КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (9), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.9.3744
УДК 004

Черниш Юлія Олександрівна
старший науковий співробітник
Військовий інститут інформаційно-телекомунікаційних технологій, Київ, Україна
ORCID: 0000-0002-6626-5656
kobernikoi@ukr.net

Мальцева Ірина Робертівна
старший науковий співробітник
Військовий інститут інформаційно-телекомунікаційних технологій, Київ, Україна
ORCID: 0000-0001-6073-4637
irenagold2402@gmail.com

Паламарчук Наталія Анатоліївна
начальник науково-дослідної лабораторії
Військовий інститут інформаційно-телекомунікаційних технологій, Київ, Україна
ORCID: 0000-0001-8818-7794
palam_sv@ukr.net

АНАЛІТИКА ПРОБЛЕМАТИКИ ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Анотація. З розширенням сфери застосування електронних документів та електронного цифрового підпису у учасників електронного документообігу та правозахисних організацій виникає все більше складнощів і питань. Питання використання електронних документів продовжують цікавити науковців різних країн світу, багато проблем залишилися все ще не розв'язаними. Проблеми впровадження електронного цифрового підпису лежать у площині забезпечення збереження і цілісності електронних документів, підтверджених електронним цифрованим підписному, і можливості забезпечення судового захисту прав учасників електронного документообігу. Не менш нагальними питаннями є проблеми використання електронних ключів та розгляд основних напрямів вдосконалення їх використання в системі документообігу Збройних сил України, можливості використання електронного цифрового підпису під час електронного документування в діяльності ЗСУ та використання альтернативних методів ідентифікації особистості при підписанні електронних документів. Упровадження електронних систем обміну даними у всіх галузях, відкриває можливість застосування величезної гнучкості в обробці та зберіганні інформації, а також змушує працювати швидше та з більшою ефективністю — приймати рішення відповідно до швидкої зміни ситуації в режимі реального часу. Також, величезне значення для забезпечення конфіденційності інформації мають криптографічні системи захисту даних. Їх застосування забезпечує конфіденційність документа навіть у разі його потрапляння до рук сторонньої особи. Немає шифрів, які не можна було б зламати — це лише питання часу і коштів. Ті алгоритми, які ще кілька років тому вважалися надійними, сьогодні вже можуть бути скомпрометованими. Незважаючи на солідний пакет нормативно-правових актів щодо забезпечення безпаперових процедур документообігу, суттєвою проблемою залишається відсутність певних норм щодо здійснення електронного діловодства.

Ключові слова: електронний цифровий підпис; електронний документ; органи державної влади; центр сертифікації ключів; ідентифікація особистості; ключі.

1. ВСТУП

Постійне збільшення кількості інформації, необхідної для прийняття адекватних управлінських рішень, призводить до того, що традиційні методи роботи з документами стають все більше нерентабельними. За даними дослідження паперовий документообіг в компаніях з кожним роком зростає приблизно на 15-25%, близько 30% часу робочих груп витрачається на пошуки та узгодження документів, 6% документів безповоротно губляться, кожен внутрішній документ копіюється до 20 разів, в середньому кожен співробітник витрачає 150 годин на рік на пошук втраченої інформації, що в результаті призводить до значного зниження продуктивності праці персоналу компаній [1]. Такого роду проблеми можна вирішити за допомогою впровадження систем електронного документообігу з електронним цифровим підписом. Традиційні методи, які відрізняються високим ступенем емпіризму, в сучасному документаційному забезпеченні управління себе вже не виправдовують. Питання використання електронних документів продовжують цікавити науковців різних країн світу, й нині, незважаючи на прийняття цілого ряду законодавчих актів у цій галузі, багато проблем залишилися все ще не розв'язаними і потребують додаткового регулювання як на законодавчому, так і на нормативно-методичному рівні.

Постановка проблеми. У зв'язку із масовим збільшенням кількості одиниць документообігу стала нагальною потреба автоматизації існуючих систем документообігу та переходу на електронний документообіг - високотехнологічний і прогресивний підхід до суттєвого підвищення ефективності роботи з документами [2]. Впровадження систем електронного документообігу викриває основні проблеми пов'язані з особливостями електронного документообігу, правовим статусом електронного документу та необхідністю впровадження електронного цифрового підпису.

Аналіз останніх досліджень і публікацій. Розробці практичних рекомендацій щодо розвитку національних інфраструктур електронного цифрового підпису (ЕЦП) присвячено багато праць вітчизняних науковців і дослідників різних структур суспільства. Значний вклад знань з питання впровадження інфраструктур ЕЦП у банківській сфері внесли такі дослідники: І.Івченко, С. Левшаков, А. Савченко, В. Степаненко. Дослідженню питань теорії та практики аналізу, синтезу та застосування ЕЦП присвячено роботи науковців: М. Бондаренко, І. Горбенко, Ю. Горбенко, В. Онопрієнко, А. Потій, С.Черних. В роботах науковців С. Бєлова і С.Мартиненка обґрунтовано моделі побудови національної інфраструктури центрів сертифікації ключів та аналізуються їх ризики.

Мета статті. Метою даної статті є аналіз проблем використання електронних ключів та розгляд основних напрямів вдосконалення їх використання в системі документообігу Збройних сил України. Аналіз можливостей використання електронного цифрового підпису під час електронного документування в діяльності ЗСУ та використання альтернативних методів ідентифікації особистості при підписанні електронних документів.

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Роки паперового діловодства створили своєрідну систему як у цивільних, так і силових структурах нашої держави. Одним із багатьох недоліків цієї системи є необхідність оперування фізичними об'єктами, що значно сповільнює більшість

пов'язаних між собою процесів (виробництво, обмін інформацією, прийняття рішень, надання послуг тощо). Побудова досконалішої системи в інформаційному суспільстві, тобто у віртуальному світі, має базуватися на найкращих здобутках «паперового світу» при одночасній мінімізації його недоліків. Цей підхід дасть можливість спростити й пришвидшити перехід на новий етап розвитку електронного документообігу — електронного діловодства. Упровадження електронних систем обміну даними у всіх галузях, а особливо в силових структурах країни, відкриває можливість застосування величезної гнучкості в обробці та зберіганні інформації, а також змушує організації чи структури працювати швидше та з більшою ефективністю — приймати рішення командирами та віддавати накази відповідно до швидкої зміни ситуації в режимі реального часу. У Міністерстві оборони України та всіх підпорядкованих йому підрозділах уже протягом кількох років використовується система обміну даними, але це одна з декількох систем, які на цей час інтегруються в життя нашої армії. Також існує система обліку рухомого та нерухомого майна, великої кількості робочого обладнання та засобів, які забезпечують виконання завдань за призначенням тих чи інших підрозділів. Уже сьогодні використання таких систем обміну даними є вкрай необхідним для подальшого існування у цифровому світі. Адже швидкість прийняття правильного рішення є запорукою успіху виконання поставлених бойових завдань та збереження життя військовослужбовців. Ці технології також дають можливість підвищити ефективність роботи та економити час у повсякденній діяльності. І ми вже стоїмо на порозі впровадження подібних систем у повсякденну діяльність, наприклад, управління різними підрозділами, віддання наказів на всіх рівнях — від тактичного до стратегічного. Використання новітніх технологій, спрямованих на збільшення ефективності роботи, водночас породжує нові ризики, які можуть призводити до розкриття службової або чутливої інформації. І якщо ця інформація є власністю держави та належить до певних силових структур, то наслідки можуть бути катастрофічними.

Військові підрозділи в усьому світі вже активно використовують захищені системи обміну даними і майже зовсім відмовилися від дідівського методу — паперового діловодства. Останніми роками попит на системи обміну інформацією в Україні інтенсивно збільшувався, але ще не всі усвідомили цінність його впровадження і постійного використання. Головним рушійним механізмом цього прогресу мають бути власники інформації — командири чи начальники підрозділів, які ставлять вимоги перед працівниками чи службовцями щодо використання цих систем.

Прикладом цього є Збройні Сили України — інтенсивний користувач системами обміну даними, тому що має тисячі локальних мережевих адресатів, які існують у сотнях систем обміну даними та якими користується велика кількість людей щодня. Усі ці елементи систем є необхідними артеріями для правильного функціонування, ефективного управління та прийняття рішень, які, у свою чергу, приносять бажані результати. Однак, упроваджуючи системи обміну даними, не можна забувати про їх безпеку, адже бажаючих мати доступ до чужих документів більше, ніж ми можемо уявити. Для кращого розуміння, як захистити комп'ютерні мережі, мережеві пристрої та операційні системи з їх файловими системами, розглянемо більш докладно системи обміну даними.

Будь-яка система, що претендує на звання «захищеної», має включати механізм захисту для: забезпечення збереженості документів, забезпечення безпечного доступу, забезпечення достовірності документів, протоколювання дій користувачів. Ці вимоги є

основою безпеки для будь-якої системи, і якщо всіх цих критеріїв буде дотримано, то ми зможемо зберігати інформацію в цілковитій безпеці.

Величезне значення для забезпечення конфіденційності інформації мають криптографічні системи захисту даних. Їх застосування забезпечує конфіденційність документа навіть у разі його потрапляння до рук сторонньої особи. Але не варто забувати, що будь-який криптографічний алгоритм має таку властивість як криптостійкість, тобто і його захист має певну межу. Немає шифрів, які не можна було б зламати — це лише питання часу і коштів. Ті алгоритми, які ще кілька років тому вважалися надійними, сьогодні вже можуть бути скомпрометованими.

На сьогодні основним і практично єдиним із запропонованих на ринку рішенням для забезпечення достовірності відправника документа є електронно-цифровий підпис (ЕЦП). Основний принцип роботи ЕЦП заснований на використанні стандартів шифрування за допомогою відкритого ключа. Слід зауважити, що ключі для шифрування і розшифрування даних різні. Є закритий ключ, який дозволяє шифрувати інформацію, він зберігається тільки у власника, а є відкритий ключ, за допомогою якого можна перевірити справжність підпису, отриманого листа, він може поширюватися публічно.

Підтвердження належності відкритих ключів конкретним особам здійснює акредитований центр сертифікації ключів — спеціальна організація або підрозділ у Збройних Силах України, що є гарантом надійності та захисту криптографічних ключів. Звернення до центрів сертифікації дає можливість кожному користувачеві переконатися, що наявні в нього копії відкритих ключів, які використовуються, дійсні і належать йому.

Вирішення проблеми авторства безпаперового документа може бути досягнуто лише з використанням електронного цифрового підпису, що визначається Л. А. Сисоєвою як "… засіб, що дозволяє на основі криптографічних методів надійно встановити авторство і справжність документа" [2, 47].

Закон Україні «Про електронні довірчі послуги», що набув чинності 7 листопада 2018 року (далі – Закон №2155) більше нагадує технічний норматив, ніж, власне, закон. Враховуючи, що попередній Закон про ЕЦП мав схожий характер і сприймався як щось нішеве, є спокуса не надавати цій реформі великого юридичного значення [3]. Однак на сьогодні резонанс як самого закону, так і теми електронної ідентифікації взагалі може бути іншим. На відміну від попереднього десятиліття, ідентифікація клієнтів і контрагентів стає суттєво більш важливим аспектом для багатьох видів діяльності. По-перше, оскільки комерційна діяльність, у найширшому сенсі, стає усе більш інтернет-залежною, а бізнес-відносини – усе більш дистанційними. По-друге, оскільки бізнеси зобов'язані ідентифікувати всіх, з ким мають справу з усе зростаючою ретельністю й з усе зростаючою відповідальністю за недотримання вимог щодо ідентифікації. Таким чином, є ймовірність, що в осяжному майбутньому застосування технологій і практик, описаних у цій статті, стане необхідністю в повсякденних робочих буднях усіх керівних ланок Збройних сил України. У цьому випадку розуміння того, як працює інфраструктура електронних підписів, може стати так само важливим, як і вміння користуватися ноутбуком – як для юристів, так і для їх клієнтів.

Одним з найважливіших положень Закону №2155 є взаємне визнання українських та іноземних сертифікатів відкритих ключів та електронних підписів.

Законом запровадились такі механізми, як електронна ідентифікація, електронний підпис, електронна печатка, електронна позначка часу, реєстрована електронна доставка, інтероперабельність тощо.

Згідно з ч.2 ст. 22 Закону № 2155 ідентифікація фізичної особи, яка звернулася за отриманням послуги формування кваліфікованого сертифіката відкритого ключа, здійснюється за умови її особистої присутності за паспортом громадянина України або за іншими документами, які унеможливлюють виникнення будь-яких сумнівів щодо особи, відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи [3].

Схема електронної ідентифікації буде встановлювати високий (використання кваліфікованих електронних підписів і печаток), середній (використання вдосконалених електронних підписів і печаток) або низький рівень довіри до використовуваних засобів електронної ідентифікації.

Отже, починаючи з 07.11.2018р., отримати послуги з формування кваліфікованих сертифікатів відкритих ключів за довіреністю (в т.ч. посвідченою нотаріально) буде неможливо. Мета таких змін — «автоматизувати» взаємовідносини осіб та замінити печатки й купи паперових договорів [3]. Отже, Закон № 2155 регулює правові відносини, що виникають між юридичними, фізичними особами, суб'єктами владних повноважень у процесі надання, одержання електронних довірчих послуг.

Проте допускається ідентифікація фізичної особи кваліфікованим надавачем електронних довірчих послуг за ідентифікаційними даними, що містяться у раніше сформованому ним кваліфікованому сертифікаті відкритого ключа, за умови чинності цього сертифіката (ч. 3 ст. 22 Закону № 2155) [3].

Скасуванню підлягає Закон України «Про електронний цифровий підпис», проте фундаментальні положення цього закону були інкорпоровані у законопроекті. Так використання електронних довірчих послуг не змінює порядку вчинення правочинів, встановленого законом. Поряд із цим свою інтерпретацію віднайшла і норма, що електронний підпис чи печатка не може бути визнаним недійсним та позбавленим можливості розглядатись як доказ у судових справах виключно на тій підставі, що він має електронний вигляд або не відповідає вимогам до кваліфікованого електронного підпису чи печатки.

Варто зазначити, що Закон № 2155 загалом інтегрує в собі всі попередні здобутки у сфері застосування електронного цифрового підпису, бо створює базу унікальних цифрових «ключів», які закріплені за кожним суб'єктом відносин.

Крім того, не варто забувати про організаційні заходи щодо захисту інформації. Якою б ефективною не була криптографія, ніщо не завадить третій особі прочитати документ, наприклад, стоячи за плечима людини, яка має доступ до нього. Або розшифрувати інформацію, скориставшись ключем, недбало кинутим у стіл співробітником. Для збереження електронно-цифрового підпису потрібно: використовувати лише захищенні носії інформації, а не диски чи флешки, з яких найпростіше можна скопіювати закритий чи відкритий ключ, що там знаходиться; конверти з паролем до ЕЦП потрібно зберігати в особистому сейфі, до якого має доступ лише власник підпису, а не класти відкритий конверт із паролем під скло свого робочого столу; виконувати всі вимоги політики безпеки системи, своєчасно змінювати паролі і не забувати про вищезазначені пункти; якщо виникають певні несправності, то не слід самому намагатися щось виправити, а необхідно покликати на допомогу кваліфікованих осіб.

ISSN 2663 - 4023

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Як бачимо, використання електронного цифрового підпису має безліч проблем та деякі взагалі не вирішені питання, що суттєво впливають на можливість її використання. З огляду на вищеперераховане пропонується розглянути як альтернативний принципово новий метод засвідчення особистості під час підписання електронних документів на основі біометричних засобів ідентифікації, що базується на фізіологічних характеристиках людини, тобто на унікальних характеристиках, даних йому від народження – малюнку папілярних ліній пальців. Біометрія дозволяє незаперечно ідентифікувати особистість, і цю інформацію неможливо підробити або виправити.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Ткачев А.В. *Правовой статус компьютерных документов: Основные характеристики*. Москва.: ООО "Городец-издат", 2000. с. 8.

[2] Сысоева Л. "Проблемы организации электронного визирования документов в системах электронного документооборота", *Делопроизводство*, № 2, с. 47, 1998.

[3] Верховна Рада України. 7 сесія, (2017, 5 грудня). *Закон Українни № 2155,* "*Про електронні довірчі послуги*" [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

[4] Наказ Державного департаменту з питань зв'язку та інформатизації Міністерства транспорту та зв'язку України №70 (2005 7 червня), *"Система електронного документообігу органу виконавчої влади. Технічні умови"* ТУ У 30.0-33240054-001:2005 [Електронний ресурс]. Режим доступу: http: // www. zakon.rada.gov.ua.

[5] Чирський Ю. Електронний цифровий підпис: правові аспекти застосування. *Довідник секретаря та офіс-менеджера*, № 1, с. 26–31, 2007.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (9), 2020
ISSN 2663 - 4023

Yuliia Chernysh
Senior Researcher
Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-6626-5656
kobernikoi@ukr.net

Irina Maltseva
Senior Researcher
Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID: 0000-0001-6073-4637
irenagold2402@gmail.com

Nataliya Palamarchuk
Head of Research Laboratory
Military Institute of Information and Telecommunication Technologies, Kyiv, Ukraine
ORCID: 0000-0001-8818-7794
palam_sv@ukr.net

ANALYSIS OF THE PROBLEMS OF USE OF ELECTRONIC RELIABLE SERVICES IN THE ARMED FORCES OF UKRAINE

Abstract. With the expansion of the scope of electronic documents and electronic digital signature, the participants of electronic documents and human rights organizations are increasingly faced with difficulties and questions. The use of electronic dokumenntiv still interested scientists around the world, many problems still remain unsolved. The problems of implementation of electronic digital signature lie in the plane of ensuring the preservation and integrity of electronic documents, confirmed by electronic digital signature, and the possibility of ensuring judicial protection of the rights of participants of electronic document circulation. No less urgent issues are the use of electronic keys and consideration of the main directions of improving their use in the document management system of the Armed Forces of Ukraine, the possibility of using electronic digital signatures in electronic documentation in the Armed Forces and the use of alternative methods of identity identification when signing electronic documents. The introduction of electronic data exchange systems in all industries, opens up the possibility of using great flexibility in processing and storing information, as well as makes you work faster and more efficiently - to make decisions in accordance with the rapidly changing situation in real time. Also, cryptographic data protection systems are of great importance for ensuring the confidentiality of information. Their use ensures the confidentiality of the document even if it falls into the hands of an outsider. There are no ciphers that cannot be broken - it's just a matter of time and money. Those algorithms that were considered reliable a few years ago can now be compromised. In spite of a solid package of legal acts for the provision of paperless document circulation procedures, the absence of certain rules for the implementation of electronic records remains a significant problem.

Keywords: electronic digital signature; electronic document; public authorities; key certification center; identity of the person; keys.

REFERENCES

[1] Tkachev L. V. *Pravovnoy status komp'yuternykh dokumeнntov: osnovnnye kharakнterystyky*. Moscow.: "Gorodets-publisher", 2000. – p. 8.

[2] Sysoeva L. "Problemy orhanyzatsyy élektronnoho vyzyrovanyya dokumentov v systemakh élektronnoho dokumentooborota", *Deloproyzvodstvo*, № 2, p. 47, 1998.

[3] Verkhovna Rada Ukrayiny. 7th session, (2017, December 5). Zakon Ukrayinny *№ 2155,* " Pro elektronni dovirchi posluhy".[Electronic resource]. Access mode: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

[4] Order of the State Department for Communications and Informatization of the Ministry of Transport and Communications of Ukraine №70 (2005, June 7), *"Systema elektronnoho dokumentoobihu orhanu vykonavchoyi vlady. Tekhnichni umovy"* TU U 30.0-33240054-001: 2005. [Electronic resource]. Access mode: http: // www. zakon.rada.gov.ua.

[5] Chyrs′kyy YU. Elektronnyy tsyfrovyy pidpys: pravovi aspekty zastosuvannya. *Dovidnyk sekretarya ta ofis-menedzhera*, № 1, p.. 26–31, 2007.