УДК 004.91

Borys Horlynskyi[1,2], Candidate of technical sciences, Principal research scientist
ORCID ID: https://orcid.org/0000–0002–9993–2427 ***e-mail:*** vjzgoxnf@gmail.com

Dmytro Bondarenko[2], Head of Department
ORCID ID: https://orcid.org/0009–0001–7815–6027 ***e-mail:*** dimbond@ukr.net

Nataliia Lysenko[2], Head of Division
ORCID ID: https://orcid.org/0009-0008-9935-7646 ***e-mail:*** natalka.lsnk@ukr.net

Tetiana Maslennykova[2], Candidate of pedagogical sciences, Associate professor, Deputy Head of Department
ORCID ID: https://orcid.org/0000–0001–6287–0878 ***e-mail:*** tmaslennykova@gmail.com

Pavlo Kurbet[1], Ph.D., Junior researcher scientist
ORCID ID: https://orcid.org/0000-0002-0612-3859 ***e-mail:*** tovsba@gmail.com

[1]Institute of Telecommunications and Global Information Space of the NASU, Kyiv, Ukraine
[2]State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Kyiv, Ukraine

RESEARCH THE PROBLEM OF USING ELECTRONIC SIGNATURE TO PROTECT INFORMATION WITH LIMITED ASSESS

Abstract. *The rapid development of electronic document management systems in the world creates real prospects for a complete abandonment of the use of paper documents.*

Currently, electronic document management systems are successfully operating in Ukraine, in which open information is processed. This is facilitated by the presence of a valid legislative framework. At the same time, the development of electronic document management systems containing information with limited access is hampered by the incompleteness of the legislative basis.

The purpose of the article is to present the main results of research work aimed at identifying problematic issues regarding the standardization of the use of electronic signatures to protect electronic documents containing information with limited access, processed in information and communication systems.

In order to eliminate fragmentation and complete the development of the legislative framework regulating electronic document flow containing information with limited access, it is proposed:

1) to develop a draft Procedure for the provision and use of electronic identification services and electronic trust services provided using information and communication systems when processing official information and information constituting a state secret, to approve it by departmental order and to coordinate it with the Ministry of Justice of Ukraine);

2) create (for several interested state bodies) experimental sections of the ICS for processing electronic documents containing official and secret information, and, in the process of comprehensive testing, investigate their operability, challenges in developing security profiles, possibilities of obtaining certificates, etc.

3) amend the Law of Ukraine "On Electronic Identification and Electronic Trust Services", as well as a number of regulatory legal acts regulating the handling of paper secret documents, providing for the concept of "electronic secret document" in them.

Keywords: *legislative framework, trust services, qualified electronic signature, qualified electronic seal, qualified certificate, qualified electronic time stamp, electronic document flow containing information with limited access.*

Б.В. Горлинський[1,2], Д.М. Бондаренко[2], Н.В. Лисенко[2], Т.А. Масленникова[2], П.М. Курбет[1]

[1]Інститут телекомунікацій і глобального інформаційного простору НАН України, м. Київ, Україна
[2]Державний науково–дослідний інститут технологій кібербезпеки та захисту інформації м. Київ, Україна

ДОСЛІДЖЕННЯ ПРОБЛЕМАТИКИ ВИКОРИСТАННЯ ЕЛЕКТРОННОГО ПІДПИСУ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Анотація. *Бурхливий розвиток систем електронного документообігу у світі створює реальні перспективи повної відмови від використання паперових документів.*

На поточний час в Україні успішно функціонують системи електронного документообігу, в яких обробляється відкрита інформація. Цьому сприяє наявність чинної законодавчої бази. Разом з тим, розвиток систем електронного документообігу, що містить інформацію з обмеженим доступом, стримується незавершеністю законодавчих підстав.

Метою статті є викладення основних результатів науково-дослідної роботи, спрямованої на визначення проблемних питань щодо унормування використання електронного підпису для захисту електронних документів, які містять інформацію з обмеженим доступом, що обробляються в інформаційно-комунікаційних системах.

Для усунення фрагментарності та завершення розбудови законодавчої бази, яка регламентує електронний документообіг, що містить інформацію з обмеженим доступом, запропоновано:

1) розробити проєкт Порядку надання та використання послуг електронної ідентифікації та електронних довірчих послуг, які надаються за допомогою інформаційно-комунікаційних систем при обробленні службової інформації та інформації, що становить державну таємницю, затвердити його наказом Адміністрації Держспецзв'язку та погодити з Міністерством юстиції України;

2) створити (декільком зацікавленим державним органам) дослідні ділянки ІКС для оброблення електронних документів, що містять службову та секретну інформацію, та, у процесі всебічних випробувань, дослідити їх роботоспроможність, виклики при розробленні профілів безпеки, можливості отримання сертифікатів тощо;

3) внести зміни до Закону України "Про електронну ідентифікацію та електронні довірчі послуги", а також низки нормативно-правових актів, що регламентують поводження з паперовими секретними документами, передбачивши в них поняття "електронний секретний документ".

Ключові слова: *законодавча база, довірчі послуги, кваліфікований електронний підпис, кваліфікована електронна печатка, кваліфікований сертифікат, кваліфікована електронна позначка часу, електронний документообіг, що містить інформацію з обмеженим доступом.*

https://doi.org/10.32347/2411-4049.2026.2.219-229

Вступ

На сучасному етапі розвитку світових комп'ютерних технологій сформувалася стійка тенденція заміни паперового документообігу електронним. Це створює цілком реальні перспективи повної відмови від паперових документів (у тому числі, і у сфері повсякденної діяльності державних органів).

Наразі, процеси цифровізації документообігу не завжди зменшують трудовитрати чи вивільняють переконливу кількість персоналу, але високі темпи розвитку цієї сфери зміцнюють впевненість у тому, що, у найближчій перспективі, ця передова технологія буде використовуватися повсюдно і, у кінцевому підсумку, забезпечить оптимізацію процесів управління, зменшення трудовитрат та кількості зайнятого персоналу, а також економію витрат на доставку і збереження електронних документів.

У той же час, система секретного документообігу, наразі, залишається паперовою.

Незважаючи на багаторічну відпрацьованість та надійність системи паперового секретного документообігу, вона морально та технічно застаріла і, загалом, потребує кардинального осучаснення шляхом автоматизації процесів створення, затвердження, доставки та зберігання документів.

Стримувальним фактором, який, наразі, впливає на розвиток системи секретного документообігу, є відсутність законодавчої бази, що не дає можливості реалізувати відповідні інформаційно-комунікаційні системи (ІКС). Зокрема, чинним законодавством не врегульовано питання щодо використання, під час поводження з інформацією з обмеженим доступом, електронного підпису (чи електронної печатки).

Таким чином, на поточний час відсутність законодавчої бази щодо регламентації електронного секретного документообігу становить суттєву проблему, яка потребує свого вирішення.

Зважаючи на це, активізація пошуку шляхів вирішення проблеми створення законодавчої бази, яка б унормувала процеси електронного секретного документообігу, що містить інформацію з обмеженим доступом, є актуальним та своєчасним завданням.

Аналіз останніх досліджень і публікацій. На поточний час напрацьований великий обсяг законодавчих актів, які регулюють електронний документообіг. Зокрема, у Законі України [1] наводиться перелік чинної законодавчої бази про електронні документи та електронний документообіг, а також встановлюються правові засади створення, використання, передачі та зберігання електронних документів, які надають їм юридичну силу ідентичну з паперовими.

Важливим кроком у цифровізації держави, яким, загалом, завершується створення законодавчих підстав щодо підтримки електронного документообігу, що містить відкриту інформацію, є Закон України [2]. Цим Законом України визначаються правові та організаційні засади надання електронних довірчих послуг, права та обов'язки суб'єктів правових відносин у сфері електронних довірчих послуг, порядок здійснення державного нагляду за дотриманням вимог законодавства у сфері електронних довірчих послуг, а також правові та організаційні засади здійснення електронної ідентифікації.

Постановою Кабінету Міністрів України [3] затверджено порядок (процедуру) авторизації з безпеки і порядок розроблення та затвердження профілів безпеки (визначають механізми розроблення та затвердження базових, галузевих та цільових профілів безпеки) інформаційних, електронних комунікаційних, ІКС, технологічних систем.

Наказом Адміністрації Держспецзв'язку [4] (опубліковано на офіційному веб-сайті) оприлюднено базовий профіль безпеки інформації для ІКС, де обробляється відкрита та службова інформація, з урахуванням якого повинні розроблятися галузеві цільові профілі безпеки інформації (базовий профіль безпеки секретної інформації надається у встановленому порядку).

Постановою Кабінету Міністрів [5] затверджено Порядок функціонування Національної електронної комунікаційної мережі (НЕКМ), який, у свою чергу, унормовує функціонування мереж та систем спеціального зв'язку, призначених для обміну інформацією, що становить державну таємницю у межах території України між різними типами користувачів.

Формулювання мети статті. Метою статті є викладення основних результатів науково-дослідної роботи, виконаної Державним науково-дослідним інститутом технологій кібербезпеки та захисту інформації, спрямованої на визначення проблемних питань щодо унормування використання електронного підпису для захисту електронних документів, які містять інформацію з обмеженим доступом, що обробляються в інформаційно-комунікаційних системах.

Виклад основного матеріалу дослідження

Носіями інформації при безпаперовому діловодстві являються електронні документи. Законом України [1] це поняття визначено наступним чином: електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. При цьому, електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму.

Однією із основних проблем при створенні електронного документа є ідентифікація автора. У якості основного засобу ідентифікації автора електронного документа використовується електронний підпис (електронні дані, що додаються до інших електронних даних або логічно з ними пов'язуються і використовуються підписувачем як підпис).

Важливою проблемою при створенні електронного документа є забезпечення довіри до того, що це оригінал документа, який несанкціоновано не змінений після накладання електронного підпису. Ключовою ознакою, що характеризує довіру до електронного документа є його цілісність. Саме ця ознака гарантує, що електронний документ не було змінено після моменту створення (наприклад, у процесі доставки чи зберігання). Іншими словами, можна сказати, що цілісність відіграє роль певного "цифрового замка", який виходить з ладу при несанкціонованому поводженні з електронним документом.

У загальному випадку, електронний підпис, окрім ідентифікації автора електронного документа, слугує також і засобом підтвердження його цілісності.

Крім того, для забезпечення достовірності походження пов'язаних електронних даних, зокрема, для засвідчення електронних підписів підписувачів на електронних документах, або для засвідчення відповідності копій документів оригіналам та виявлення порушення цілісності може використовуватися також електронна печатка (електронні дані, що додаються до інших електронних даних або логічно з ними пов'язуються).

Таким чином, створення електронного документа завершується накладанням електронного підпису та/або електронної печатки (фізично це відбувається шляхом доповнення обсягу електронного документа даними електронного підпису та електронної печатки).

Законом України [2] конкретизовано поняття "електронний підпис", зокрема, визначено два його різновиди, які відрізняються рівнями безпеки та довіри: удосконалений електронний підпис (УЕП), що базується на кваліфікованому сертифікаті електронного підпису, та кваліфікований електронний підпис (КЕП).

Удосконалений електронний підпис, що базується на кваліфікованому сертифікаті електронного підпису – удосконалений електронний підпис, що створюється з використанням кваліфікованого сертифіката електронного підпису, виданого кваліфікованим надавачем електронних довірчих послуг, та не містить відомостей про те, що особистий ключ зберігається у засобі кваліфікованого електронного підпису. Він має середній рівень захисту, але дозволяє ідентифікувати підписувача (його часто використовують для повсякденних дій, наприклад, надання звітності підприємцями).

Кваліфікований електронний підпис – удосконалений електронний підпис, що створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті електронного підпису. КЕП має найвищий рівень захисту і забезпечує надійну ідентифікацію підписувача та цілісність даних. Кваліфікований електронний підпис має таку саму юридичну силу, як і власноручний підпис, та має презумпцію його відповідності власноручному підпису. Кваліфікована електронна печатка має презумпцію цілісності електронних даних і достовірності походження електронних даних, з якими вона пов'язана.

Електронний підпис та електронна печатка дають можливість організувати і підтримувати електронний документообіг у розумінні сукупності процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, що виконуються із застосуванням перевірки цілісності, ідентифікації автора та, у разі необхідності, з підтвердженням факту одержання таких документів.

Забезпечення електронної взаємодії двох або більше суб'єктів відбувається шляхом надання електронних довірчих послуг надавачем електронних довірчих послуг, якому ці суб'єкти довіряють.

Надавачі електронних довірчих послуг зобов'язані забезпечувати: відповідність засобів електронної ідентифікації встановленим рівням довіри, захист персональних даних користувачів, захист інформації і ІКС, що використовується для надання послуг електронної ідентифікації, здійснення ідентифікації фізичних та юридичних осіб під час надання послуг електронної ідентифікації, інформування користувачів про порушення конфіденційності та/або цілісності інформації, що впливають на надання їм послуг електронної

ідентифікації, постійне зберігання документів та електронних даних, отриманих під час реєстрації користувачів засобів електронної ідентифікації.

Статтею 16 Закону України [2] також визначаються вимоги до електронних довірчих послуг та їх склад. Зважаючи на різні рівні довіри, вони можуть бути як просто електронні довірчі послуги (забезпечують середній рівень довіри), так і кваліфіковані електронні довірчі послуги (забезпечують високий рівень довіри).

Таким чином, можна прийти до висновку, що законодавча база щодо проблематики використання електронного підпису та інших електронних засобів, які покликані підтвердити особу користувача, а також цілісність інформації, що циркулює в ІКС, загалом, напрацьована. На поточний час це дає можливість створити та забезпечити достатньо успішне функціонування низки загальнодержавних застосунків (наприклад, загальновідомий застосунок "Дія").

Що стосується системи секретного документообігу, то частиною 2 статті 2 вищеозначеного Закону України [2] наголошено, що цей Закон не поширюється на здійснення електронної ідентифікації та надання електронних довірчих послуг у системах, у яких обробляються службова інформація та державна таємниця, а також у системах, які використовуються виключно визначеною групою учасників на договірних засадах для внутрішніх потреб юридичних або фізичних осіб.

Проведений аналіз наявної законодавчої бази дає можливість зробити висновок, що, загалом, вона не унормовує документообіг електронних службових та секретних документів, а тому потребує уточнення.

Наразі, вважається, що кваліфікований електронний підпис, який базується на кваліфікованому сертифікаті електронного підпису, а також кваліфікована електронна печатка, що базується на кваліфікованому сертифікаті електронної печатки, є найбільш надійними засобами автентифікації користувача та підтвердження цілісності електронного документа. Тому, видається, що в ІКС забезпечення секретного електронного документообігу доцільно використовувати саме ці атрибути.

Разом з тим, для усунення вищеозначеної законодавчої прогалини щодо унормування суспільних відносин при наданні послуг електронної ідентифікації та електронних довірчих послуг доцільно розробити проєкт Порядку надання та використання послуг електронної ідентифікації та електронних довірчих послуг (Порядок), які надаються за допомогою ІКС при обробленні службової інформації та інформації, що становить державну таємницю.

При цьому, до проєкту Порядку доцільно включити:

положення щодо того, що в ІКС, призначених для оброблення службової інформації та інформації, що становить державну таємницю (Закриті системи), повинні застосовуватися кваліфіковані електронні довірчі послуги;

положення, що для надання кваліфікованих електронних довірчих послуг у Закритих системах повинні використовуватися кваліфіковані електронні підписи та печатки, а також електронні підписи та печатки, які базуються на кваліфікованих сертифікатах відкритих ключів;

схеми взаємодії Закритих систем з ресурсами кваліфікованого надавача;

положення щодо того, що рішення про застосування конкретної схеми приймає власник Закритої системи з урахуванням особливостей її функціонування;

вимоги до кваліфікованих надавачів під час надання кваліфікованих електронних довірчих послуг у Закритих системах;

вимоги до ідентифікації користувачів Закритих систем під час формування та видачі кваліфікованого сертифіката відкритого ключа;

рекомендації щодо вибору квантовостійких криптоалгоритмів.

При цьому, вимога щодо вибору квантовостійких алгоритмів пов'язана з викликами, які невдовзі виникнуть після створення потужних квантових комп'ютерів.

Для прискорення процесів прийняття нормативно-правового акту пропонується затвердити Порядок наказом Адміністрації Держспецзв'язку та зареєструвати його у Міністерстві юстиції України.

Зважаючи на те, що проєкт Порядку передбачає використання кваліфікованих електронних довірчих послуг, доцільно було б до Закону України [2] включити положення про те, що порядок оброблення інформації в ІКС, у яких обробляється службова інформація та інформація, що становить державну таємницю, розробляється Адміністрацією Держспецзв'язку.

Одним із основних завдань при забезпеченні функціонування Закритих систем є захист інформації. Згідно із Законом України [6] захист інформації в ІКС забезпечується її власником, зусилля якого повинні бути спрямовані на запобігання порушенню цілісності, конфіденційності і доступності інформації. Важливо, що об'єктами захисту в ІКС є не тільки інформація, що обробляється в ній, а й програмне забезпечення, яке призначене для обробки цієї інформації.

Згідно з цим Законом України державні інформаційні ресурси повинні оброблятися в авторизованих системах з безпеки або системах, які мають сертифікати відповідності стандарту інформаційної безпеки та мають документальне підтвердження (рішення) щодо можливості функціонування, зважаючи на їх відповідність вимогам законодавства, національним стандартам та нормативним документам у сферах:

технічного захисту, що включає комплекс інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації;

криптографічного захисту, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування, відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

кіберзахисту, як взаємопов'язаної сукупності організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на захист від кіберзагроз, забезпечення кібербезпеки, стійкості, цілісності, доступності та конфіденційності інформаційних ресурсів у кіберпросторі, а також здатності інфраструктури до їх обробки.

Інформація, що становить державну таємницю, має оброблятися у системі, об'єкті критичної інфраструктури із застосуванням комплексу технічного захисту інформації з підтвердженою відповідністю та за умови використання засобів криптографічного захисту суб'єктів господарювання, які провадять ліцензовану діяльність відповідно до законодавства.

Програмне забезпечення, що забезпечує функціонування інформаційних, електронних, комунікаційних, інформаційно-комунікаційних та технологічних систем, в яких обробляється інформація, що становить державну таємницю, використовується також за умови проведення державної експертизи у сфері захисту інформації.

Авторизація з безпеки, а також підтвердження дотримання вимог з безпеки систем, в яких обробляються державні інформаційні ресурси, здійснюється у відповідності до порядку, затвердженого постановою Кабінету Міністрів України [3]. Згідно з цим порядком для ІКС розробляється три різновиди профілів безпеки:

базовий профіль безпеки – мінімальні вимоги з безпеки інформації та взаємопов'язана сукупність заходів щодо її захисту, які встановлюються залежно від інформації (відкрита інформація чи інформація з обмеженим доступом), або функціонального призначення такої системи;

галузевий профіль безпеки – взаємопов'язана сукупність заходів щодо захисту інформації, визначених органом державної влади у межах своїх повноважень у відповідній сфері або галузі (для відповідної категорії систем), залежно від інформації, що обробляється, з урахуванням базового профілю;

цільовий профіль безпеки системи – взаємопов'язана сукупність заходів із захисту інформації, визначених власником або розпорядником для відповідних систем з урахуванням базового та галузевого профілів, вимог законодавства та національних стандартів у сферах криптографічного та технічного захисту інформації, кіберзахисту, а також політик безпеки, призначення системи, її структурно-функціональних характеристик та особливостей функціонування, результатів проведеної оцінки (аналізу) ризиків безпеки.

Вищезазначеною постановою Кабінету Міністрів України визначені також процедурні особливості авторизації з безпеки для систем електронного документообігу, що не містять та містять інформацію з обмеженим доступом. Зокрема, авторизація з безпеки здійснюється для систем, щодо яких затверджено цільовий профіль. Під час розроблення та затвердження цільового профілю власник або розпорядник системи самостійно обирає національні стандарти у сферах технічного та криптографічного захисту інформації, кіберзахисту, засоби і методи здійснення таких заходів.

Оприлюднений базовий профіль безпеки [4] містить конкретні вимоги до побудови та експлуатації систем електронного документообігу, що містить відкриту та службову інформацію (базовий профіль безпеки для систем електронного документообігу, що містять секретну інформацію, надається встановленим порядком).

У загальному випадку до базового профілю з безпеки включені вимоги до побудови та управління системою, персоналу, порядку взаємодії з користувачами, оцінки та моніторингу безпеки, способів реагування на інциденти, методи фізичного захисту щодо доступу, методи забезпечення цілісності системи та інформації, перевірок системи тощо, покликані забезпечити безпеку оброблення інформації.

Що стосується регламентації чинними нормативно-правовими актами передавання інформації з обмеженим доступом, то згідно з чинним законодавством, замість використання комунікаційних мереж загального користування, рекомендується використання Національної електронної комунікаційної мережі (НЕКЗ) [5], як захищеної системи передавання інформації.

Типовим кроком при створенні будь-якої складної ІКС є попереднє розроблення її дослідної ділянки. Саме у процесі створення та дослідної експлуатації дослідної ділянки ІКС можна відпрацювати велику кількість проблемних питань, які б могли суттєво ускладнити побудову повноцінної ІКС. Тому реалізація етапу експериментального відпрацювання ІКС видається безальтернативною.

Також з метою унормування порядку поводження із секретними електронними документами в ІКС електронного секретного документообігу необхідно визначити поняття “електронний секретний документ” в нормативно-правових актах, що унормовують поводження з секретними паперовими документами.

Таким чином, реалізація вищеозначених кроків може стати ключовим фактором у питанні розблокування напряму електронного секретного документообігу і дасть можливість започаткувати створення відповідних ІКС.

Науково-дослідна робота, висвітлена в цій статті, була завершена в серпні 2025 року.

Слід зазначити, що станом на лютий 2026 року прийняті наступні нормативні документи:

26 листопада 2025 року Кабінет Міністрів України затвердив нову редакцію постанови № 373, згідно з вимогами якої створення та/або обробка в ІКС електронних документів, аналоги яких на паперових носіях повинні містити власноручний підпис відповідно до законодавства, здійснюються із застосуванням електронного підпису чи печатки відповідно до Закону України “Про електронну ідентифікацію та електронні довірчі послуги” або Порядку, перевірка електронного підпису чи печатки в ІКС, у яких обробляється службова інформація та/або інформація, що становить державну таємницю, проводиться з дотриманням вимог Порядку, електронна ідентифікація та автентифікація користувачів в ІКС здійснюється відповідно до вимог статті 14 Закону України “Про електронну ідентифікацію та електронні довірчі послуги”, Порядку та інших нормативно-правових актів у сферах електронної ідентифікації та електронних довірчих послуг.

28 січня 2026 року наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України № 67/ДСК, що зареєстрований в Міністерстві юстиції України від 09.02.2026 за № 174/45568, затверджено “Порядок надання та використання послуг електронної ідентифікації та електронних довірчих послуг, які використовуються в ІКС, в яких обробляються службова інформація та державна таємниця”.

Висновки та перспективи подальших досліджень

Розбудова законодавчої бази щодо забезпечення можливості створення систем електронного документообігу, що містить інформацію з обмеженим доступом, наразі не завершена. Зокрема, у нормативно-правових актах відсутнє поняття “електронний секретний документ” та не унормовано поводження з такими документами.

Для подальшого унормування питань щодо розвитку систем електронного документообігу, що містить інформацію з обмеженим доступом, видається доцільним вжити наступних заходів:

1) створити (можливо, декільком зацікавленим державним органам) дослідні ділянки ІКС для оброблення електронних документів, що містять службову та секретну інформацію, та, у процесі всебічних випробувань, дослідити їх роботоспроможність, виклики при розробленні профілів безпеки, можливості отримання сертифікатів тощо;

2) внести зміни до Закону України “Про електронну ідентифікацію та електронні довірчі послуги”, а також низки нормативно-правових актів, що регламентують поводження з паперовими секретними документами, передбачивши в них поняття “електронний секретний документ”.

Подальші дослідження доцільно спрямувати на розроблення проєктів законодавчих актів та їх всебічне відпрацювання.

СПИСОК ЛІТЕРАТУРИ

1. Закон України “Про електронні документи та електронний документообіг” від 22.05.2003 № 851-IV.
2. Закон України “Про електронну ідентифікацію та електронні довірчі послуги” від 05.10.2017 № 2155-VIII.
3. Постанова Кабінету Міністрів України “Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем” від 18.06.2025 № 712.
4. Наказ Адміністрації Держспецзв’язку від 24.06.2024 № 317 “Про визначення Базового профілю безпеки інформації”. https://www.cip.gov.ua/ua/doks/nakaz-administraciyi-derzhspeczv-yazku-vid-24-06-2024-317-pro-viznachennya-bazovogo-profilyu-bezpeki-informaciyi
5. Постанова Кабінету Міністрів України “Деякі питання функціонування Національної електронної комунікаційної мережі” від 16.12.2020 № 1358.
6. Закон України “Про захист інформації в інформаційно-комунікаційних системах” від 05.07.1994 № 80/94-ВР.

Стаття надійшла до редакції 22.01.2026, надійшла після рецензування 13.03.2026, прийнята 30.03.2026

REFERENCES

1. Verkhovna Rada of Ukraine. (2003, May 22). *Pro elektronni dokumenty ta elektronnyi dokumentoobih* [On electronic documents and electronic document circulation] (No. 851-IV).
2. Verkhovna Rada of Ukraine. (2017, October 5). *Pro elektronnu identyfikatsiiu ta elektronni dovirchi posluhy* [On electronic identification and electronic trust services] (No. 2155-VIII).
3. Cabinet of Ministers of Ukraine. (2025, June 18). *Deiaki pytannia zakhystu informatsiinykh, elektronnykh komunikatsiinykh, informatsiino-komunikatsiinykh, tekhnolohichnykh system* [Some issues of protection of information, electronic communication, information and communication, and technological systems] (No. 712).
4. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2024, June 24). *Pro vyznachennia bazovoho profiliu bezpeky informatsii* [On approval of the basic information security profile] (No. 317). https://www.cip.gov.ua/ua/doks/nakaz-administraciyi-derzhspeczv-yazku-vid-24-06-2024-317-pro-viznachennya-bazovogo-profilyu-bezpeki-informaciyi
5. Cabinet of Ministers of Ukraine. (2020, December 16). *Deiaki pytannia funktsionuvannia Natsionalnoi elektronnoi komunikatsiinoi merezhi* [Some issues of functioning of the National electronic communication network] (No. 1358).

6. Verkhovna Rada of Ukraine. (1994, July 5). *Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh* [On protection of information in information and communication systems] (No. 80/94-VR).

The article was received 22.01.2026, received after revision 13.03.2026, accepted 30.03.2026

Горлинський Борис Вікторович
кандидат технічних наук, головний науковий співробітник, Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України
Адреса робоча: Україна, м. Київ, вул. Чоколівський бульвар, 13
ORCID ID: https://orcid.org/0000–0002–9993–2427 ***e-mail:*** vjzgoxnf@gmail.com

Бондаренко Дмитро Михайлович
начальник центру, Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації
Адреса робоча: Україна, м. Київ, вул. М. Залізняка, 3, корпус 6
ORCID ID: https://orcid.org/0009–0001–7815–6027 ***e-mail:*** dimbond@ukr.net

Лисенко Наталія Володимирівна
начальник відділу, Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації
Адреса робоча: Україна, м. Київ, вул. М. Залізняка, 3, корпус 6
ORCID ID: https://orcid.org/0009-0008-9935-7646 ***e-mail:*** natalka.lsnk@ukr.net

Масленникова Тетяна Андріївна
кандидат педагогічних наук, доцент, заступник начальника центру, Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації
Адреса робоча: Україна, м. Київ, вул. М. Залізняка, 3, корпус 6
ORCID ID: https://orcid.org/0000–0001–6287–0878 ***e-mail:*** tmaslennykova@gmail.com

Курбет Павло Миколайович
доктор філософії (Ph.D.), молодший науковий співробітник, Інститут телекомунікацій і глобального інформаційного простору Національної академії наук України
Адреса робоча: Україна, м. Київ, вул. Чоколівський бульвар, 13
ORCID ID: https://orcid.org/0000-0002-0612-3859 ***e-mail:*** tovsba@gmail.com