УДК 002:001.1(100)
DOI: 10.31866/2616-7654.9.2022.259142

ЗАРУБІЖНИЙ ДОСВІД ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Марина Цілина,
доцентка кафедри документознавства та інформаційно-аналітичної діяльності Київського національного університету культури і мистецтв,
кандидатка філологічних наук, доцентка (Київ, Україна)
e-mail: macilin@ukr.net
ORCID: 0000-0001-5339-5147

Метою статті є з'ясувати набільш безпечні умови для функціонування документів, а також знайти найефективніші способи уникнення потенційних ризиків і небезпек у вітчизняному інформаційному просторі.

Методологію дослідження становила сукупність загальнонаукових та спеціальних методів студіювання проблематики. Оглядово-аналітичний метод було застосовано під час опрацювання фахової і профільної літератури та визначення теоретичного підґрунтя дослідження, системний метод виявився ефективним під час вивчення окремих зарубіжних практик гарантування конфіденційності інформації. Застосування методу індукції дало змогу провести узагальнення і зробити висновок стосовно можливості використання досвіду інших країн у межах українського інформаційного простору.

Спеціальні методи, а саме метод дослідження документних потоків та метод визначення інформативності документа, стали у пригоді у ході розгляду процесу переміщення документів в інформаційному полі, можливості/неможливості пошкодження чи втрати інформації та способів запобігання таких небажаних явищ.

Наукова розвідка ґрунтувалася на принципах об'єктивності та цілісності. Використання комплексу наукових методів дало змогу дослідити специфіку конфіденційної документної інформації, із якою працюють за кордоном, та з'ясувати основні загрози порушенню цілісності й доступності інформації.

Наукова новизна. Досліджено новітні практики Англії, Європейського Союзу та Сполучених Штатів Америки у сфері гарантування конфіденційності документа. Розглянуто основні рекомендації щодо захисту конфіденційної інформації, конфіденційні угоди, упроваджені за кордоном. Установлено особливості безпечного використання документної інформації. Запропоновано низку системних заходів проти загроз, що виникають у процесі роботи з конфіденційними документами.

Основні висновки. Проведене дослідження дає змогу стверджувати, що українську законодавчо-нормативну базу варто формувати з урахуванням світових законодавчих ініціатив і впроваджень. Фірмам, організаціям, установам, а також окремим особам необхідно забезпечити захист конфіденційності інформації, з огляду на загрози слід упровадити відповідні кроки задля гарантування безпечної роботи. Не слід також нехтувати правилами проведення ідентифікації та аутентифікації, використовувати жорстку політику паролів. Проблема захисту інформації вирішується тільки комплексно.

Ключові слова: автентифікація, доступність інформації, захист конфіденційної інформації, ідентифікація, угода про конфіденційність інформації, цінність документної інформації

ВСТУП

У сучасному глобалізованому світі все частіше постає проблема збереження інформації. Інколи ця тема може об'єднувати і на міжнародному рівні як зусилля законодавців, програмістів, керівників установ та організацій, так і співробітників цих структур, оскільки, з одного боку, є комплексною, а з іншого – саме пересічні працівники фірм і компаній можуть навіть через свою необачність чи недогляд порушувати цілісність, доступність інформації або сприяти її витоку. Тому нагальним завданням нині є запобігти подібним ситуаціям і втручанням у функціонування інформаційних систем.

Мета дослідження – на основі сучасних зарубіжних практик роботи з конфіденційною інформацією з'ясувати набільш безпечні умови для функціонування документів у вітчизняному інформаційному просторі, а також знаходити способи уникнення потенційних ризиків і небезпек.

ТЕОРЕТИЧНЕ ПІДҐРУНТЯ

Задля усебічного розгляду теми враховано різноаспектні підходи до створення системи захисту конфіденційної інформації. До уваги взято досвід Європейського Союзу, США та Англії. Так, законодавчо-правові основи роботи із конфіденційними даними розкрито у публікації Дж. Карбо (Carbo, 2020), тут також подано найкращі практики щодо того, як фірми, організації, установи й окремі особи мають забезпечити захист конфіденційності. Рекомендації щодо захисту конфіденційної інформації, створені на основі законодавчих актів Англії та введені до обігу не тільки у Великобританії, а й в інших країнах, детально простудійовано Д. Уокером (Wolker, 2016). Найпоширеніші загрози безпеці документів і системні заходи, котрі треба вжити проти них, охарактеризовано Е. Уакніним (Ouaknine, 2020). Сучасні виклики у сфері захисту персональних даних репрезентовано у посібнику із захисту персональних даних у Європейському Союзі, зокрема, подано основну термінологію, правила європейського права, ключові принципи захисту інформації (*Посібник з європейського права*, 2018). Крім цього, здійснено порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних в однойменній книзі В. М. Брижко, А. І. Радянської, М. Я. Швець (2006), де також опубліковано переклади законодавчих актів Європейського Союзу стосовно цієї теми. Однак з огляду на вже порушені проблеми все ж існує необхідність упорядкування теоретичної інформації і переміщення акцентів на практичну складову, бо саме незнання і невміння породжують надалі помилки у роботі з документною інформацією.

МЕТОДИ І МАТЕРІАЛИ

Результати дослідження ґрунтуються на використанні сукупності наукових методів, зокрема, аналізу, системного методу та індукції. Оглядово-аналітичний метод було застосовано під час опрацювання фахової і профільної літератури та визначення теоретичного підґрунтя дослідження, системний метод виявився ефективним під час вивчення окремих зарубіжних практик гарантування конфіденційності інформації. Застосування методу індукції дало змогу провести узагальнення і зробити висновок стосовно можливості використання досвіду інших країн у межах українського інформаційного простору.

Спеціальні методи, а саме метод дослідження документних потоків та метод визначення інформативності документа, стали у пригоді у ході розгляду процесу переміщення документів в інформаційному полі, можливості/неможливості пошкодження чи втрати інформації та способів запобігання таких небажаних явищ.

Використання комплексу наукових методів дало змогу встановити специфіку конфіденційної документної інформації, із якою працюють за кордоном, та з'ясувати основні загрози порушенню цілісності й доступності інформації.

Джерельну основу дослідження становили публікації у фахових і профільних виданнях, контент вебсайтів.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Закони про конфіденційність даних у Сполучених Штатах Америки створюються задля того, аби дати змогу особам зрозуміти типи, способи доступу або видалення даних, які компанії збирають про них. Мета законів про конфіденційність даних полягає у тому, щоб надати певний контроль над даними особи та забезпечити прозорість їх збирання та охорону.

До появи таких нормативних актів було важко зрозуміти, яка інформація збирається та як використовується, чи продавав вебсайт інформацію іншим компаніям. Окрім того, оплата послуги не є гарантією того, що ваша інформація не продається. Закони про конфіденційність даних намагаються вирішити ці проблеми, вимагаючи від компаній отримання позитивної згоди від окремих осіб, пояснення того, що збирається, та визначення мети використання.

Існує чимало проблем як для окремих людей, так і для компаній. Різні опитування показують, що кількість захищених паролем облікових записів на одну людину коливається від 25 до 90. Працівники організацій повинні бути обізнаними із різними законами про конфіденційність даних, які є чинними, та розробляти внутрішні межі для дотримання і захисту даних. Навіть якщо обидві сторони грають чесно, це також є складним викликом.

Так, наприклад, для компаній у США існує перелік правил щодо конфіденційності даних (Carbo, 2020):

– Закон США про конфіденційність 1974 р. – застосовується до державних установ, проте забезпечує належну основу і для інших організацій;

– Закон про перенесення та підзвітність медичного страхування – створений для захисту медичної інформації;

– Правила захисту конфіденційності дітей в інтернеті – створені для захисту інформації про дітей до 13 років;

– Закон Гремма-Ліча-Блейлі – вимагає від фінансових установ документально підтвердити, якою інформацією послуговуються та яким чином вона захищена;

– Закон про конфіденційність споживачів Каліфорнії – діє з січня 2020 року для захисту інформації громадян Каліфорнії;

– Загальний регламент захисту даних – Закон ЄС, який має глобальне значення;

– державні закони – кожен штат може мати власні закони про конфіденційність із невеликими змінами.

Закони про конфіденційність даних можна інтерпретувати по-різному, порівнювати і знаходити суперечності. Як і рамки безпеки та засоби контролю, зако-

ни про конфіденційність необхідно розглядати як мінімальну основу для захисту персональних даних. Фізичні особи та компанії повинні застосовувати здоровий підхід до захисту інформації, щоб заповнити прогалини, що існують у законах про конфіденційність даних. Вони мають розуміти, які відомості збираються, яке їх призначення і чи потрібно їх мати взагалі. Найкращий спосіб захистити інформацію – це взагалі не мати її, бо чого немає, того й не можна втратити. Це дає змогу звернути увагу на залишкові дані та їх захист.

Існує кілька найкращих практик щодо того, як фірми, організації, установи, окремі особи також мають забезпечити захист конфіденційності (Carbo, 2020).

1. Необхідно захищати усю зібрану інформацію.

Дотримуватись розумних заходів безпеки, щоб уберегти особисту інформацію осіб від неналежного та несанкціонованого доступу. Зменшити кількість зібраних даних лише до того, що необхідно для надання послуги. Щоб обмежити доступ до даних, використовувати керування доступом на основі ролей. Завжди шифрувати інформацію у стані спокою та під час транспортування. Створити надійну стратегію резервного копіювання та протестувати її, аби переконатися в цілісності та доступності.

2. Бути відкритими і чесними щодо того, як зібрана, використана інформація, ділитись особистою інформацією. Подумати про те, як люди можуть використати дані, і створити налаштування для захисту своєї інформації за замовчуванням. Дозволити людям користуватися інформацією та переглянути те, що зараз зберігається про них.

3. Виховувати довіру. Повідомити громадськості чітко і стисло, що означає конфіденційність для вашої організації, та упроваджувати заходи для досягнення і збереження конфіденційності. Це має бути зроблено за допомогою публічної політики конфіденційності, яка є доступною та зрозумілою. Політика повинна оновлюватися із розвитком законів про конфіденційність та внутрішніх процедур.

4. Особиста інформація – це як гроші, треба цінувати і захищати її. Така інформація, як, наприклад, історія покупок або місцезнаходження, також має цінність. Варто подумати про те, хто отримує такі відомості та як вони збираються через програми і вебсайти. Необхідно видаляти програми, що не використовуються, підтримувати іншими актуальними та переглядати дозволи додатків. Знати про те, які вебсайти чи програми надсилають запити, і чи є сенс користуватися послугою. Мати на увазі, що сайти та послуги можуть обмінюватися інформацією. Збір інформації з різних джерел може дати точний профіль людей.

5. Ділитися обережно. Подумати, перш ніж публікувати про себе та інших в інтернеті. Поміркувати, хто відкриє інформацію, зможе її побачити і як це можна сприймати зараз і в майбутньому. Інформація – це вдалий ресурс для атак соціальної інженерії.

6. Володіти своєю присутністю в інтернеті. Встановити параметри конфіденційності та безпеки на вебсайтах та у додатках відповідно до рівня комфорту для обміну інформацією. Кожен пристрій, програма чи вебперегляд, які використовують, мають різні функції для обмеження того, як і з ким можна ділитись інформацією. Завжди варто почати з найбільш обмежувальних налаштувань і повільно зменшувати обмеження, якщо це необхідно. Мета – знайти обмежувальну, але придатну для використання установку.

Якщо інформацію розміщено в мережі інтернет, вона залишається там назавжди. Закони про конфіденційність дають змогу особам вимагати видалення

персональних даних у певних компаній. Інформація видаляється з цієї компанії, але може бути доступна в іншому місці. Тому треба не покладатись на закони про конфіденційність для повного захисту інформації. Критично подумати, перш ніж ділитися особистою інформацією, зрозуміти, що збирається, і попросити видалити особисту інформацію, коли більше не треба користуватися послугою.

Існують також рекомендації щодо захисту конфіденційної інформації, створені на основі законодавчих актів Англії та можуть бути взяті до уваги та введені до обігу не тільки у Великобританії, а й в інших країнах (Wolker, 2016):

1. Знати, кому розкриваємо інформацію.

Якщо є занепокоєння щодо здатності особи зберігати конфіденційність інформації, не розкривати її саме цій людині. Навіть якщо знаємо особу одержувача і довіряємо його здатності зберігати інформацію конфіденційною. Професійні консультанти повинні повністю усвідомлювати та розуміти свої зобов'язання щодо конфіденційності, але інші люди, наприклад, працівники одержувача, можуть цього не робити. Чітко визначити, хто може, а хто не зможе отримати інформацію, і переконатися, що кожен, кому одержувач розкриває інформацію, також має юридичний обов'язок зберігати її конфіденційною.

2. Чітко позначити всю конфіденційну інформацію як «конфіденційну».

Це означає написати «конфіденційно» на документах або будь-якій папці, де вони зберігаються. Якщо надсилаємо електронний лист, треба переконатися, що заголовок чітко ідентифікує його як конфіденційний.

Коли передаємо комусь документи, варто повідомити, що інформація є конфіденційною і що розкривати її треба відповідно до умов угоди про конфіденційність. Якщо одночасно розкриваємо конфіденційну та неконфіденційну інформацію, робимо все окремо.

Якщо обговорюємо конфіденційну інформацію, необхідно дати зрозуміти, що ця інформація є конфіденційною, і її не варто дублювати.

3. Використовувати паролі та зашифровані файли для електронних документів.

Це допоможе уникнути випадкового розкриття чи допитливих очей, які дивляться на те, чого не повинні бачити. Надійність пароля або рівень шифрування, очевидно, змінюватимуться залежно від чутливості інформації. Передусім треба переконатись, що пароль знають лише авторизовані особи.

4. Надати первинні та постійні поради окремим особам.

Що стосується конфіденційної інформації, не треба думати, що кожен знає, що йому слід робити. Чітко пояснюємо, що можна, а чого не слід робити з інформацією та яких заходів треба вжити для її захисту.

5. Вести облік відкритої інформації.

Завжди зберігати записи про те, яку конфіденційну інформацію розкрито одержувачу і коли. Це важливо, оскільки допоможе відстежити будь-яке несанкціоноване відкриття інформації. Крім того, якщо вимагається повернення або знищення вашої інформації наприкінці угоди, то можна переконатися, що це зроблено.

6. Надати паперові копії замість електронних документів.

Електронні документи легко копіювати та розповсюджувати одним натисканням кнопки. Це не так просто для паперового документа, тому натомість можна роздати копії конфіденційного документа на нараді. Після цього відвідувачі можуть їх переглянути, а потім можна зібрати їх наприкінці зустрічі без заборонених копій.

7. Створити кабінет даних.

Це поширений метод захисту конфіденційної інформації, зокрема під час продажу бізнесу. Вся інформація зберігається в одному місці, і потенційні покупці зможуть увійти до кабінету, щоб переглянути її. Також можна використовувати віртуальні або електронні кабінети даних.

Ніколи не варто бути самовпевненими, коли справа стосується конфіденційної інформації, або думати, що можна покладатися виключно на угоду про нерозголошення, щоб захистити вас. Здоровий глузд завжди повинен бути в усьому.

В Англії існують угоди про конфіденційність, які укладають до того, як обговорять конфіденційність інформації із, наприклад, потенційним діловим партнером, або перш ніж розкриють йому конфіденційну інформацію. Такий документ:

– містить повну редакційну записку, яка пояснює, як її заповнити та персоналізувати відповідно до ваших конкретних потреб;
– призначений для використання як компаніями, так і приватними особами;
– підходить, якщо одна або обидві сторони розкривають конфіденційну інформацію.

Слід зауважити, що угода укладається відповідно до законодавства Англії та передбачає, що обидві сторони проживають у Великобританії. Якщо одна сторона працює в іншій країні, можуть застосовуватися різні закони, тому необхідно звернутися до юриста організації, до юрисдикції якої планується передати інформацію.

Крім того, закони про захист даних можуть застосовуватися до будь-якої конфіденційної інформації, яка містить персональні дані. Ця угода не охоплює дотримання законів про захист даних, тому треба звернутися за окремою консультацією, якщо вважаємо, що це може стосуватися нас.

Підтримання високого рівня безпеки є надзвичайно важливим для роботи з документами у будь-якій галузі.

Загрози безпеці документів можуть включати:

– порушення безпеки;
– неструктуровані дані;
– незахищені файли;
– людську недбалість;
– несанкціонований доступ до сховищ.

Це означає і можливий ризик базами даних клієнтів, і фінансовими реквізитами або навіть поточними угодами, особливо коли йдеться про компанії, що надають фінансові послуги.

Клієнтам важливо мати довіру до фірм, організацій і установ, це стає необхідністю бізнесу. Безпека документів – питання, що може навіть лякати. Проте потрібно про це просто знати і, відповідно, робити необхідні кроки задля дотримання безпечної роботи.

Дослідження CloudEntr («Стан кібербезпеки малого та середнього бізнесу») в США показало, що 77 % організацій визначили співробітників як найслабшу ланку для підтримки безпеки даних та мережі (Ouaknine, 2020). Аби зменшити ризики, варто запровадити суворі організаційні кодекси та практики.

Найпоширенішими загрозами безпеці документів є внутрішні, і тому проти них треба вжити системних заходів, а саме:

1. Запобігати можливості співробітникам стати жертвами фішингу.

На фішинг електронної пошти сьогодні припадає 90–95 % кібератак в усьому світі. Це представляє найбільшу внутрішню загрозу. Тут хакери діють як надійні

організації, такі, як постачальники, колеги чи навіть клієнти, і просять конфіденційної інформації. Обов'язково треба перевірити фактичну адресу електронної пошти відправника, а не лише ім'я. Орфографічні помилки, неправильні або трохи змінені логотипи також є приводом замислитись. Якщо не впевнені, перевірити електронну адресу зі своєю ІТ-командою, щоб не компрометувати будь-які конфіденційні документи. Надійними засобами гарантування безпеки інформації стануть безпечні посилання, які аналізують зовнішні посилання та виявляють підозрілі, що використовуються у фішинг-листах, та безпечні відправники для збереження списку надійних відправників.

Віруси та програми-вимагачі можуть пошкодити всі документи, що зберігаються на серверах. Варто бути обережним під час роботи з політикою щодо спаму та фішинг-листів.

2. Керувати своїми документами.

Захист документів найкраще працює, коли права доступу до документів надаються за необхідністю. Блокування документів паролями та обмеження доступу – ефективні способи створення безпечного середовища для документів. Системи електронного документообігу можуть бути надзвичайно корисними, бо мають аудиторські потоки, які контролюють документи та записують будь-які зміни та загальну діяльність. Дуже важливо, щоб ці потоки активно перевірялися на підозрілу активність, що може становити загрозу для стандартів безпеки документів. Багато користувачів покладаються на такі системи захисту даних, як Azure Information Protection, для класифікації, маркування та захисту документів на основі їх чутливості.

Це також порушує питання фізичних документів, які залишаються в офісі, і їх можуть побачити усі. Важливо, щоб цього не сталося. Треба переконатися, що колеги надійно знищують конфіденційні документи (замість того, щоб просто вилучити їх у кошик), або безпечно заховати їх.

3. Пам'ятати про спільні пристрої.

Спільні пристрої, такі як принтери та сканери, є ще одним недоліком безпеки документів. Щоб обмежити небезпеку, лише авторизовані користувачі повинні мати доступ до мережевих програм та ресурсів із цих систем. Принтери треба захищати паролем або автентифікацією на основі смарт-карт, використовуючи наявну інфраструктуру безпеки, що зменшує потребу в додаткових паролях. Програмне забезпечення для управління друком може використовуватися для утримання документів у черзі друку та підтримки повної перевірки аудиту діяльності з документами. Також поширеною є ситуація, коли обмежують доступ до фізичних портів (USB, флеш-накопичувач), щоб ніхто не викрав конфіденційні документи або не заразив мережу компанії.

Загрози безпеці зовнішніх документів також варто зменшити. Документи можна зламати, незважаючи на наявність заходів безпеки. Щоб обмежити порушення безпеки, необхідно дотримуватися таких практик:

1. Захищати свої дані.

Відсутність ефективного методу шифрування може виявитися фатальною помилкою. Само собою зрозуміло, що установа чи організація повинні мати оновлене антивірусне та шпигунське програмне забезпечення. Оскільки робота вдома зараз стає більш поширеною, ми покладаємося на захист віддаленої робочої сили від Microsoft Defender ATP (Advanced Threat Protection). Крім того, фільтрація доступу

до інтернету у всій компанії зменшує ймовірність того, що співробітники можуть стати жертвами зовнішніх фішингових сайтів або завантажити шкідливе програмне забезпечення, яке може поширюватися всередині організації. Використовувати корпоративну мережу VPN, коли єдиний вихід – це загальнодоступний Wi-Fi.

Апаратне шифрування також є обов'язковим: що станеться, якщо вкрадуть ноутбук? Для блокування даних, що зберігаються на жорстких дисках ноутбуків, можна вибрати Microsoft BitLocker.

2. Змінити формат документа.

Надсилання документів у форматі PDF усуває залежні від формату документа вузькі місця та перетворює цифрові документи на файли, захищені паролем, із захищеним шифруванням та елементами керування дозволами для керування редагуваннями. Це означає, що їх не може редагувати ніхто, крім автора документа, що зменшує ризик підробки. PDF-файли також перешкоджають хакерам отримувати метадані автора документа під час використання форматів Word/PowerPoint (див. рис. 1).

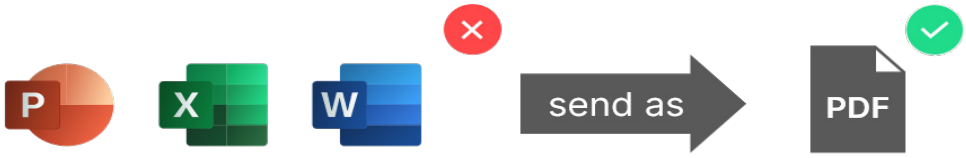

Рис. 1. Залежність стану захищеності інформації документа від формату
Джерело: https://www.upslide.net/en/the-importance-of-document-security-and-how-to-make-sure-you-are-working-safely

Окрім того, електронні підписи можуть не тільки допомогти відправникам швидко підписати вихідні документи, а й дати змогу одержувачам переконатися, що документи, які вони отримують, справді надходять від тих, від кого вони претендують, і що жодних змін не відбулося з моменту їх автентифікації.

3. Використовувати паролі з розумом.

Не забувати паролі. Рекомендовано використовувати жорстку політику паролів у поєднанні з MFA (багатофакторною автентифікацією), щоб уникнути зміни паролів кожні 3 місяці. Також добре нагадати колегам про деякі основні правила щодо паролів:

– ніколи не писати паролі на наліпках, а потім «ховати» їх за клавіатурою;
– не повторювати свій пароль у кількох облікових записах та на різних платформах;
– перевіряти, чи ваш обліковий запис не зламано, спочатку звернувши увагу на свою електронну адресу;
– чим довший пароль, тим краще.

ВИСНОВКИ

Проведене дослідження дає змогу підсумувати, що, по-перше, українську законодавчо-нормативну базу варто формувати з урахуванням світових законодавчих ініціатив і впроваджень. По-друге, фірмам, організаціям, установам, а також окремим особам необхідно забезпечити захист конфіденційності інформації,

з огляду на загрози слід упровадити відповідні кроки задля гарантування безпечної роботи. По-третє, не нехтувати правилами проведення ідентифікації та автентифікації, використовувати жорстку політику паролів. Проблема захисту інформації вирішується тільки комплексно.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

Брижко В. М., Радянська А. І., Швець М. Я. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних. Київ : Тріумф, 2006. 256 с.

Василюк В. Система захисту інформації приватного підприємства. Організація служби захисту приватного підприємства. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2007. Вип. 1(14). С. 45–51.

Вимоги до роботи з конфіденційною інформацією установи. *Баланс-Бюджет*. 2020. № 51. URL: https://balance.ua/news/post/trebovaniya-k-rabote-s-konfidencialnoy-informaciey-uchrezhdeniya (дата звернення: 23.10.2021).

Гуцалюк М. В. Організація захисту інформації. 2-е вид., перероб. та допов. Київ : Альтерпрес, 2011. 308 с.

Електронне урядування та електронна демократія / за заг. ред. А. І. Семенченка, В. М. Дрешпака. Київ. 2017. Частина 13: Захист інформації в системах електронного урядування / [О. М. Хошаба]. Київ : ФОП Москаленко О. М., 2017. 72 с.

Кукарін О. Б. Електронний документообіг та захист інформації / за заг. ред. Н. В. Грицяк. Київ : НАДУ, 2015. 84 с.

Особливості роботи з документами з грифом «Для службового користування». *Юридична газета online*. 5 лип. 2019. URL: https://yur-gazeta.com/publications/practice/sudova-praktika/osoblivosti-roboti-z-dokumentami-z-grifom-dlya-sluzhbovogo-koristuvannya.html (дата звернення: 22.10.2021).

Посібник з європейського права у сфері захисту персональних даних / Агенція Європейського Союзу з питань основоположних прав та Рада Європи. Київ. 2018. 432 с. URL: https://www.echr.coe.int/Documents/Handbook_data_protection_UKR.pdf (дата звернення: 15.11.2021).

Про доступ до публічної інформації : Закон України № 2939-VI від 13.01.2011. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 22.09.2021).

Про захист персональних даних : Закон України № 2297-VI від 01.06.2010. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 22.09.2021).

Про інформацію : Закон України № 2657-XII від 02.10.1992. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 22.09.2021).

Стінен Дж. Безпека документів та управління ідентифікацією в Україні. Київ. 2015. URL: https://docplayer.net/67464988-Bezpeka-dokumentiv-ta-upravlinnya-identifikaciieyu-v-ukrayini-dzhon-stinen.html (дата звернення: 15.11.2021).

Carbo Dzh. Don't Just Rely On Data Privacy Laws to Protect Information. 2020, February 24. URL: https://www.securitymagazine.com/articles/91775-dont-just-rely-on-data-privacy-laws-to-protect-information (дата звернення: 15.09.2021).

Ouaknine E. The Importance of Document Security and How to Make Sure You are Working Safely. 2020, August 6. URL: https://www.upslide.net/en/the-importance-of-document-security-and-how-to-make-sure-you-are-working-safely/ (дата звернення: 15.09.2021).

Wolker D. The DNA of NDA's – are Confidentiality Agreements Worth the Paper They are Written on? 2016, February 22. URL: http://www.gridlaw.com/are-confidentiality-agreements-worth-the-paper-they-are-written-on/ (дата звернення: 15.09.2021).

REFERENCES

Bryzhko, V. M, Radianska, A. I., & Shvets, M. Ia (2006). *Porivnialno-pravove doslidzhennia vidpovidnosti zakonodavstva Ukrainy zakonodavstvu YeS u sferi personalnykh danykh [Comparative Legal Study of Compliance of Ukrainian Legislation With EU Legislation in the Field of Personal Data]*. Triumph [in Ukrainian].

Vasyliuk, V. (2007). Systema zakhystu informatsii pryvatnoho pidpryiemstva. Orhanizatsiia sluzhby zakhystu pryvatnoho pidpryiemtva [Information Protection System of a Private Enterprise. Organisation of Private Enterprise Protection Service.] *Legal, Regulatory and Metrological Support of Information Security System in Ukraine*, *1*(14), 45–51 [in Ukrainian].

Vymohy do roboty z konfidentsiinoiu informatsiieiu ustanovy [Requirements for Working With Confidential Information of the Institution]. (2020, Dezember 8). *Balance-Budget*, *51*. https://balance.ua/news/post/trebovaniya-k-rabote-s-konfidencialnoy-informaciey-uchrezhdeniya [in Ukrainian].

Hutsaliuk, M. V. (2011). *Orhanizatsiia zakhystu informatsii [Organisation of Information Protection]* (2nd ed.). Alterpress [in Ukrainian].

Semenchenko, A. I., & Dreshpak, V. M. (Eds.). (2017). *Elektronne uriaduvannia ta elektronna demokratiia [E-government and e-democracy]* (Pt. 13: O. M. Hoshaba, (Ed.), Zakhyst informatsii v systemakh elektronnoho uriaduvannia [Information Protection in E-government Systems]). FOP Moskalenko O. M. [in Ukrainian].

Kukarin, O. B. (2015). *Elektronnyi dokumentoobih ta zakhyst informatsii [Electronic Document Management and Information Protection]*. National Academy of Public Administration under the President of Ukraine [in Ukrainian].

Osoblyvosti roboty z dokumentamy z hryfom "Dlia sluzhbovoho korystuvannia" [Features of Working With Documents Marked "For Official Use"]. (2019, Juli 5). *Legal newspaper online*. https://yur-gazeta.com/publications/practice/sudova-praktika/osoblivosti-roboti-z-dokumentami-z-grifom-dlya-sluzhbovogo-koristuvannya.html [in Ukrainian].

European Union Agency for Fundamental Rights and Council of Europe. (2018). *Posibnyk z yevropeiskoho prava u sferi zakhystu personalnykh danykh [Guide to European Law in the Field of Personal Data Protection]*. https://www.echr.coe.int/Documents/Handbook_data_protection_UKR.pdf [in Ukrainian].

Verkhovna Rada of Ukraine. (2011, January 13). *Pro dostup do publichnoi informatsii [On Access to Public Information]* (№ 2939-VI). https://zakon.rada.gov.ua/laws/show/2939-17#Text [in Ukrainian].

Verkhovna Rada of Ukraine. (2010, Juni, 1). *Pro zakhyst personalnykh danykh [On Personal Data Protection]* (№ 2297-VI). https://zakon.rada.gov.ua/laws/show/2297-17#Text [in Ukrainian].

Verkhovna Rada of Ukraine. (1992, October 2). *Pro informatsiiu [On Information]* (2657-XII). https://zakon.rada.gov.ua/laws/show/2657-12#Text [in Ukrainian].

Stinen, Dzh. (2015). *Bezpeka dokumentiv ta upravlinnia identyfikatsiieiu v Ukraini [Document Security and Identification Management in Ukraine]*. https://docplayer.net/67464988-Bezpeka-dokumentiv-ta-upravlinnya-identifikaciieyu-v-ukrayini-dzhon-stinen.html [in Ukrainian].

Carbo, D. (2020, February 24). *Don't Just Rely On Data Privacy Laws to Protect Information*. https://www.securitymagazine.com/articles/91775-dont-just-rely-on-data-privacy-laws-to-protect-information [in English].

Ouaknine, E. (2020, August 6). *The Importance of Document Security and How to Make Sure You are Working Safely*. https://www.upslide.net/en/the-importance-of-document-security-and-how-to-make-sure-you-are-working-safely/ [in English].

Wolker, D. (2016, February 22). *The DNA of NDA's – are Confidentiality Agreements Worth the Paper They are Written on?* URL: http://www.gridlaw.com/are-confidentiality-agreements-worth-the-paper-they-are-written-on/ [in English].

UDC 002:001.1(100)

Maryna Tsilyna,
Associate Professor, Department of Documentation and Data Analytics, Kyiv National University of Culture and Arts, PhD in Philology, Associate professor (Kyiv, Ukraine)
e-mail: macilin@ukr.net
ORCID: 0000-0001-5339-5147

FOREIGN EXPERIENCE AND PRACTICE OF ENSURING THE CONFIDENTIALITY OF INFORMATION AND CREATING SECURE CONDITIONS FOR THE FUNCTIONING OF DOCUMENTS

The aim of the article is to find out the safest conditions for the functioning of documents, as well as to find the most effective ways to avoid potential risks and dangers in the domestic information space.

The research methodology consisted of a set of general scientific and special methods of studying the issue. The review and analytical method was used to work on the professional and specialised literature and to determine the theoretical basis of the research, the systematic method proved to be effective in studying certain foreign practices of ensuring the confidentiality of information. The application of the induction method made it possible to generalise and draw a conclusion about the possibility of using the experience of other countries within the Ukrainian information space. Special methods, namely the method of researching document flows and the method of determining the information content of the document, were useful in considering the process of moving documents in the information field, the possibility/impossibility of damage or loss of information, and ways to prevent such undesirable situations.

The scientific research was based on the principles of objectivity and integrity. The use of a set of scientific methods made it possible to study the special features of confidential document information that is processed abroad, and to identify the main threats to the violation of the integrity and accessibility of information.

Scientific novelty. The latest practices of England, the European Union, and the United States in the field of document confidentiality are studied. The main recommendations for the protection of confidential information, and confidential agreements implemented abroad are considered. Features of secure use of document information are established. The article proposes a number of systematic measures against threats that arise in the process of working with confidential documents**.**

Conclusions. The study allows us to conclude that the Ukrainian legislative and regulatory framework should be formed taking into account global legislative initiatives and implementations. Companies, organisations, institutions, as well as individuals, need to ensure the protection of confidentiality of information, and given the threats, appropriate steps should be taken to ensure safe operation. The rules of identification and authentication should not be neglected, and a strict password policy should be used. The issue of information protection could be solved only in a comprehensive way.

Keywords: authentication, availability of information, protection of confidential information, identification, information confidentiality agreement, the value of documentary information

Стаття надійшла до редакції 21.03.2022 р.