DOI: http://doi.org/10.37734/2409-6873-2019-4-7 УДК 651

ІНФОРМАЦІЙНА БЕЗПЕКА В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Л. В. ПІДДУБНА, кандидат філософських наук, доцент;
В. М. ПАВЛІЧЕНКО, доктор юридичних наук
(Харківський інститут фінансів
Київського національного торговельно-економічного університету)

Анотація. Мета *статті полягає у виявленні загроз інформаційної безпеки систем електронного документообігу, які використовуються в державних та комерційних структурах, на великих та середніх підприємствах, в організаціях, установах, і шляхів їх подолання.* ***Методика дослідження.*** *Вирішення поставлених у публікації завдань здійснено за допомогою таких загальнонаукових і спеціальних методів дослідження, як аналіз та синтез, порівняння та аналогія, систематизація та узагальнення, діалектичний підхід.* ***Результати****. Запропоновано напрями підвищення рівня інформаційної безпеки систем електронного документообігу, проаналізовано засоби захисту систем електронного документообігу. Визначено, що інформаційна безпека в системах електронного документообігу є комплексним завданням, вирішення якого потребує поєднання заходів на законодавчому, адміністративному, процедурному та програмно-технічному рівнях. Розглянуто сучасний законодавчий рівень протидії загрозам, який представлено законами України «Про електронні документи та електронний документообіг», «Про електронні довірчі послуги», «Про Національну програму інформатизації», «Про обов'язковий примірник документів», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про Національну систему конфіденційного зв'язку». Під час упровадження в діяльність суб'єкта господарювання систем електронного документообігу необхідно пам'ятати про безпеку системи, так як особливий інтерес із боку зловмисників викликають саме документи фізичної чи юридичної особи. Говорячи про захищений документообіг, мають на увазі захист даних від несанкціонованого доступу, захист апаратних елементів системи (комп'ютерів, серверів, елементів комп'ютерної мережі та мережевого обладнання), захист файлів програмного забезпечення й бази даних. Загрози в системах електронного документообігу стандартні та складаються із загроз цілісності, конфіденційності, працездатності системи. У будь-якій «захищеній» системі електронного документообігу мають бути передбачені механізми забезпечення збереження документів, безперечного доступу, справжності документів , протоколювання дії користувачів.* ***Практична значущість результатів дослідження.*** *У статті обґрунтовано, що впровадження заходів інформаційної безпеки в системах електронного документообігу сприятиме підвищенню ефективності прийняття управлінських рішень, прозорості в діяльності організації, покращенню рівня безпеки та збереженню інформації. Основні наукові положення статті можна використовувати в документаційній діяльності будь-якого суб'єкта господарювання.*

Ключові слова: *системи електронного документообігу, електронний документ, електронний цифровий підпис, інформаційна безпека.*

Постановка проблеми в загальному вигляді та зв'язок із найважливішими науковими чи практичними завданнями. Сьогодні вже ні в кого не виникає сумнівів щодо необхідності впровадження систем електронного документообігу (СЕД) в діяльність бідь-якого суб'єкта господарювання. Електронний документообіг є основою функціонування організацій із різним типом діяльності, формами власності, розмірами. На думку фахівців, попит на СЕД із року в рік постійно зростає. Їх упровадження забезпечує чималу гнучкість в обробці та зберіганні інформації, змушує бюрократичну систему організації працювати швидше та якісніше, впливає на ефективність прийняття управлінських рішень, прозорість діяльності організації, ефективність її системи контролю якості й відповідність міжнародним стандартам, збільшення продуктивності праці, зменшення витрат на копіювання, зберігання, пошук, доставку та архівування документів у паперовому вигляді, підвищення рівня безпеки інформації за рахунок видачі особистих повноважень доступу кожному користувачеві СЕД та підвищення рівня збереження інформації, формалізує роботу працівників із можливістю збереження історії їх діяльності.

Розвиток сучасного інформаційного простору визначає нові потреби у формуванні умов для надійного функціонування суб'єктів господарювання, зокрема протидію інформаційним війнам і захист власного кіберпростору. Інформатизація та комп'ютеризація всіх галузей життя призвели до того, що електронні документи циркулюють в інформаційних системах і мережах, починаючи й закінчуючи свій життєвий цикл без жодної роздруківки. Зазначене має свої позитивні та негативні наслідки. З одного боку, це економія часу, паперу, можливість швидко отримати потрібний документ. З іншого – це загроза несанкціонованого доступу до інформації, її безпека. Проблема безпечної та гарантованої доставки електронних документів нині є актуальною як ніколи.

Формулювання цілей статті (постановка завдання). Метою публікації є дослідження проблеми інформаційної безпеки в системах електронного документообігу, які активно застосовуються в державних та комерційних структурах, на великих та середніх підприємствах, в організаціях, установах як в Україні, так і за кордоном. Під час упровадження СЕД головною проблемою є безпека системи, адже особливий інтерес із боку хакерів викликають саме документи фізичної або юридичної особи та зневага захистом обов'язково сприятиме появі нових загроз конфіденційності.

Аналіз останніх досліджень і публікацій. В умовах розвитку ринкових відносин, інформатизації та комп'ютеризації всіх галузей життя, інтенсифікації інформаційних обмінів проблеми захисту інформаційних потоків суб'єктів господарювання є вкрай актуальними, особливо це стосується систем електронного документообігу. Дослідженням проблем побудови та організації систем електронного документообігу, юридичного статусу, обґрунтованості та захисту електронних документів займалися О. Соколов, В. Шаньгин [1], Т. Ільіна, О. Логінова, Д. Романов [2, 3], В. Писаренко [4] та ін. Не зменшуючи важливості отриманих ними результатів та напрацювань, зазначимо, що існує низка важливих проблем, пов'язаних з упровадженням систем електронного документообігу та конфіденційністю інформації, яка в них циркулює, що потребує подальшого вирішення.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. У світовій та українській практиці електронний документообіг розпочав використання у сфері податкової звітності та банківській діяльності для документування розрахункових операцій. У Положенні про міжбанківські розрахунки, затвердженому Постановою Правління Національного Банку України 08.10.1998 року № 414, запроваджено практику використання електронних документів. Подальше розповсюдження електронний документообіг знайшов в системах електронного урядування, поступово охоплюючи роботу різноманітних суб'єктів господарювання, діяльність яких неможлива без руху документів.

Для документа як носія інформації характерними властивостями є: цінність, достовірність, актуальність, конфіденційність, цілісність, доступність, спостережність. Останні чотири атрибути характеризують документ із боку інформаційної безпеки. Так, конфіденційність полягає в тому, що документ може отримати тільки авторизований користувач. Цілісність документа означає можливість модифікації інформації авторизованим користувачем. Доступність свідчить, що документ може отримати в будь-який час авторизований користувач, який має відповідні повноваження. Спостережність характеризує властивість документа на всіх етапах його обробки та передачі знаходитись під контролем системи захисту. Комплекс заходів, спрямованих на забезпечення захищеності документів від використання, оприлюднення, несанкціонованого доступу, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення даних,

характеризує інформаційну безпеку СЕД, яку досліджують у контексті безпеки держави, організації та особистості.

Документ є базовим елементом системи організації документообігу, який може бути файлом, або записом у базі даних. Кажучи про безпечний документообіг, часто мають на увазі саме захист документів, тобто збереження інформації, яку ці документи в собі несуть. У цьому випадку все зводиться до захисту даних від несанкціонованого доступу. Однак мова йде не лише про захист даних усередині системи, а про захист усієї системи, її працездатності, швидке оновлення після ушкоджень, збоїв і навіть після знищення. Саме тому захист СЕД повинен бути комплексним на всіх рівнях, починаючи від захисту фізичних носіїв інформації і даних на них та закінчуючи організаційними заходами. Отже, по-перше, потрібно захищати апаратні елементи системи (комп'ютери, сервери, елементи комп'ютерної мережі та мережеве обладнання як активне – маршрутизатори, свічі, так і пасивне – кабелі, розетки тощо). Потрібно враховувати такі загрози, як вихід із ладу устаткування, доступ зловмисника до обладнання, відключення живлення тощо. По-друге, необхідно передбачити захист файлів системи, а саме файлів програмного забезпечення та бази даних тощо, інакше відкривається можливість впливу як би зовні на файли СЕД зловмисниками або зовнішніми обставинами без проникнення в систему. Тобто, файли бази можуть бути пошкоджені в результаті збою операційної системи чи обладнання або скопійовані зловмисником. Потретє, слід захищати документи й інформацію, що знаходяться всередині системи.

У системах електронного документообігу існує стандартний перелік загроз, які умовно поділяються на загрози цілісності, загрози конфіденційності та загрози працездатності системи. До загроз конфіденційності можна зарахувати будь-які порушення конфіденційності, у тому числі крадіжки, перехоплення інформації, зміни маршрутів переміщення. До загроз цілісності можна віднести пошкодження, знищення або спотворення інформації як у разі помилок і збоїв, так і зловмисне. У якості загроз працездатності можна розглядати різні загрози, реалізація яких сприятиме порушенням або припиненню роботи системи, наприклад, хакерські атаки, помилки користувачів, збої в обладнанні та програмному забезпеченні. Сучасні СЕД спроможні реалізувати захист від цих загроз. Існує певний парадокс, відповідно до якого впровадження СЕД, упорядкування і консолідація інформації, з одного боку, збільшують ризики реалізації загроз, а з іншого, дозволяють вибудовувати більш якісну систему захисту.

Сьогодні значна частина інформації, яка циркулює в організації, має гриф конфіденційності, бо визначає її напрями діяльності та розвитку. Для ефективного управління конфіденційною інформацією, окрім упровадження електронних систем управління, потрібно мати високий організаційний та технічний рівень інформаційної безпеки. Зазвичай, захист даних, що зберігаються на серверах, здійснюється за допомогою контролю доступу та шифрування. Якщо вся корпоративна мережа організації знаходиться в межах однієї локальної обчислювальної системи, то цього може бути достатньо для прийнятного рівня захисту конфіденційної інформації. Однак якщо організація має розгалужену структуру, що поєднує філії, структурні підрозділи, регіональні представництва, співробітників, які працюють віддалено, питання захисту інформації під час обміну конфіденційними даними загострюється. Для повсякденної роботи користувачів не завжди такі засоби інформаційної безпеки, як Virtual Private Network (VPN, віртуальна приватна мережа) і просте шифрування даних виявляються зручними та прийнятними. Так, безпека передачі інформації через загальнодоступні мережі здійснюється за допомогою шифрування, завдяки чому з'являється закритий для сторонніх користувачів канал обміну інформацією. За клієнт-серверною технологією VPN інтегрується декілька географічно віддалених мереж або користувачів у єдину мережу із застосовуванням для зв'язку між ними захищених каналів.

Існує декілька джерел загроз, до яких можна зарахувати користувачів системи, адміністративний IT-персонал (персонал служби IT-безпеки), зовнішніх зловмисників. Користувачі системи – це потенційні зловмисники, які свідомо чи ні можуть порушувати конфіденційність інформації. Відомі випадки, коли використання найвитонченіших систем захисту було марним у зв'язку з тим, що їх користувачі не бажали їх застосовувати через незвичність, незручності, небажання вчитися новому функціоналу. Також основною проблемою систем захисту документообігу залишається лояльність користувачів. Як тільки документ опиняється в користувача, його конфіденційність відносно інших користувачів уже порушена, адже він має безліч способів скопіювати інформацію, наприклад, шляхом фотографування документа за допомогою камери, вбудованої в стільниковий телефон, відправлення на електронну поштову скриню, розміщення у соціальних мережах або збереження на зовніш-

ній носій. Особливої уваги з точки зору безпеки СЕД заслуговує адміністративний ІТ-персонал, який має необмежені повноваження, доступ до сховищ даних і є найбільш кваліфікованим у питаннях безпеки та інформаційних можливостей системи. На думку дослідників [5], на внутрішні загрози припадає від 70 до 80 % втрат інформації. У якості зовнішніх зловмисників найчастіше виступають конкуренти, партнери, клієнти. За даними статистики, 45 % випадків втрати важливої інформації припадає на фізичні причини, пов'язані з відмовою апаратури та стихійним лихом, 35 % – обумовлені помилками користувачів і близько 20 % – діями шкідливих програм і зловмисників. Опитування компанії DeloitteTouche у 2016 р. свідчать, що більш половини компаній-користувачів СЕД стикалися із втратою даних протягом останніх 12 місяців. 33 % цих втрат призвели до серйозних фінансових збитків. Представники половини компаній, які пережили втрату даних, заявляють, що причиною інциденту став саботаж або недбале ставлення до правил інформаційної безпеки компанії, і тільки 20 % респондентів повідомили, що інтелектуальна власність їх компаній захищена належним чином. В ефективності захисту СЕД впевнені 24 % учасників опитування [5].

В інформаційній безпеці документообігу можна виокремити два якісно різних напрями. Один характеризує захист інформації у формі відомостей на традиційних носіях (паперовому, магнітному, оптичному). Другий напрям визначає захист процесів перетворення інформації, тобто технології її обробки. Історично в СЕД сформувалися дві типові схеми технологічного комплексу обробки інформації. Одна реалізується на базі сервера колективної роботи багатьох користувачів, а інша ґрунтується на поштовому сервері, який працює в якості інтернет-сервера, забезпечуючи підтримку територіально розподілених співробітників для ефективної їх взаємодії з офісом. Використання інтернет-сервера дозволяє здійснювати моніторинг різних інформаційних баз організації через мережу Інтернет.

Загроза СЕД може бути викликана: неповнотою, невірогідністю та невчасністю інформації, що використовується; несанкціонованим розповсюдженням, використанням і порушенням цілісності, конфіденційності та доступності інформації; відмовою від узятих зобов'язань; негативним інформаційним впливом; шахрайством під час проведення торговельних і фінансових операцій; несанкціонованим доступом до систем управління організацією та технологічними процесами.

Найважливішим фактором забезпечення інформаційної безпеки є законодавчий рівень протидії загрозам. Саме розробка та прийняття законодавчих актів забезпечують умови для безпечного використання СЕД, доступу та захисту інформації від несанкціонованого доступу. В Україні процес організації сучасного діловодства був унормований за допомогою створення нормативно-правової бази, розроблення єдиної державної системи діловодства та документаційного управління, уніфікації систем організаційно-розпорядчої документації, що стало підґрунтям для врегулювання відносин між суб'єктами в таких сферах діяльності, як електронна торгівля, електронна комерція, складання електронної звітності, надання електронних адміністративних послуг тощо. Були впроваджені Закони України «Про електронні документи та електронний документообіг», «Про електронні довірчі послуги», «Про Національну програму інформатизації», «Про обов'язковий примірник документів», «Про телекомунікації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про Національну систему конфіденційного зв'язку».

Закон «Про електронні документи та електронний документообіг» [6] визначає головні організаційно-правові засади електронного документообігу, регулює відносини, що пов'язані зі створенням, передачею, одержанням документа. Відповідно до цього Закону електронний документ уважається одержаним адресатом із моменту надходження автору електронного повідомлення про його отримання, якщо немає інших домовленостей між суб'єктами електронного документообігу. Електронний документ має юридичну силу, однак існують певні обмеження на використання електронного документа як оригіналу. Так сьогодні не має юридичної сили електронне свідоцтво про право на спадщину, або інший документ, який, відповідно до законодавства, може існувати лише в одному примірнику.

Відповідно до Закону «Про електронні довірчі послуги» [7] становлення цілісності отриманого електронного документа відбувається шляхом перевірки справжності електронного цифрового підпису (ЕЦП), що було на нього накладено. ЕЦП отримується внаслідок криптографічного перетворення набору електронних даних і засвідчує захищеність електронного документа від несанкціонованого спотворення або знищення у процесі переміщення від відправника до одержувача. ЕЦП дозволяє ідентифікувати підписанта й за правовим статусом прирівнюється до особистого підпису

(печатки), якщо: ЕЦП засвідчено із застосуванням посиленого сертифіката ключа за допомогою перевірених засобів цифрового підпису; під час перевірки використовувався посилений сертифікат ключа, який є діючим на момент накладання електронного цифрового підпису; особистий ключ підписанта відповідає відкритому ключу, зазначеному в сертифікаті. ЕЦП накладається за допомогою особистого (закритого, секретного) ключа, який повинен бути відомий лише його володарю, та перевіряється за допомогою відкритого ключа, що доступний усім учасникам електронного документообігу. Підробка особистого ключа неможлива за умови його правильного зберігання власником. Особистий ключ формується генератором випадкових величин і являє собою унікальну послідовність символів довжиною 264 біта. Підтвердження чинності відкритого ключа відбувається шляхом формування документа, що видається центром сертифікації ключів, який має назву сертифіката відкритого ключа. Сертифікат включає: найменування та реквізити центру сертифікації ключів; інформацію, що сертифікат виданий в Україні; унікальний реєстраційний номер сертифіката ключа; основні дані (реквізити) підписанта – власника особистого ключа; дату, час початку та завершення терміну дії сертифіката; відкритий ключ; найменування криптографічного алгоритму, що використовується власником особистого ключа; інформацію про обмеження використання підпису. В Україні послуги з надання ЕЦП впроваджуються акредитованими центрами сертифікації ключів.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [8] регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, визначає об'єкти захисту та суб'єкти відносин, порядок доступу до інформації, умови обробки та забезпечення захисту інформації, відповідальність за порушення законодавства. Закон України «Про телекомунікації» регламентує засади захисту прав і безпеки споживачів та контролю з боку держави ринку телекомунікацій.

1. Функціонування СЕД, рівень її безпеки залежать від низки факторів: Різнорідність апаратного та програмного забезпечення, що використовується в СЕД, впливає на процес технічного обслуговування (управління оновленнями та конфігураціями програмних засобів) та проведення стандартних, базових заходів у галузі інформаційної безпеки. У більшості випадків робочі місця користувачів СЕД облаштовані операційною системою Windows. Опрацювання інформації в СЕД та важливі інформаційні ресурси зберігаються в базах даних, які знаходяться в операційних системах Solaris, Linux, FreeBSD. Сьогодні все частіше користувачі СЕД використовують портативні мобільні пристрої (планшети, смартфони), які побудовані на базі операційних систем iOS та Android.

2. Підключення зовнішніх користувачів (підприємств, організацій, окремих працівників) до відкритих сервісів і надання прав персоналу щодо віддаленої роботи із внутрішніми інформаційними ресурсами призводить до збільшення загальної кількості загроз, пов'язаних із можливістю несанкціонованого доступу до інформаційних ресурсів організації.

3. Наявність значної кількості вузлів корпоративної мережі в організаціях із розгалуженою структурою, що поєднує філії, структурні підрозділи, регіональні представництва, співробітників, які працюють віддалено, і відсутність часу для моніторингу параметрів конфігурації основних програмних засобів не дозволяє своєчасно технічному персоналу контролювати роботу й безпеку користувачів у розподілених СЕД.

4. Чіткий розподіл функціональних обов'язків персоналу підрозділу технічного обслуговування, який вирішує питання системного та мережевого адміністрування, та персоналу служби IT-безпеки, який опікується питаннями безпеки на адміністративному, технічному, організаційному та інших рівнях.

5. Використання в роботі із СЕД для забезпечення доступу до Інтернет Wi-Fi мережі з дотриманням правил безпеки процедурного рівня, до яких можна зарахувати: правильний підбір типу шифрування протоколу взаємодії з роутером (точкою доступу) Wi-Fi мережі, відключення віддаленого доступу до адміністрування роутера або точки доступу із глобальної мережі Інтернет, фільтрацію пристроїв комп'ютерної мережі за MAC-адресою, надійні паролі.

6. Наявність високого програмно-технічного рівня протидії загрозам інформаційної безпеки СЕД, що передбачає такі механізми безпеки: управління доступом до комп'ютерів; аутентифікація та ідентифікація користувачів; екранування каналів зв'язку; криптографія; забезпечення високої доступності, аудит, протоколювання, використання проксі-серверів тощо.

Висновки із зазначених проблем і перспективи подальших досліджень у поданому напрямі. Інформаційна безпека в системах електронного документообігу є комплексною проблемою, вирішення якої потребує поєднання заходів на законодавчому, адміністративно-

му, процедурному та програмно-технічному рівнях. Вимоги суб'єктів господарювання до функціональних можливостей СЕД та інформаційної безпеки специфічні й направлені на опрацювання різних видів інформації, зокрема метаданих, даних про бізнес-процеси й контент. У подальших наукових дослідженнях плануємо проаналізувати безпеку інформації в системі електронного документообігу Alfresco.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Соколов А. В. Защита информации в распределенных корпоративных сетях и системах / А. В. Соколов, В. Ф. Шаньгин. – Москва : ДМК Пресс, 2002. – 656 с.
2. Ильина Т. Н. Защита систем электронного документооборота / Т. Н. Ильина, А. Ю. Логинова, Д. А. Романов. – Москва : ДМК, 2018. – 224 с.
3. Романов Д. А. Правда об электронном документообороте / Д. А. Романов, Т. Н. Ильина, А. Ю. Логинова. – Москва : ДМК Пресс, 2008. – 220 с.
4. Писаренко В. П. Організаційно-правові засади електронного документування в органах влади : монографія / Писаренко В. П. – Полтава : ПУЕТ, 2012. – 250 с.
5. Защита систем электронного делопроизводства [Електронний ресурс]. – Режим доступу: http://www.ixbt.com/soft/sed.shtml (дата звернення: 30.09.2019). – Назва з екрана.
6. Про електронні документи та електронний документообіг [Електронний ресурс] : Закон України від 22 травня 2003 р. № 851-IV. – Режим доступу: https://zakon.rada.gov.ua/laws/show/851-15 (дата звернення: 18.09.2019). – Назва з екрана.
7. Про електронні довірчі послуги [Електронний ресурс] : Закон України від 05 жовтня 2017 р. № 2155-VIII. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#n534 (дата звернення: 18.09.2019). – Назва з екрана.
8. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : Закон України від 05 липня 1994 р. № 80/94-ВР. – Режим доступу: https://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2% D1%80 (дата звернення: 18.09.2019). – Назва з екрана.

REFERENCES

1. Sokolov, A. V. & Shangin, V. F. (2002). Zaschita informatsii v raspredelennyih korporativnyih setyah i sistemah. [*Information security in distributed corporate networks and systems*]. Moscow : DMK Press [in Russian].
2. Ilina, T. N., Loginova, A. Yu., Romanov, D. A. (2018). Zaschita sistem elektronnogo dokumentooborota [*Protection of electronic document management systems*]. Moscow : DMK [in Russian].
3. Romanov, D. A., Ilina, T. N., Loginova, A. Yu. (2008). Pravda ob elektronnom dokumentooborote [*The truth about electronic document flow*]. Moscow : DMK Press [in Russian].
4. Pysarenko, V. P. (2012). Organizatsiino-pravovi zasady elektronnogo dokumentuvannia v organah vlady : monografiia. [*Organizational and legal principles of electronic documentation in the authorities*]. Poltava : PUET [in Ukrainian].
5. Zaschita sistem elektronnogo deloproizvodstva Retrieved from http://www.ixbt.com/soft/sed.shtml. (accessed 30.09.2019) [in Russian].
6. Zakon Ukrainy "Pro elektronni dokumenty ta elektronnyy dokumentoobih": vid 22 travnya 2003 r. № 851-IV. [Law of Ukraine "About electronic documents and electronic document flow" from May 22, 2003, № 851-IV]. Retrieved from https://zakon.rada.gov.ua/laws/show/851-15 (accessed 18 September 2019) [in Ukrainian].
7. Zakon Ukrainy "Pro elektronni dovirchi posluhy": vid 05 zhovtnya 2017 r. № 2155-VIII. [Law of Ukraine "About electronic trust services" from October 05, 2017, № 2155-VIII]. Retrieved from https://zakon.rada.gov.ua/ laws/show/2155-19#n534 (accessed 18 September 2019) [in Ukrainian].
8. Zakon Ukrainy "Pro zakhyst informatsiyi v informatsiyno-telekomunikatsiynykh systemakh": vid 05 lypnya 1994 r. № 80/94-BP. [Law of Ukraine "About information security in information and telecommunication systems" from July 05, 1994, № 80/94-BP]. Retrieved from https://zakon2.rada. gov.ua/ laws/show/80/94-%D0%B2%D1%80 (accessed 18 September 2019) [in Ukrainian].

Л. В. Поддубная**,** *кандидат философских наук, доцент;* ***В. Н. Павличенко,*** *доктор юридических наук (Харьковский институт финансов Киевского национального торгово-экономического университета).* ***Информационная безопасность в системах электронного документооборота.***

Аннотация. Цель *статьи заключается в определении угроз информационной безопасности систем электронного документооборота, которые используются в государственных и коммерческих структурах, на больших и средних предприятиях, в организациях, учреждениях, и путей их ликвидации.* ***Методика исследования.*** *Решение задач, поставленных в статье, осуществляется с помощью таких общенаучных и специальных методов исследования, как анализ и синтез, сравнение и аналогия, систематизация и обобщение, диалектический подход.* ***Результаты.*** *Предложены направления повышения уровня информационной безопасности систем электронного документооборота, проанализированы средства защиты систем электронного документооборота. Определено, что проблема информационной безопасности в системах электронного документооборота есть комплексной задачей, решение которой требует объединения мероприятий на законодательном, административном, процедурном и программно-техническом уровнях. Рассмотрено современное законодательство по вопросам защиты информации в системах электронного документооборота. Оно представлено законами Украины «Об электронных документах и электронном документообороте», «Об электронных доверительных услугах», «О Национальной программе информатизации», «Об обязательном экземпляре документов», «О телекоммуникациях», «О защите информации в информационно-телекоммуникационных системах», «О Национальной системе конфиденциальной связи». При внедрении в деятельность субъекта хозяйствования систем электронного документооборота необходимо помнить о безопасности системы, так как особый интерес со стороны злоумышленников вызывают именно документы физического или юридического лица. Говоря о защищенном документообороте, подразумевают защиту данных от несанкционированного доступа, защиту аппаратных элементов системы (компьютеров, серверов, элементов компьютерной сети и сетевого оборудования), защиту файлов программного обеспечения и базы данных. Угрозы в системах электронного документооборота стандартные и состоят из угроз целостности, конфиденциальности, работоспособности системы. В любой «защищенной» системе электронного документооборота должны быть предусмотрены механизмы обеспечения сохранности документов, безопасного доступа, подлинности документов, протоколирование действия пользователей.* ***Практическая значимость результатов исследования.*** *В статье обосновано, что внедрение мероприятий информационной безопасности в системах электронного документооборота будет способствовать повышению эффективности принятия управленческих решений, прозрачности в деятельности организации, улучшению уровня безопасности и сохранности информации. Основные научные положения статьи можно использовать в документационной деятельности любого субъекта хозяйствования.*

Ключевые слова: *системы электронного документооборота, электронный документ, электронная цифровая подпись, информационная безопасность.*

L. Piddubna, *Cand. Philosophy Sci., Docent;* ***V. Pavlichenko,*** *Dr. of legal Sci. (Kharkiv Institute of Finance of Kiev National Trade and Economic University).* ***Information security in electronic document management systems.***

Annotation. The purpose *of the article is to identify threats to information security in electronic document management systems (EDMS) and ways to eliminate them. EDMS used in government and commercial structures, in large and medium enterprises, organizations, institutions.* ***Methodology of research.*** *The solution of the problems posed in the article is carried out using such general scientific and special research methods as analysis and synthesis, comparison and analogy, systematization and generalization, and the dialectical approach.* ***Findings.*** *Directions of increasing the level of information*

security of electronic document management systems are proposed, means of protecting electronic document management systems are analyzed. It is proved that the problem of information security in electronic document management systems can be addressed comprehensively at the legislative, administrative, procedural and software-technical levels. The current legislation on the protection of information in electronic document management systems is considered. It is represented by the laws of Ukraine «On electronic documents and electronic document management», «On electronic trust services», «On the National Informatization Program», «On the mandatory copy of documents», «On telecommunications», «On the protection of information in information and telecommunication systems», «On the National Confidential Communication System». When introducing electronic document management systems into the activities of a business entity, it is necessary to remember the security of the system, since it is the documents of an individual or legal entity that attract particular interest from attackers. Speaking about secure workflow, they mean protecting data from unauthorized access, protecting system hardware elements (computers, servers, computer network elements and network equipment), protecting software and database files. Threats in electronic document management systems are standard and consist of threats to the integrity, confidentiality and operability of the system. In any «secure» electronic document management system, mechanisms should be provided to ensure the safety of documents, secure access, authenticity of documents, and logging user actions. ***Practical value.*** *The article substantiates that the use of information security mechanisms in electronic document management systems will increase the efficiency of managerial decision-making, transparency in the organization's activities, improve the level of security and safety of information. The main scientific provisions of the article can be used in the documentation activities of any business entity.*

Keywords: *electronic document management systems, electronic document, electronic digital signature, information security.*