронні документи (дані), подавати електронну звітність або електронні декларації посадова особа має отримати КЕП. Видача останнього, здійснюється Кваліфікованими надавачами електронних довірчих послуг (далі – КНЕДП), які внесені до довірчого списку.

5) удосконалений електронний підпис – електронний підпис, створений за результатом криптографічного перетворення електронних даних, з якими пов'язаний цей електронний підпис, з використанням засобу удосконаленого електронного підпису та особистого ключа, однозначно пов'язаного з підписувачем, і який дає змогу здійснити електронну ідентифікацію підписувача та виявити порушення цілісності електронних даних, з якими пов'язаний цей електронний підпис;

6) засіб удосконаленого електронного підпису чи печатки – апаратно-програмний або апаратний пристрій чи програмне забезпечення, які реалізують криптографічні алгоритми генерації пар ключів та/або створення удосконаленого електронного підпису чи печатки, та/або перевірки удосконаленого електронного підпису чи печатки, та/або зберігання особистого ключа удосконаленого електронного підпису чи печатки.

Окремо слід сказати про систему електронного документообігу, а саме про організацію роботи щодо підготовки до передавання на архівне зберігання електронних документів, де окрім обов'язкового застосування кваліфікованого електронного підпису (печатки), затверджені вимоги до формату даних та найменування файлу електронних документів, описів справ в електронній формі, вимоги нормативно-правових актів у сфері захисту інформації та ін. Зазначені вимоги значно ускладнюють передавання електронних документів на архівне зберігання. При чому, установи зобов'язані створювати документи постійного та тривалого (понад 10 років) зберігання у двох формах: паперовій та електронній [4].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Учасники електронного документообігу чи електронної взаємодії для засвідчення чинності відкритого ключа повинні використовувати лише кваліфікований сертифікат відкритого ключа, видача якого здійснюється КНЕДП, який внесений до довірчого списку, а для здійснення повноважень, спрямованих на набуття, зміну чи припинення прав та/або обов'язків фізичної або юридичної особи, здійснення інформаційного обміну з іншими юридичними особами, – виключно захищені носії особистих ключів. В органах управління необхідно мати відповідальний підрозділ (працівника), який забезпечує ведення обліку захищених носіїв особистих ключів та засобів КЕП чи печатки, а також,

зберігання оригіналів документів та/або їх копій, на підставі яких отримано кваліфіковані електронні довірчі послуги.

Організаційно-правову форму електронного підпису/печатки на сьогодні недооцінювати неможливо, оскільки, від надійності та правильності організації та поводження з засобами КЕП чи печаткою залежить система документообігу, електронна взаємодія, звітність, архівне зберігання електронних документів та інші види забезпечення життєдіяльності сучасних установ, організацій. Питання й надалі залишається доволі актуальним та потребує комплексного поєднання нормативних організаційних та технічних заходів складових реалізації ЕП для систем різного призначення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Про електронні довірчі послуги, Закон України № 2155-VIII (Україна). https://zakon.rada.gov.ua/laws/show/2155-19#Text.
2 Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, Постанова Кабінету Міністрів України № 373 (Україна). https://zakon.rada.gov.ua/laws/show/373-2006-п#Text.
3 Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності, Постанова Кабінету Міністрів України № 749 (2021) (Україна). https://zakon.rada.gov.ua/laws/show/749-2018-п#Text.
4 Про затвердження Порядку роботи з електронними документами у діловодстві та їх підготовки до передавання на архівне зберігання, Наказ Міністерства юстиції України № 1886/5 (2014) (Україна). https://zakon.rada.gov.ua/laws/show/z1421-14#Text
5 *Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу* (НД ТЗІ 2.5-004-99).
6 Кукарін, О. Б. (2015). *Електронний документообіг та захист інформації. Навчальний посібник*. Київ.
7 Карнаух, Д.В. Проблеми та перспективи використання електронного цифрового підпису в Україні. http://www.kpi.kharkov.ua/archive.
8 Ткач, Ю.М. Електронний цифровий підпис. http://uchil.net/?cm=167737.
9 Трофименко, О. Г., Логінова, Н.І., Буката, Л.М. (2016). Електронне врядування в Україні у контексті розвитку інформаційного суспільства. *Порівняльно-аналітичне право: електронне наукове фахове видання*, 1, 231 – 234.
10 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. https://eur-lex.europa.eu/eli/dir/1999/93/oj.
11 Ковтун, В. (2020). Хмарна платформа Сайфер для комплексної роботи з електронним підписом. У *«PKI-FORUM 2019»*.
12 Ковтун, В., Охріменко, А., & Стокіпний, О. (2019). Побудова довгострокового архіву електронних документів. У *«PKI-FORUM 2019»*.
13 AC CWA 14167-1-2004. Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures. https://www.gostinfo.ru/catalog/Details/?id=3915529.
14 Trusted Computer Systems Evaluation Criteria, TCSEC https://csrc.nist.gov/csrc/media/publications/conferencepaper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (14), 2021
ISSN 2663 - 4023

Palamarchuk Svitlana
Head of Research Department
Military Institute of Telecommunications and Informatization Heroes of Kruty, Kyiv, Ukraine
ORCID ID: 0000-0001-7483-9165
palam_sv@ukr.net

Palamarchuk Natalia
Head of Research Department
Military Institute of Telecommunications and Informatization Heroes of Kruty, Kyiv, Ukraine
ORCID ID: 0000-0001-8818-7794
3ndl3@ukr.net

Tkach Vladimir
Senior Research
Military Institute of Telecommunications and Informatization Heroes of Kruty, Kyiv, Ukraine
ORCID ID: 0000-0003-0013-7368
tkachwolodymyr@gmail.com

Shugaly Olga
Senior Research
Military Institute of Telecommunications and Informatization Heroes of Kruty, Kyiv, Ukraine
ORCID ID: 0000-0002-6587-0096
olga.shugaliy@gmail.com

FORMS OF ELECTRONIC SIGNATURE AND FEATURES OF ITS USE IN SECURED INFORMATION SYSTEMS

Abstract. The Law of Ukraine “On Electronic Documents” and “On Electronic Digital Signature”, which came into force on December 28, 2003 and January 1, 2004, respectively, gave the “green light” to the widespread use of electronic documents and digital signatures in the country. Continuation in the introduction of electronic documents, including electronic signature forms and their use in secure information systems, was the adoption in 2018 of the Law of Ukraine "On electronic trust services" (Law of Ukraine "On electronic digital signature" expired) and a number of bylaws regarding electronic interaction between two information resources (state registers / information and telecommunication systems…) and / or for the provision of administrative services. At the same time, the use of the latest technologies aimed at increasing the efficiency of work creates new risks that can lead to the disclosure of sensitive information, the consequences of which can be critical. To prevent this from happening, the system being created or the existing system must be well protected and comply with the Concept of "Secure Information Systems". This Concept includes a number of legislative initiatives, scientific, technical and technological solutions. Also, it is necessary to refer to the definition of a reliable information system, which is provided in the "Orange Book". According to which, a reliable information system is defined as “a system that uses sufficient hardware and software to ensure the simultaneous reliable processing of information of varying degrees of secrecy by different users or groups of users without violating access rights, integrity and confidentiality of data and information, and which maintains its performance under the influence of a set of external and internal threats. " Today, among the established methods of information protection, a special place is occupied by an electronic signature (both for verifying the integrity of the document, confirmation of authorship and for user authentication).

Keywords: electronic signature; qualified electronic signature; private key; public key; secure information systems; electronic interaction.

REFERENCES

1 Pro elektronni dovirchi posluhy, Zakon Ukrainy № 2155-VIII (Ukraina). https://zakon.rada.gov.ua/laws/show/2155-19#Text.

2 Pro zatverdzhennia Pravyl zabezpechennia zakhystu informatsii v informatsiinykh, telekomunikatsiinykh ta informatsiino-telekomunikatsiinykh systemakh, Postanova Kabinetu Ministriv Ukrainy № 373 (Ukraina). https://zakon.rada.gov.ua/laws/show/373-2006-p#Text.
3 Pro zatverdzhennia Poriadku vykorystannia elektronnykh dovirchykh posluh v orhanakh derzhavnoi vlady, orhanakh mistsevoho samovriaduvannia, pidpryiemstvakh, ustanovakh ta orhanizatsiiakh derzhavnoi formy vlasnosti, Postanova Kabinetu Ministriv Ukrainy № 749 (2021) (Ukraina). https://zakon.rada.gov.ua/laws/show/749-2018-p#Text.
4 Pro zatverdzhennia Poriadku roboty z elektronnymy dokumentamy u dilovodstvi ta yikh pidhotovky do peredavannia na arkhivne zberihannia, Nakaz Ministerstva yustytsii Ukrainy № 1886/5 (2014) (Ukraina). https://zakon.rada.gov.ua/laws/show/z1421-14#Text
5 Kryterii otsinky zakhyshchenosti informatsii v kompiuternykh systemakh vid nesanktsionovanoho dostupu (ND TZI 2.5-004-99).
6 Kukarin, O. B. (2015). Elektronnyi dokumentoobih ta zakhyst informatsii. Navchalnyi posibnyk. Kyiv.
7 Karnaukh, D.V. Problemy ta perspektyvy vykorystannia elektronnoho tsyfrovoho pidpysu v Ukraini. http://www.kpi.kharkov.ua/archive.
8 Tkach, Yu.M. Elektronnyi tsyfrovyi pidpys. http://uchil.net/?cm=167737.
9 Trofymenko, O. H., Lohinova, N.I., Bukata, L.M. (2016). Elektronne vriaduvannia v Ukraini u konteksti rozvytku informatsiinoho suspilstva. Porivnialno-analitychne pravo: elektronne naukove fakhove vydannia, 1, 231 – 234.
10 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. https://eur-lex.europa.eu/eli/dir/1999/93/oj.
11 Kovtun, V. (2020). Khmarna platforma Saifer dlia kompleksnoi roboty z elektronnym pidpysom. U «PKI-FORUM 2019».
12 Kovtun, V., Okhrimenko, A., & Stokipnyi, O. (2019). Pobudova dovhostrokovoho arkhivu elektronnykh dokumentiv. U «PKI-FORUM 2019».
13 AC CWA 14167-1-2004. Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures. https://www.gostinfo.ru/catalog/Details/?id=3915529.
14 Trusted Computer Systems Evaluation Criteria, TCSEC https://csrc.nist.gov/csrc/media/publications/conferencepaper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf.