МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТАВРІЙСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ В.І. ВЕРНАДСЬКОГО
КАФЕДРА КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

На правах рукопису

КВАЛІФІКАЦІЙНА РОБОТА НА ЗДОБУТТЯ СТУПЕНЯ ВИЩОЇ ОСВІТИ «МАГІСТР»
МЕХАНІЗМИ ЕЛЕКТРОННОГО НАДАННЯ ДОКУМЕНТАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СУЧАСНОЇ УСТАНОВИ

Здобувачки вищої освіти
Дудченко Наталії Костянтинівни
спеціальності «Інформаційна,
бібліотечна та архівна справа»
Навчально-наукового інституту
муніципального управління та
міського господарства

_____
(підпис)

Науковий керівник:
доктор філософії Кучерявий В.М.

_____
(підпис)

Національна шкала відмінно
Кількість балів 91
Оцінка: ECTS A

Київ – 2024

АНОТАЦІЯ

Дудченко Наталія. Механізми електронного надання документаційного забезпечення сучасної установи.

У роботі досліджуються механізми електронного надання документаційного забезпечення сучасної установи. Під час написання роботи було розглянуто теоретичні основи організації роботи механізмів електронного надання документаційного забезпечення; досліджено систему електронного надання документаційного забезпечення сучасної установи (на прикладі Товариства з додатковою відповідальністю Страхова компанія «Ю.Ес.Ай.»); висвітлено шляхи удосконалення механізмів надання документаційного забезпечення сучасної установи.

Ключові слова: установа, е-документообіг, електронний підпис, документаційне забезпечення, захист інформації.

S U M M A R Y

Dudchenko Nataliia. Mechanisms of electronic documentation of a modern institution.

The mechanisms of electronic provision of documentation support of a modern institution are investigated in the work. During the writing of the work the theoretical bases of the organization of work of mechanisms of electronic rendering of documentary maintenance were considered; the system of electronic provision of documentation support of a modern institution has been studied (on the example of the Additional Liability Company Insurance Company "USA"); the ways of improving the mechanisms of providing documentation for a modern institution are highlighted.

Key words: institution, e-document circulation, electronic signature, documentation support, information protection.

ЗМІСТ

ВСТУП

Актуальність дослідження. Стан та подальший супровід документів сучасної установи повністю залежить від рівня інформаційного забезпечення її структурних підрозділів. Увесь життєвий цикл документів на сьогодні передбачає електронну роботу з ними. Тому, актуальність магістерської кваліфікаційної роботи посилюється на теоретичному рівні вирішенням проблем, пов’язаних безпосередньо із механізмами е-документаційного забезпечення, на практичному – втіленням цих механізмів у роботу фахівців установ різних форм власності. Безсумнівно, ключову роль у підході до механізмів документаційного забезпечення відіграє доступ до неструктурованої інформації, процесів організації вхідної, вихідної, внутрішньої та зовнішньої систем документообігу, формування основних звітів, і , звичайно, здійснення контролю на їхнім виконанням.

У цілому, сучасні програми е-документаційного забезпечення повинні вирішувати ряд комплексних задач, ключовими серед яких є: автоматизація процесів опрацювання вхідних, вихідних, внутрішніх, організаційно-розпорядчих, нормативних та інших видів документів; автоматизація процесів опрацювання звернень громадян; автоматизація процесів опрацювання запитів на публічну інформацію; автоматизація процесів опрацювання заявок на надання послуг; автоматизація процесів надання адміністративних послуг; можливість автоматизації процесів ведення різноманітних реєстрів; автоматизація процесів обліку договорів і контролю їх виконання; наскрізний контроль строків виконання документів, оповіщення виконавця і контролера про наближення строків виконання, про невиконані в строк документи; підтримка перехресних посилань і зв’язків між документами; застосування шаблонів документів; підтримка версій документів; застосування електронного підпису [67].

Окрім того, сучасні програми з е-документаційного забезпечення повинні підтримувати обмін даними і документами з системою електронної

взаємодії структурних підрозділів установи. Також, необхідно враховувати і необхідність забезпечення формування баз даних для обробки публічної інформації для подальшої публікації на веб-сайтах. Сучасні системи електронного документообігу повинні підтримувати і технології, що мають сервіси з автоматизації різноманітних ділових процесів:

- розробку маршрутів (схем бізнес-процесів);

- контроль виконання;

- розсилання повідомлень засобами самої системи, електронної пошти, SMS-повідомлень, тощо;

- можливість виконання автоматичних операцій системою електронного документообігу та/або іншими системами при досягненні певного кроку (етапу) маршруту або стану документу [67].

При виборі системи документаційного забезпечення треба враховувати і те, що ряд установ мають територіально-розподілену структуру і зможуть працювати через веб-доступ. Тобто, веб-інтерфейс системи повинен дозволяти територіально віддаленим та мобільним користувачам отримувати доступ до центральної бази даних системи для виконання всіх необхідних дій у процесах документообігу, у тому числі ведення власного локального документообігу, відповідно до наданих прав і повноважень. Робота фахівців у системі через веб-доступ має іти шляхом застосовування браузера Google Chrome, мати програмний інтерфейс (API) для інтеграції з іншими програмними додатками, а також підтримувати можливість експорту (імпорту) даних в інші формати (наприклад, XML, MS Office) [67].

Упродовж ІІ та ІІІ розділу магістерської роботи механізми електронного документаційного забезпечення будуть розглянуті нами на прикладі роботи сучасної страхової компанії, оскільки, структурні підрозділи працюють із великою кількістю організаційно-розпорядчих, особових, господарських та інформаційно-довідкових документів, то механізми роботи з ними лише посилюють актуальність дослідження. Маємо наголосити, що основну роботу з документами перебирають на себе страхові агенти. Відповідно до

законодавства, право здійснювати страхову діяльність на території України мають:

- фінансові установи, які створені у формі акціонерних, повних, командитних товариств або товариств з додатковою відповідальністю згідно із Законом України «Про господарські товариства» [44], з урахуванням того, що учасників кожної з таких фінансових установ повинно бути не менше трьох, та інших особливостей, передбачених Законом, а також одержали у встановленому порядку ліцензію на здійснення страхової діяльності, тобто, є страховиками-резидентами [44];

- зареєстровані Уповноваженим органом відповідно до Закону та законодавства України постійні представництва у формі філій іноземних страхових компаній, які також одержали у встановленому порядку ліцензію на здійснення страхової діяльності. В окремих випадках, встановлених законодавством України, страховиками визнаються державні організації, які створені і діють відповідно до Закону. У цьому разі використання слів «державна», «національна» або похідних від них у назві страховика дозволяється лише за умови, що єдиним власником такого страховика є держава [44].

Слова «страховик», «страхова компанія», «страхова організація» та похідні від них дозволяється використовувати у назві лише тим юридичним особам, які мають ліцензію на здійснення страхової діяльності [63]. За даними сучасних дослідників, зокрема Жук О. О. [18], світовий страховий ринок є досить сприятливим. Так, досвід Англії був «взятий за основу страхових норм у багатьох інших країнах. Страхові компанії Англії прагнули як можна більше підвищити якість послуг, пов’язаних із страхуванням, направляючи свою діяльність на спеціалізацію за окремими видами. При цьому, в них страхування відбувається в п’яти основних напрямах - короткострокового страхування життя, майнове, морське, авіаційне й автомобільне страхування» [18].

Так, у Німеччини страхова діяльність «складається із чотирьох напрямів: страхування на випадок захворювання, пенсійне страхування, страхування на випадок безробіття, страхування від нещасного випадку на виробництві. При цьому, основним нормативно-правовим актом, за допомогою якого здійснюється правове регулювання страхових правовідносин у Німеччині виступає Закон «Про страховий договір» [18]. натомість, у Японії «має місце посилення конкурентної боротьби з боку іноземних страхових організацій, які поглинають збанкрутілі японські організації. При цьому, значна кількість страхових організацій в Японії збанкрутувала ще в 1999-2000 роках. («Toho Mutual Life Insu- rance» - червень 1999 р., «Daihyaku Mutual Life Insurance» - травень 2000 р., «Taisho Life Insurance» - серпень 2000 р., «Chiyoda Mutual Life Insurance» - жовтень 2000 р., «Kyoei Life Insurance» - жовтень 2000 р., «Токіо Mutual Life Insurance» - березень 2001 р.)» [18].

Проблема вивчення особливостей механізмів електронного надання документаційного забезпечення сучасної установи є ключовою у дослідженнях багатьох українських науковців та вчених. Так, проблеми загального діловодства висвітлені у підручниках М. Безкровного, М. Кропивки, Ю. Палехи, Т. Іщенко. Вимоги до структури та змісту XML-схеми метаданих е-документів є об’єктом уваги О. Гараніна, Т. Купринець, Ю. Ковтанюка, Н. Христової та інших. Страхове документаційне забезпечення розглянуто у роботах О. Жук, О. Гаманкової, Л. Кінащук, Г. Піратовського тощо [2, 6, , 18, 40].

Об’єктом магістерської роботи є: механізми електронного надання документаційного забезпечення сучасної установи.

Предметом магістерської робити є: вивчення особливостей механізмів електронного надання документаційного забезпечення на прикладі Товариства з додатковою відповідальністю страхова компанія «Ю.Ес.Ай.».

Мета магістерської роботи – дослідити теоретичні основи та визначити на практичному рівні механізми електронного надання документаційного забезпечення сучасної установи

Досягнення поставленої мети зумовило необхідність розв’язання таких **завдань**:

- з’ясувати законодавчо-правові основи електронного надання документаційного забезпечення сучасної установи;

- проаналізувати організацію електронного документаційного забезпечення сучасної установи;

- проаналізувати системи захисту інформації в електронному документообігу;

- дослідити нормативне підґрунтя механізмів електронного надання документаційного забезпечення у Товаристві з додатковою відповідальністю страхова компанія «Ю.Ес.Ай.»;

- дослідити системи внутрішнього та зовнішнього документаційного забезпечення структурних підрозділів Товариства з додатковою відповідальністю страхова компанія «Ю.Ес.Ай.»;

- визначити шляхи удосконалення механізмів надання документаційного забезпечення Товариства з додатковою відповідальністю страхова компанія «Ю.Ес.Ай.».

Структура роботи: випускна робота складається зі вступу, трьох розділів, рисунків, висновків, списку використаних джерел, додатків.

РОЗДІЛ І. ТЕОРЕТИЧНІ ОСНОВИ ОРГАНІЗАЦІЇ РОБОТИ МЕХАНІЗМІВ ЕЛЕКТРОННОГО НАДАННЯ ДОКУМЕНТАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ

1.1. Законодавчо-правові основи електронного надання документаційного забезпечення

Теоретичні основи організації роботи механізмів електронного надання документаційного забезпечення у І розділі будуть обґрунтовані нами з огляду на сучасний стан нормативно-законодавчої бази, надалі ми проаналізуємо принципи електронного документообігу і захист інформації у системі електронного документаційного забезпечення установ. Маємо наголосити, що на сьогодні регулювання механізмів електронного надання документаційного забезпечення здійснюється через Конституцію України [27], Цивільний процесуальний кодекс України [73], Законами України «Про інформацію» [55], «Про захист інформації в автоматизованих системах» [52], «Про державну таємницю» [46], «Про телекомунікації» [53], «Про обов'язковий примірник документів» [60], «Про Національний архівний фонд та архівні установи» [59], Законом України «Про електронні документи та електронний документообіг» [49], ДСТУ 4163:22020 [12], іншими нормативно-правовими актами.

Так, новим по відношенню до усталеної раніше інформації, у проєкті ДСТУ 4163:2020 [12], є те, що «код юридичної особи проставляють за ЄДРПОУ згідно з Постановою Кабінету Міністрів України «Про внесення змін до Положення про Єдиний державний реєстр підприємств та організацій України». На загальному бланку юридичної особи та на бланку конкретного виду документа цей код розміщують під реквізитом «Код форми документа» (за його наявності), а на бланку листа – після реквізиту «Довідкові дані про юридичну особу» [12].

Відповідно до закону України «Про електронні документи та електронний документообіг» [49], електронний документ - документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. Важливим у системі електронного документаційного забезпечення є дотримання принципів управління якістю, що «не лише забезпечує безпосередні переваги, а й є складовою управління витратами та ризиками». З огляду на те, що міркування керівництва щодо переваг, витрат та ризику є важливими для установи, її замовників та інших зацікавлених сторін, то загальні показники діяльності установи можуть впливати на:

- прихильність замовників;

- стабільність ділової активності та відгуки про установу;

- результати підприємницької діяльності, а саме: доходи та ринкова частка;

- гнучкість та швидкість реагування на зміни ситуації на ринку [49];

- витрати та тривалість циклу завдяки результативному та ефективному використанню ресурсів;

- встановлення послідовності процесів, завдяки яким краще можна досягти бажаних результатів;

- конкурентну перевагу завдяки покращенню можливостей установи;

- розуміння та мотивацію співробітниками мети та завдань установи [49];

- впевненість зацікавлених сторін у результативності та ефективності діяльності установи, доведених фінансовими та соціальними вигодами, підтверджених її показниками, життєвим циклом продукції та репутацією;

- здатність створювати цінності як для установи, так і для її постачальників завдяки оптимізації витрат та ресурсів, гнучкості та швидкості спільного реагування на зміни ринкової ситуації [49].

У свою чергу, установа повинна:

а) визначити процеси, необхідні для системи управління якістю, їхнє застосування на всіх рівнях;

б) визначити послідовність та взаємодію цих процесів;

в) визначити критерії та методи, необхідні для забезпечення результативності функціонування цих процесів та управління ними;

г) забезпечити наявність ресурсів та інформації, необхідних для підтримання функціонування та моніторингу цих процесів [49];

д) здійснювати моніторинг, вимірювання та аналізування цих процесів:

е) вживати заходи, необхідні для досягнення запланованих результатів та постійного поліпшення цих процесів.

Установа повинна управляти цими процесами відповідно до вимог проєкту державного стандарту. Якщо для будь-якого процесу, що впливає на відповідність продукції вимогам, установа обирає стороннього виконавця, то необхідно забезпечити контроль за процесами, встановленими у системі управління якістю. Керівництво повинне визначити документацію (у тому числі відповідні протоколи), що необхідна для створення, впровадження та актуалізації системи управління якістю і для забезпечення результативного та ефективного функціонування процесів, застосовуваних в організації [49].

Характер та обсяг документації, адаптованої до профілю установи, мають задовольняти контрактні, законодавчі вимоги, потреби та очікування замовників, інших зацікавлених сторін. Документація може бути подана в будь-якій формі чи на будь-якому носії, залежно від потреб установи, Для того, щоб документація, створювала можливість задовольнити потреби та очікування зацікавлених сторін, керівництво повинне враховувати [49]:

- контрактні вимоги замовників та інших зацікавлених сторін;

- прийняття міжнародних, національних, регіональних та інших стандартів;

- відповідні законодавчі та регламентувальні вимоги;

- рішення, що ухваляє установа;

- джерела зовнішньої інформації, що сприяє підвищенню компетентності установи;

- інформацію про потреби та очікування зацікавлених сторін. Створення, застосування документації і управління нею слід оцінювати з погляду результативності та ефективності організації за такими критеріями: функціональність (наприклад, швидкість опрацювання); зручність користування; необхідні ресурси; політика та цілі; поточні та майбутні вимоги до управління знаннями; зіставне оцінювання (бенчмаркінг) систем документації; взаємозв'язки, застосовувані замовниками установи, її постачальниками та іншими зацікавленими сторонами [49].

Виходячи з політики організації в сфері інформування, за дослідниками, необхідно забезпечити доступ до документації працівникам організації та іншим зацікавленим сторонам. Тому, відповідно до світового досвіду та ДСТУ ISO 9001:2015 Системи управління якістю документація системи управління якістю повинна містити [13]: документально оформлені політику та цілі в сфері якості; настанову з якості; документи, необхідні установі для забезпечення результативного планування, функціонування та контролю процесів. Заразом, обсяги документації системи управління якістю можуть бути різними для кожної конкретної установи і зумовленими: розміром установи та видами її діяльності; складністю процесів та їх взаємодіями; компетентністю персоналу.

Канцелярією чи службою діловодства установи, фахівці якої несуть відповідальність за систему документаційного забезпечення, повинні розробити алгоритм, що визначає управлінські дії, необхідні для: затвердження документів як відповідних перед їх введенням в дію; аналізування та, в разі потреби, актуалізації документів і нового їх затвердження; забезпечення ідентифікації змін та статусу чинної переглянутої версії документів; забезпечення наявності відповідних версій чинних документів у місцях застосування; забезпечення розбірливості та простоти ідентифікації документів; забезпечення ідентифікації документів зовнішнього

походження і контролю за їхнім розповсюдженням; запобігання ненавмисному застосуванню застарілих документів і застосування належної ідентифікації цих документів у разі їх зберігання в будь-яких цілях [13].

За слушним зауваженням сучасних дослідників, «для успішного очолювання і спрямовування діяльності установи потрібно, щоб управління нею було систематичним та прозорим». Так, запропоновані у державному стандарті ДСТУ ISO 9001:2015 [14] рекомендації щодо управління ґрунтуються на восьми принципах управління. Ці принципи розроблені для застосування найвищим керівництвом із метою спрямування діяльності установи на покращення її показників:

1. Орієнтація на замовника. Установи залежать від замовників і тому повинні розуміти їхні поточні та майбутні потреби, виконувати їхні вимоги і прагнути до перевищення їхніх очікувань.

2. Лідерство. Керівники встановлюють єдність мети та напрямів діяльності установи. Вони мають створювати та підтримувати внутрішнє середовище, в якому можливе повне залучення працівників до діяльності, спрямованої на досягнення цілей установи.

3. Залучення працівників. Працівники на всіх рівнях становлять основу установи, і їхнє повне залучення дає змогу використовувати їхні здібності на користь організації [6, с.5].

4. Процеси й підхід. Бажаного результату досягають більш ефективно, коли діяльністю та пов’язаними з нею ресурсами управляють як процесом.

5. Системний підхід до управління. Установлення і розуміння взаємопов’язаних процесів та управління ними як системою сприяє організації більш результативно та ефективно досягати цілі.

6. Постійне удосконалення. Постійне удосконалення загальних показників діяльності установи необхідно вважати незмінною її метою.

7. Прийняття рішень на підставі фактів. Ефективні рішення ґрунтуються на аналізі даних та інформації.

8. Взаємовигідні стосунки з постачальниками. Установа та її постачальники є взаємозалежними, і взаємовигідні стосунки підвищують здатність обох сторін створювати цінності [6, с.5].

Отже, мінімальне дотримання перерахованих нами восьми принципів управління уможливить зацікавленим сторонам одержати переваги такі, наприклад, як зростання прибутків, створення цінностей та підвищення стабільності.

Окрім того, на систему електронного надання документаційного забезпечення впливає і грамотне дотримання оформлення електронних документів. Оскільки, «склад та порядок розміщення обов'язкових реквізитів електронних документів визначається законодавством». Відповідно до Закону України «Про електронні документи та електронний документообіг» [49], «електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму». Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною.

Оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до Закону України «Про електронні довірчі послуги». У разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа [49].

Якщо автором створюються ідентичні за документарною інформацією та реквізитами електронний документ та документ на папері, кожен з документів є оригіналом і має однакову юридичну силу. Оригінал електронного документа повинен давати змогу довести його цілісність та справжність у порядку, визначеному законодавством; у визначених законодавством випадках може бути пред'явлений у візуальній формі

відображення, в тому числі у паперовій копії. Електронна копія електронного документа засвідчується у порядку, встановленому законом [49].

Копією документа на папері для електронного документа є візуальне подання електронного документа на папері, яке засвідчене в порядку, встановленому законодавством. Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму. Допустимість електронного документа як доказу не може заперечуватися виключно на підставі того, що він має електронну форму. Електронний документ не може бути застосовано як оригінал:

1) свідоцтва про право на спадщину;

2) документа, який відповідно до законодавства може бути створений лише в одному оригінальному примірнику, крім випадків існування централізованого сховища оригіналів електронних документів;

3) в інших випадках, передбачених законом.

Нотаріальне посвідчення цивільно-правової угоди, укладеної шляхом створення електронного документа (електронних документів), здійснюється у порядку, встановленому законом [49].

У цілому, електронний документообіг (обіг електронних документів) - сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів. Порядок електронного документообігу визначається державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності згідно з законодавством.

Відправлення та передавання електронних документів здійснюються автором або посередником в електронній формі за допомогою засобів інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем або шляхом відправлення електронних носіїв, на яких записано цей документ. Якщо автор і адресат у письмовій формі попередньо не домовилися

про інше, датою і часом відправлення електронного документа вважаються дата і час, коли відправлення електронного документа не може бути скасовано особою, яка його відправила. У разі відправлення електронного документа шляхом пересилання його на електронному носії, на якому записано цей документ, датою і часом відправлення вважаються дата і час здавання його для пересилання [49].

Вимоги підтвердження факту одержання документа, встановлені законодавством у випадках відправлення документів рекомендованим листом або передавання їх під розписку, не поширюються на електронні документи. У таких випадках підтвердження факту одержання електронних документів здійснюється згідно з вимогами Закону. Електронний документ вважається одержаним адресатом із часу надходження авторові повідомлення в електронній формі від адресата про одержання цього електронного документа автора, якщо інше не передбачено законодавством або попередньою домовленістю між суб'єктами електронного документообігу.

Якщо попередньою домовленістю між суб'єктами електронного документообігу не визначено порядок підтвердження факту одержання електронного документа, таке підтвердження може бути здійснено в будь-якому порядку автоматизованим чи іншим способом в електронній формі або у формі документа на папері. Зазначене підтвердження повинно містити дані про факт і час одержання електронного документа та про відправника цього підтвердження [49].

У випадку ненадходження до автора підтвердження про факт одержання цього електронного документа вважається, що електронний документ не одержано адресатом. Якщо автор і адресат у письмовій формі попередньо не домовилися про інше, електронний документ вважається відправленим автором та одержаним адресатом за їх місцезнаходженням (для фізичних осіб - місцем проживання), у тому числі якщо інформаційна, телекомунікаційна, інформаційно-телекомунікаційна система, за допомогою якої одержано

документ, знаходиться в іншому місці. Місцезнаходження (місце проживання) сторін визначається відповідно до законодавства [49].

Перевірка цілісності електронного документа проводиться шляхом перевірки електронного підпису. Суб'єкти електронного документообігу повинні зберігати електронні документи на електронних носіях інформації у формі, що дає змогу перевірити їх цілісність на цих носіях. Строк зберігання електронних документів на електронних носіях інформації повинен бути не меншим від строку, встановленого законодавством для відповідних документів на папері. У разі неможливості зберігання електронних документів на електронних носіях інформації протягом строку, встановленого законодавством для відповідних документів на папері, суб'єкти електронного документообігу повинні вживати заходів щодо дублювання документів на кількох електронних носіях інформації та здійснювати їх періодичне копіювання відповідно до порядку обліку та копіювання документів, встановленого законодавством [49].

Якщо неможливо виконати зазначені вимоги, електронні документи повинні зберігатися у вигляді копії документа на папері (у разі відсутності оригіналу цього документа на папері). При копіюванні електронного документа з електронного носія інформації обов'язково здійснюється перевірка цілісності даних на цьому носії. При зберіганні електронних документів обов'язкове додержання таких вимог:

1) інформація, що міститься в електронних документах, повинна бути доступною для її подальшого використання;

2) має бути забезпечена можливість відновлення електронного документа у тому форматі, в якому він був створений, відправлений або одержаний;

3) у разі наявності повинна зберігатися інформація, яка дає змогу встановити походження та призначення електронного документа, а також дату і час його відправлення чи одержання [49].

Електронний документообіг здійснюється відповідно до законодавства України або на підставі договорів, що визначають взаємовідносини суб'єктів електронного документообігу. Використання електронного документа у цивільних відносинах здійснюється згідно із загальними вимогами вчинення правочинів, встановлених цивільним законодавством. Якщо в процесі організації електронного документообігу виникає необхідність у визначенні додаткових прав та обов'язків суб'єктів електронного документообігу, що не визначені законодавством, такі права та обов'язки можуть встановлюватися цими суб'єктами на договірних засадах. Особи, винні в порушенні законодавства про електронні документи та електронний документообіг, несуть відповідальність згідно з законами України [49].

Отже, законодавчо-правові основи електронного надання документаційного забезпечення регулюють процеси, пов'язані як із адміністративною, так і комерційною діяльністю установ державної чи приватної форм власності. На законодавчому рівні обґрунтовано доцільність повного переходу на систему електронного документаційного забезпечення, що буде проаналізовано нами у підрозділі 1.2.

1.2. Організація електронного документаційного забезпечення

Організація електронного документаційного забезпечення, з огляду на світовий досвід, є складовою успішності функціонування та підвищення конкурентноспроможності установи. Адже, скерована на широке використання сучасних інформаційно-комунікаційних технологій для досягнення необхідного рівня ефективності та результативності. Інструменти е-документаційного забезпечення здатні забезпечити значне покращення якості обслуговування фізичних і юридичних осіб, підвищення відкритості, прозорості та ефективності діяльності установ різного типу власності.

Відповідно до теорії сучасного документознавства, організація е-документаційного забезпечення ґрунтується на таких принципах:

- рух документів повинен мати мінімальну кількість повернень на попередні етапи;

- документи повинні спрямовуватись виконавцям у відповідності з їх обов'язками, щоб уникнути дублювання операцій [38, с.78].

Е-документаційне забезпечення охоплює три основні завдання стосовно програмних засобів автоматизації:

- документування (створення документів, які підтримують і реєструють управлінську діяльність, тобто їх підготовку, оформлення, узгодження та виготовлення);

- організація документообігу (забезпечення руху, пошуку, зберігання і використання документів);

- систематизація архівного зберігання документів [38, с.78].

Етапи переведення документа в електронну форму такі:

1. Сканування документа і створення його електронної копії у вигляді зображення (образ документа). У процесі сканування виконується візуальний контроль якості.

2. Розпізнавання сканованих документів - переведення зображення у текстовий документ. З точки зору переведення документа у електронний вид їх умовно поділяють на кілька типів (Рис. 1.1) [31, с.56]. Переведення кожного із видів документів у електронну форму має такі особливості:

- для фотографій достатньо їх електронного зображення;

- при переведенні текстів - їх необхідно розпізнати, можливо, відновити форматування:

- при введенні анкет, бюлетенів для голосування та ін., зазвичай, не потрібно зображення власне документа, а достатньо лише інформації про те, за кого віддано голос.

Рис. 1.1. Типи поділу електронних документів

Служби документаційного забезпечення управління можуть мати різні назви: управління справами, відділ діловодства, відділ документаційного забезпечення управління, загальний відділ, секретаріат, служба управління документацією та ін. Назва служби документаційного забезпечення управління не має принципового значення [31, с.57]. Структура служби документаційного забезпечення управління залежить від обсягу документообігу, від технології роботи з документами і може бути представлена, наприклад, такими підрозділами:

- секретаріат (приймальня, секретаріат директора, секретаріати заступників, секретаріат колегії, протокольне бюро);

- канцелярія (експедиція, бюро реєстрації, копіювально-множильне бюро);

- відділ листів;

- відділ упровадження технічних засобів вдосконалення документообігу;

- архів [31, с.57].

Деякі з цих підрозділів можуть існувати як самостійні структури або об’єднуватись у межах інших структур. У невеликих установах служба документаційного забезпечення як самостійний структурний підрозділ може не існувати, оскільки, робота з документами може бути покладена на офіс-

менеджера чи іншу особу. Основними завданнями служби документаційного забезпечення є:

- забезпечення єдиного порядку документування і роботи з документами в установі у відповідності з чинними нормативами;

- удосконалення форм і методів роботи з документами з урахуванням автоматизації діловодних процесів [31, с.57].

У відповідності із завданнями, служба документаційного забезпечення виконує такі функції, пов'язані з документуванням управлінської діяльності:

- розробка бланків документів і забезпечення їх виготовлення;

- забезпечення копіювання та тиражування документів;

- контроль за якістю підготовки і оформлення документів, а також за дотриманням встановленої процедури узгодження і засвідчення документів;

- функції, пов'язані з організацією роботи з документами:

- встановлення єдиного порядку проходження документів (документообігу установи) [31, с.59].

Крім того, удосконалення е-документаційного забезпечення є базовою передумовою для ефективної цифрової економіки і цифрового ринку, його подальшої інтеграції до єдиного цифрового ринку ЄС (EU Digital Single Market Strategy). Інтеграція, за дослідниками, може здійснюватися декількома шляхами. Так, трансформаційний шлях акцентує на посиленні функціональних можливостей е-документаційного забезпечення, зниженні витрат на реалізацію повноважень шляхом застосування сучасних інноваційних підходів, методологій та технологій, включаючи Інтернет речей, хмарні інфраструктури, Blockchain, Mobile ID, shareding economy, просування методики опрацювання даних великих обсягів (Big Data), нормативно-правове врегулювання принципів «цифровий за замовчуванням», «одноразове введення інформації» та «сумісність за замовчуванням» [25, с.89].

Застосування перспективних форм організації виконання завдань і проєктів розвитку е-документаційного забезпечення через підтримку доступних та прозорих, безпечних та не корупційних, найменш затратних,

швидких та зручних електронних послуг уможливить покращити якість надання послуг фізичним та юридичним особам, підвищити їхню мобільність та конкурентоспроможність, зменшить корупційні ризики та забезпечить, щоб електронні послуги обслуговували економіку майбутнього. З урахуванням переваг технологій електронних послуг основними заходами із забезпечення розвитку е-документаційного забезпечення є:

- удосконалення вже наявних електронних послуг, у тому числі адміністративних, надання інтегрованих електронних послуг за життєвими та бізнес-ситуаціями;

- подальше удосконалення принципу єдиного вікна («one-stop-shop») шляхом забезпечення розвитку та функціонування Єдиного державного порталу адміністративних послуг як єдиної точки доступу фізичних та юридичних осіб до електронних послуг [25, с.90];

- удосконалення електронних публічних закупівель, електронних договорів і рахунків, електронних аукціонів;

- стимулювання використання електронних послуг фізичними та юридичними особами.

У свою чергу, відповідно до Закону України «Про доступ до публічної інформації» [48] оприлюднення публічної інформації у формі відкритих даних для вільного використання дасть змогу створити додаткові механізми реалізації права на доступ до інформації, що перебуває у володінні органів влади, підвищити прозорість діяльності таких органів, забезпечить вільний обіг інформації та можливість її подальшого використання з метою реалізації особистих прав та свобод людини і громадянина, розвитку інновацій та стимулювання ведення господарської діяльності, а також запобігання та викриття корупції.

З урахуванням переваг технологій відкритих даних основними заходами е-документаційне забезпечення включає:

- формування та розвиток інфраструктури відкритих даних на базі єдиного державного веб-порталу відкритих даних, інтегрованих з ним інших

веб-порталів відкритих даних, публічних інтерфейсів прикладного програмування (API), відкритих стандартів та форматів [48];

- оприлюднення та регулярне оновлення наборів даних у формі відкритих даних відповідно до суспільного інтересу, кращих світових практик, встановлених вимог щодо якості даних і відкритості та прозорості діяльності;

- стимулювання розвитку на базі відкритих даних загальнодоступних проектів і сервісів (соціальних, громадських, медійних та комерційних), у тому числі у співпраці з органами влади, для підвищення відкритості та ефективності їх діяльності, надання якісних послуг та розвитку інноваційного бізнесу [48].

Активне впровадження інформаційно-комунікаційних технологій розширює можливості впливу на прийняття управлінських рішень, створює умови для формування якісно нового рівня взаємодії між установою та громадяни. З урахуванням переваг електронних інструментів основні заходи передбачають:

- удосконалення інституту електронних звернень та електронних петицій;

- удосконалення інструментів «відкритий бюджет», «громадський бюджет», он-лайн обговорення проєктів нормативно-правових актів та інших інструментів у прийнятті управлінських рішень [17, с.346];

- удосконалення електронних форм зворотного зв’язку на офіційних веб-сайтах, у тому числі тематичних, для отримання якісного зворотного зв’язку з різних питань;

- широке залучення громадських об’єднань та профільних асоціацій до планування розвитку та моніторингу стану розвитку е-документаційного забезпечення;

- подальше стимулювання використання електронних інструментів у сфері е-документаційного забезпечення [17, с.347].

Маємо наголосити, що подальший розвиток інфраструктури електронної ідентифікації дасть змогу забезпечити зручний та безпечний

доступ до визначених даних з інформаційних систем, різноманітних електронних послуг та інтерактивних інструментів без необхідності використання декількох облікових записів в різних інформаційних системах, сприятиме розвитку електронних форм взаємодії. З урахуванням переваг технологій електронної ідентифікації основними заходами із забезпечення подальшого розвитку е-документаційного забезпечення є:

- розвиток електронних довірчих послуг відповідно до вимог Регламенту (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 р. про електронну ідентифікацію та довірчі послуги для електронних транзакцій в межах внутрішнього ринку та про скасування Директиви 1999/93/ЄС [28, с.24];

- сприяння наповненню єдиного демографічного реєстру та поширенню паспортів громадянина України у формі ID-карти;

- розвиток існуючих та запровадження нових схем і засобів електронної ідентифікації та встановлення рівнів довіри до них (у тому числі Mobile ID, Bank ID);

- реалізація принципу «single-sign-on» шляхом впровадження інтегрованої системи електронної ідентифікації та автентифікації і повторного використання в інформаційно-телекомунікаційних системах [28, с.25].

Запровадження автоматизованого обміну даними між інформаційно-телекомунікаційними системами дасть змогу забезпечити підвищення ефективності роботи шляхом скорочення часу отримання необхідних даних, покращення якості та актуальності опрацьованих даних, ліквідації багаторазового збору та дублювання даних в різних інформаційних системах, покращення доступності інформаційних ресурсів та їх систематизацію. З урахуванням переваг технологій електронної взаємодії основними заходами із забезпечення подальшого розвитку е-документаційного забезпечення є:

- подальше запровадження системи електронної взаємодії електронних інформаційних ресурсів;

- удосконалення вже наявної електронної взаємодії суб'єктів владних повноважень на базі системи електронної взаємодії електронних інформаційних ресурсів, у тому числі підключення базових державних реєстрів і баз даних, центрів надання адміністративних послуг, а також розвиток транскордонної електронної взаємодії [28, с.30];

- удосконалення організаційної, технічної та семантичної інтероперабельності інформаційно-телекомунікаційних систем, у тому числі поширення унікального номера запису в реєстрі єдиного демографічного реєстру для зв'язування даних в різних державних реєстрах та базах даних.

Науковці переконані, що е-документаційне забезпечення і надалі «сприятиме підвищенню оперативності та ефективності у вирішенні поставлених перед установою задач у розрізі роботи із документами за рахунок прискорення та оптимізації внутрішніх процесів діловодства, посилення виконавської дисципліни та відповідного поточного контролю за нею, зміцнення інформаційно-аналітичної підтримки прийняття управлінських рішень, підвищення відкритості та прозорості діяльності» [33]. З урахуванням переваг технологій електронного документообігу завданнями є:

- подальший розвиток систем внутрішнього електронного документообігу та системи електронної взаємодії між установами різних форм власності;

- запровадження державного електронного архіву та електронних архівів і визначення порядку передачі електронних документів в державний електронний архів та порядку їх архівного зберігання;

- визначення порядку приймання-передачі електронних документів до державних архівних установ;

- визначення вимог до формату уніфікованого інформаційного об'єкта, що призначений для обміну електронними документами [33].

Зрештою, ефективне управління будь-якою установою у сучасних умовах неможливе без широкого застосування сучасних інструментів е-

документаційного забезпечення, у тому числі автоматизації обробки великих об’ємів даних та інформаційно-аналітичного забезпечення прийняття управлінських рішень, оптимізації та автоматизації адміністративних процесів, запровадження електронних форм взаємодії. Основними завданнями із забезпечення розвитку е-документаційного забезпечення в установах різних форм власності є запровадження інформаційно-телекомунікаційних систем підтримки прийняття управлінських рішень та автоматизації адміністративних процесів (зокрема з використанням перспективних геоінформаційних технологій, Інтернету речей, технологій опрацювання даних великих обсягів (Big Data) і Blockchain) [33].

Отже, сучасна організація е-документаційного забезпечення обумовлює відкритість і прозорість діяльності установи, зменшує витрати на механічну роботу з документами, фактично усуває повторність та одноманітність процесів, пов’язаних із життєвим циклом документа, зрештою, що є найбільш актуальним, зводить нанівець корупційну складову.

1.3. Захист інформації в електронному документообігу

Повноцінне функціонування системи е-документаційного забезпечення неможливе без захисту інформації. Накопичення персональних даних, створення клієнтської бази, зрештою, обробка е-документів – все це вимагає захисту від вірусів, втручання та просто витоку інформації для конкурентів. За теорією, захист інформації в системі – «діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі; комплексна система захисту інформації - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації» [33]. Суб'єктами відносин, пов’язаних із захистом інформації в системах, є:

- володільці інформації;
- власники системи;
- користувачі;

- спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв’язку та захисту інформації і підпорядковані йому регіональні органи [57].

Одним із видів захисту інформації є криптографічний захист, за якого відбувається перетворення інформації «із використанням спеціальних даних (ключових даних) із метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо» [57]. Для забезпечення захисту інформації у системі створюється комплексна система захисту інформації, яка призначається для захисту інформації від:

- витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;

- несанкціонованих дій з інформацією, у тому числі з використанням комп’ютерних вірусів;

- спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування [57].

Відповідно до пунктів Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації (далі - КЗІ), «криптографічне перетворення інформації - перетворення інформації з використанням ключових даних з метою приховування (відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства, дати створення тощо» . У свою чергу, «шифрування - перетворення відкритого тексту в шифротекст (зашифрування) та відновлення відкритого тексту із шифротексту (розшифрування) при відомих ключових даних» [57]. Залежно від виконання встановлюються такі види засобів КЗІ:

- вид А - засоби, які на конструктивному, алгоритмічному та програмному рівнях є єдиними виробами, що функціонують (експлуатуються) відокремлено від будь-яких інших технічних засобів;

- вид Б - засоби, які на конструктивному, алгоритмічному та програмному рівнях є єдиними виробами та призначені для використання у складі комплексів оброблення та передавання інформації.

Засоби виду Б поділяються на:

- підвид Б1 - вироби, які встановлюються в розрив телекомунікаційного каналу та/або розділяють потоки захищеної інформації та інформації, що підлягає захисту, а також вироби, що забезпечують відокремлення оброблення захищеної інформації та інформації, що підлягає захисту, в обчислювальній системі [57];

- підвид Б2 - апаратні, апаратно-програмні або програмні вироби, які підключаються до інших засобів та виконують функції криптографічних перетворень у взаємодії з ними або під їх управлінням;

- вид В - криптографічні модулі, які не використовуються (не експлуатуються) окремо, а застосовуються як складові частини при побудові засобів КЗІ видів А та Б [57].

Залежно від призначення встановлюються такі категорії засобів КЗІ:

- засоби шифрування інформації (засоби категорії «Ш»);

- засоби, призначені для виготовлення ключових даних або ключових документів (незалежно від виду носія ключової інформації) та управління ключовими даними, що використовуються в засобах КЗІ (засоби категорії «К»);

- засоби захисту від нав'язування неправдивої інформації або захисту від несанкціонованої модифікації, що реалізовують алгоритми криптографічного перетворення інформації (далі - криптоалгоритми), у тому числі засоби імітозахисту та електронного цифрового підпису (засоби категорії «П»);

- засоби захисту інформації від несанкціонованого доступу (у тому числі засоби розмежування доступу до ресурсів електронно-обчислювальної техніки), у яких реалізовані криптоалгоритми (засоби категорії «Р») [57];

- засоби (засоби, об'єднані в комплекси), спеціально призначені для розроблення, дослідження, виробництва та випробувань засобів КЗІ, у тому числі програмування та/або запису в їх апаратні компоненти (програмовані логічні інтегральні схеми, контролери), перевірки та контролю правильності реалізації в засобах КЗІ криптографічних функцій (засоби категорії «З»).

Захист інформації від витоку технічними каналами забезпечується в системі у випадку, коли в ній обробляється інформація, що становить державну таємницю, або коли відповідне рішення щодо необхідності такого захисту прийнято власником (розпорядником) інформації. Захист інформації від несанкціонованих дій, у тому числі від комп'ютерних вірусів, забезпечується в усіх системах [57].

Захист інформації від спеціального впливу на засоби обробки інформації забезпечується в системі, якщо рішення про необхідність такого захисту прийнято власником (розпорядником) інформації . Відповідальність за забезпечення захисту інформації в системі, своєчасне розроблення необхідних для цього заходів та створення системи захисту покладається на керівника (заступника керівника) установи, яка є власником (розпорядником) системи, та керівників її структурних підрозділів, що забезпечують створення та експлуатацію системи.

Організація та проведення робіт із захисту інформації в системі здійснюється службою захисту інформації, яка забезпечує визначення вимог до захисту інформації в системі, проєктування, розроблення і модернізацію системи захисту, а також виконання робіт з її експлуатації та контролю за станом захищеності інформації. Служба захисту інформації утворюється згідно з рішенням керівника організації, що є власником (розпорядником) системи. У випадку, коли обсяг робіт, пов'язаних із захистом інформації в системі, є незначний, захист інформації може здійснюватися однією особою.

Захист інформації на всіх етапах створення та експлуатації системи здійснюється відповідно до розробленого службою захисту інформації плану захисту інформації в системі [57].

План захисту інформації в системі містить:

- завдання захисту, класифікацію інформації, яка обробляється в системі, опис технології обробки інформації;

- визначення моделі загроз для інформації в системі;

- основні вимоги щодо захисту інформації та правила доступу до неї в системі;

- перелік документів, згідно з якими здійснюється захист інформації в системі;

- перелік і строки виконання робіт службою захисту інформації [57].

На підставі укладеного договору або за дорученням власник системи може надати право розпоряджатися системою іншій фізичній або юридичній особі - розпоряднику системи. Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються володільцем інформації. Порядок доступу до державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством.

У випадках, передбачених законом, доступ до інформації в системі може здійснюватися без дозволу її володільця в порядку, встановленому законом. Власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із володільцем інформації, якщо інше не передбачено законом [57]. Власник системи на вимогу володільця інформації надає відомості щодо захисту інформації в системі. Власник системи надає користувачеві відомості про правила і режим роботи системи та забезпечує йому доступ до інформації в системі відповідно до визначеного порядку доступу.

Власник системи, яка використовується для обробки інформації з іншої системи, забезпечує захист такої інформації в порядку та на умовах, що визначаються договором, який укладається між власниками систем, якщо інше не встановлено законодавством. Власник системи, яка використовується для обробки інформації з іншої системи, повідомляє власника зазначеної системи про виявлені факти несанкціонованих дій щодо інформації в системі. Умови обробки інформації в системі визначаються власником системи відповідно до договору з володільцем інформації, якщо інше не передбачено законодавством [57].

Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності комплексної системи захисту інформації здійснюється за результатами державної експертизи, яка проводиться з урахуванням галузевих вимог та норм інформаційної безпеки у порядку, встановленому законодавством [57].

Підтвердження відповідності та проведення державної експертизи засобів технічного і криптографічного захисту інформації здійснюються в порядку, встановленому законодавством. Для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації, та засоби технічного захисту інформації які мають позитивний експертний висновок за результатами державної експертизи у сфері технічного захисту інформації або сертифікат відповідності, виданий органом з оцінки відповідності, який акредитовано:

- національним органом України з акредитації;

- національним органом з акредитації іншої держави, якщо і національний орган України з акредитації, і національний орган з акредитації

такої держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності [5].

Державні інформаційні ресурси та інформація з обмеженим доступом, крім державної таємниці, службової інформації та державних і єдиних реєстрів, створення та забезпечення функціонування яких визначено законами, можуть оброблятися в системі без застосування комплексної системи захисту інформації у разі виконання всіх таких умов:

- підтвердження відповідності системи управління інформаційною безпекою за результатами процедури з оцінки відповідності національним стандартам України щодо систем управління інформаційною безпекою, яка проведена органом з оцінки відповідності, акредитованим національним органом України з акредитації чи національним органом з акредитації іншої держави, якщо і національний орган України з акредитації, і національний орган з акредитації такої держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності [5];

- використання для захисту інформації в системі засобів криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації;

- жоден з елементів системи не може бути розташований на територіях України, на яких органи державної влади України тимчасово не здійснюють своїх повноважень, на територіях держав, визнаних Верховною Радою України державами-агресорами, на територіях держав, щодо яких застосовані санкції відповідно до Закону України «Про санкції» [61], та на територіях держав, які входять до митних союзів із такими державами;

- виконання особливих вимог, встановлених Кабінетом Міністрів України до забезпечення захисту інформації в системах залежно від категорії

державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, що обробляються [5].

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи. Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Про спроби та/ або факти несанкціонованих дій у системі щодо державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган. Вимоги до забезпечення захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України. Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації [5]:

- розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;

- визначає вимоги та порядок створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

- організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації [5];

- здійснює контроль за забезпеченням захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

- здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дає рекомендації з питань запобігання такій загрозі.

Державні органи в межах своїх повноважень за погодженням відповідно із спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкованим йому регіональним органом встановлюють особливості захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом. Особливості захисту інформації в системах, які забезпечують банківську діяльність, встановлюються Національним банком України [5].

Особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно із законом. Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, визначено інші правила, ніж ті, що передбачені цим Законом, застосовуються норми міжнародного договору.

Отже, функціонування системи е-документаційного забезпечення сучасної установи потребує належного та якісного захисту інформації. Маємо констатувати, що чинні нормативно-законодавчі документи на сьогодні уповні віддзеркалюють та пояснюють стан захисту інформації, включаючи негативний вплив збоку інших держав, про що висвітлено у Законі України «Про санкції».

У цілому, теоретичні основи організації роботи механізмів електронного надання документаційного забезпечення у розділі проаналізовані з огляду на сучасний стан законів України та Положень.

РОЗДІЛ ІІ. СИСТЕМА ЕЛЕКТРОННОГО НАДАННЯ ДОКУМЕНТАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СУЧАСНОЇ УСТАНОВИ (НА ПРИКЛАДІ ТОВАРИСТВА З ДОДАТКОВОЮ ВІДПОВІДАЛЬНІСТЮ СТРАХОВА КОМПАНІЯ «Ю.Ес.Ай.»)

2.1. Нормативне підґрунтя механізмів електронного надання документаційного забезпечення у Товаристві з додатковою відповідальністю страхова компанія «Ю.Ес.Ай»

На практичному рівні механізми електронного надання документаційного забезпечення будуть розглянуті нами на прикладі української страхової компанії. Також, упродовж ІІ розділу ми проаналізуємо як саме здійснюється документаційне забезпечення при роботі фахівців різних структурних підрозділів страхової компанії із внутрішніми та зовнішніми е-документами. За М. Булавою, лише «сучасна, інноваційна страхова компанія, яка успішно працює на страховому ринку України, готова запропонувати повний спектр страхових послуг» [4, с.86]. Однією із потужних страхових компаній на сучасному ринку послуг є Товариство з додатковою відповідальністю страхова компанія «Ю.Ес.Ай.» (далі - Компанія). Компанія є Асоційованим членом Моторно (Транспортного) Страхового Бюро України (МТСБУ), членом Ліги Страхових організацій України та Асоціації « Страховий бізнес» [37].

Товариство проводить свою діяльність на підставі 53- х ліцензій із обов'язкових та добровільних видів страхування. За даними рейтингу «Insurance Top» за підсумками І кварталу 2024 року СК «Ю.Ес.Ай.» увійшла в ТОП-5 на ринку обов'язкового страхування цивільно-правової відповідальності власників наземного транспорту, в ТОП-15 з добровільного страхування на випадок хвороби (12 місце) та в ТОП-25 зі страхування туристів (добровільне страхування медичних витрат, 21 місце). Страхова компанія «Ю.Ес.Ай.» є другою в рейтингу за рівнем виплат [37].

Товариство з додатковою відповідальністю «Страхова компанія «Ю.Ес.Ай.» (стара назва ТДВ «СК «ПСК – ЗАХІД») зареєстрована 11 червня 2003 р. Радивілівською районною державною адміністрацією. Перереєстрація проведена 27.12.2007 р. Шевченківською районною у м. Києві державною адміністрацією, 24.03.2010 року проведена перереєстрація Шевченківською районною у м. Києві державною адміністрацією. У зв'язку зі зміною юридичної адреси проведена перереєстрація 04.02.2014 р. Печерською районною у м. Києві державною адміністрацією. У зв'язку зі зміною юридичної адреси проведена перереєстрація 23.09.2016 р. Шевченківською районною у м. Києві державною адміністрацією [37].

У зв'язку зі зміною власників, пов'язаною з цим зміною в установчих документах та зміною посадових осіб Компанії проведена перереєстрація 23.05.2017 р. Шевченківською районною у м. Києві державною адміністрацією. На посаду Генерального директора ТДВ «Страхова компанія «Ю.Ес.Ай.» (стара назва ТДВ «СК «ПСК – ЗАХІД») було обрано громадянку України Ким Г. Г. з 30.05.2017 р., зміни затверджені Протоколом №69 позачергових Загальних зборів учасників Компанії від 29.05.2017 р. Протягом звітного періоду Товариство пройшло процедуру перереєстрації, внаслідок чого відбулася зміна найменування та адреси реєстрації (місцезнаходження) Товариства [37].

Так, з 13.07.2017 р., повне найменування Товариства: Товариство з додатковою відповідальністю «Страхова компанія «Ю.Ес.Ай.» (скорочене - ТДВ «СК «Ю.Ес.Ай.»). Місцезнаходження: проспект Героїв Сталінграда, 4, корпус 6а, Київ, 04210, Україна. Компанія успішно здійснює добровільне страхування (за 13 ліцензіями), обов'язкове страхування (за 9 ліцензіями), з 26.04.2017 р. є членом Моторно (транспортного) страхового бюро України, з листопада 2017 року ЛСОУ. Компанія має безстрокові ліцензії Державної комісії з регулювання ринків фінансових послуг України на здійснення страхування [37].

Основним видом діяльності ТДВ «СК «Ю.Ес.Ай.» є надання страхових послуг на території України (Код КВЕД 65.12 Інші види страхування, крім страхування життя). ТДВ «СК «Ю.Ес.Ай.» не має відокремлених підрозділів на території України. Органами управління Товариства є Загальні Збори учасників. Загальні Збори учасників є вищим органом управління Товариства. Вони складаються з учасників Товариства або призначених ними представників. Чергові Збори Товариства скликаються не рідше одного разу на рік. Діяльність Загальних Зборів учасників Товариства відповідає всім вимогам законодавства, статуту і внутрішніх положень [37].

Станом на 31.12.2023 р. Статутний капітал Компанії «Ю.Ес.Ай.» (Товариства) становить 16 000,00 тисяч гривень. Розподіл часток у Товаристві здійснюється так:

1) ТОВ «БК-ЕКСПЕРТ» - частка у статутному капіталі ТДВ становить 99,98% (15 996,8 тис. грн.);

2) Берназюк Олександр Олександрович - володіє часткою у статутному капіталі ТДВ у розмірі 0,019% (3,04 тис. грн.);

3) Біла Тетяна Павлівна - володіє часткою у статутному капіталі ТДВ у розмірі 0,001% (0,16 тис. грн.) [37].

Діяльність Страхової компанії здійснюється на території України. У зв’язку з анексією Автономної республіки Крим, проведенням антитерористичної операції на сході України та після початку повномасштабного вторгнення російською федерацією політична та економічна ситуація в Україні була вкрай нестабільною та продовжує залишатися непередбаченою. Вказані події призвели до спаду валового внутрішнього продукту, суттєвої девальвації національної валюти по відношенню до основних валют, нестабільності фондового ринку, погіршення ліквідності банківського сектору, збільшення безробіття. Політичні зміни призвели зміни у законодавчій, податковій, регуляторній основі діяльності компаній в Україні [37].

Спеціалісти переконані, що майбутня стабільність економіки в значній мірі залежить від успішності реформ та ефективності економічних, фінансових та монетарних заходів, що будуть здійснюватися урядом країни. Станом на 2023 рік Страхова компанія не мала нерухомості та інших активів, що розташовані на території Автономної республіки Крим та у Луганській та Донецькій областях, інших тимчасово окупованих територіях. Компанія постійно стежить за поточним станом подій, зміною законодавства і вживає всіх необхідних заходів з метою підтримання сталої діяльності Компанії. Вплив кризи на результати діяльності та фінансовий стан Компанії не може бути належним чином оцінений зараз, однак у майбутньому він може досягти суттєвого рівня. Процес, який використовується для прийняття рішень щодо припущень - складний, особливо по ризикам, пов’язаним із договорами страхування. Найбільшими ризиками Компанії є страхові збитки, пов’язані зі страхування автотранспортних засобів (КАСКО), медичного страхування (безперервне страхування здоров’я), страхування фінансових ризиків та інше [37].

Для оцінки своїх зобов’язань з виплати страхових відшкодувань Компанія використовує припущення, які базуються, в основному, на власних аналітичних даних. Внутрішні дані отримуються, головним чином, із квартальних звітів Компанії про страхові збитки. Для оцінки адекватності резервів незароблених премій використовуються загальноприйняті актуарні методи, методи математичного моделювання комбінованої збитковості, теорії випадкових процесів, методи теорії ймовірностей та математичної статистики [37].

Загалом, усі послуги, що надаються страховою кампанією «Ю.Ес.Ай.», обов’язково супроводжуються е-документаційним забезпеченням. Зокрема, одним із важливих та найбільш затребуваних страхових документів є договір страхування. За теорією як документознавства, так і страхової справи договір страхування або поліс - письмова угода між страхувальником і страховиком, відповідно до якої страховик бере на себе зобов'язання у разі настання

страхового випадку виплатити страхову суму або відшкодувати завданий збиток у межах страхової суми страхувальнику чи іншій особі, визначеній страхувальником, або на користь якої укладено договір страхування (подати допомогу, виконати послугу тощо), а страхувальник зобов'язується сплачувати страхові платежі у визначені терміни та виконувати інші умови договору.

Основні вимоги до змісту та порядку укладання договорів страхування, права та обов'язки сторін визначені в Законі України «Про страхування» [63]. Договір страхування повинен містити: назву документа; назву та адресу страховика; прізвище, ім'я, по батькові або назву страхувальника і його адресу; зазначення об'єкта страхування; розмір страхової суми; перелік страхових випадків; визначення розміру тарифу, розмір страхових внесків і терміни їх сплати; термін дії договору; порядок зміни і припинення дії договору; права та обов'язки сторін і відповідальність за невиконання або неналежне виконання умов договору; інші умови за згодою сторін; підписи сторін [63].

Договір страхування може бути укладено на будь-який строк, за домовленістю сторін. Умови стандартних договорів страхування належать до категорії нормативно установлених. Страховик і страхувальник не можуть вносити будь-які зміни або інші умови до стандартних договорів страхування на власний розсуд. Підставою для укладення договору є заява страхувальника. Вона містить виражений та адресований страховику намір страхувальника укласти договір страхування на відповідних умовах. У ній обов'язково повинні бути викладені всі суттєві особливості ризику, який передбачається страхувати.

Страховик, розглянувши заяву, може прийняти її або відхилити. Підтвердженням укладення відповідного договору страхування є страховий поліс (свідоцтво, сертифікат), який містить усі істотні умови договору страхування і видається страхувальнику. Договори страхування можуть укладатися з фізичними та юридичними особами та передбачати виконання

зобов’язання на користь третьої особи. Виплата страхових сум і страхового відшкодування проводиться страховиком згідно з договором страхування на підставі заяви страхувальника (його правонаступника або третіх осіб, визначених умовами страхування) та страхового акта (аварійного сертифіката), який складається страховиком або уповноваженою ним особою [63].

Страховик може відмовити у виплаті страхової суми або страхового відшкодування у випадках:

- навмисних дій страхувальника або особи, на користь якої укладено договір страхування, спрямованих на настання страхового випадку;

- скоєння страхувальником або іншою особою, на користь якої укладено договір страхування, умисного злочину, що призвів до страхового випадку;

- подання страхувальником свідомо неправдивих відомостей про об'єкт страхування;

- отримання страхувальником повного відшкодування збитків за майновим страхуванням від особи, винної в їхньому заподіянні [63];

- несвоєчасного повідомлення страхувальником про настання страхового випадку без поважних причин або створення страховикові перешкод у визначенні обставин, характеру та розміру збитків тощо.

Рішення про відмову у виплаті страхових сум приймається страховиком у строк не більший, ніж передбачено правилами страхування, та повідомляється страхувальнику в письмовій формі з обґрунтуванням причин відмови.

Відмову страховика у виплаті страхових сум може бути оскаржено страхувальником у судовому порядку. Дія договору страхування припиняється за згодою страхувальника та страховика, а також у випадку: закінчення строку його дії; виконання страховиком зобов’язань перед страхувальником у повному обсязі; несплати страхувальником страхових платежів у встановлені договором строки; ліквідації страхувальника - юридичної особи; смерті страхувальника-громадянина чи втрати ним

дієздатності; ліквідації страховика в порядку, передбаченому законодавством України; прийняття судового рішення про визнання договору страхування недійсним.

Дію договору страхування може бути достроково припинено за вимогою, якщо це передбачено умовами договору страхування. Також, однією із найбільш суттєвих та головних умов належного функціонування страхової компанії є клієнтська база. За дослідженням Г. Піратовського [40, с. 94], «більшість страховиків України вже зіткнулися з проблемою втрати клієнтів, оскільки за статистикою, лише 12 % страхових договорів завершуються пролонгацією, решта клієнтів перехоплюються іншими страховиками або виходять з-під страхового захисту». Імовірність втрати клієнта, який має один договір страхування, досягає 70 %, два – 40 %, три – не більше 10 % [40, с. 213]. Отже, сьогодні страховику, у першу чергу, необхідно для забезпечення ефективності бізнесу компанії зосередитися на наданні кращого персонального обслуговування клієнтів. Це досягається, зокрема, через формування, нарощування та управління взаємовідносинами з клієнтами. До речі, ця проблема ще більш загострилася під впливом світової фінансово-економічної кризи, яка розпочалася у 2008 році.

За С. Ткаченко, як наслідок, «перед менеджментом провідних страхових компаній особливо гостро постала проблема розвитку бізнесу в нових, більш жорстких і більш конкурентних умовах, коли мова йде вже не про збільшення обсягу страхової премії, а хоча б про утримання досягнутого рівня». За дослідником, у такій ситуації «на перше місце з більшою гостротою вийшла проблема утримання клієнтів» [71]. У сучасному страховому бізнесі клієнтоорієнтоване управління отримало розповсюдження під абревіатурою CRM. Дефініція CRM (Customer Relationship Management - управління взаємовідносинами з клієнтами) є сьогодні не лише найбільшим напрямком у царині страхових послуг, але й дійсно нагальною необхідністю. Основна ідея управління такими взаємовідносинами - підвищення стійкості та лояльності страхувальників, оскільки чим більш жорстка конкуренція на ринку страхових

послуг, тим складніше знайти та утримати клієнта, і тим більш затребуваними є такі технології [71].

Метою клієнтоорієнтованої компанії в умовах конкурентної боротьби є налагодження довготривалих відносин як з існуючими, так із потенційними клієнтами, що дозволить підвищити обсяги продажу страхових продуктів завдяки швидкому та якісному обслуговуванню. У свою чергу, клієнтоорієнтований підхід в установі скерований на використання надсучасних управлінських та інформаційних технологій, через які компанія здатна вибудовувати взаємовигідні відносини з клієнтами, запропонувавши кожному з них реальне індивідуальне обслуговування на всіх етапах надання страхового продукту [71].

Згідно з теорією менеджменту, виділяється зовнішнє та внутрішнє середовище компанії [1]. Для впровадження клієнтоорієнтованого підходу потрібно вирішити подвійне завдання:

- по-перше, ззовні переорієнтувати всю діяльність компанії з урахуванням інтересів клієнта;

- по-друге, зсередини досягти цієї мети при оптимальному використанні наявних в її розпорядженні ресурсів [1].

Центральним аспектом управління клієнтоорієнтованістю є, звичайно, споживачі (рис. 2.2.) [1]. У страховій послузі моменти придбання та користування рознесені в часі, до того ж, останній момент може і не наступити, у разі, якщо страховий випадок не відбудеться. За таких умов утримання клієнта залежить значною мірою від того, які взаємовідносини з ним сформувала страхова компанія за рамками врегулювання претензій. Не можна оминути увагою і такий фактор зовнішнього середовища страхової компанії як конкуренти, зміна поведінки яких впливає на конкурентоспроможність компанії в очах клієнтів [1].

Так, якщо конкурент удосконалив окремий страховий продукт та покращив систему врегулювання збитків, то, зрозуміло, що клієнти страховика очікуватимуть аналогічних дій, а в іншому разі – перейдуть до

інших страховиків. У разі несвоєчасної реакції на зміну конкурентного зовнішнього середовища відбуватиметься зниження рівня задоволеності клієнтів.

Рисунок 2.2. (за Ткаченко С. В.)

Варто підкреслити, що існує ряд причин, які перешкоджають повноцінному впровадженню систем CRM в практику українських страхових компаній, а саме:

1) недооцінка стратегічної ролі CRM у забезпеченні конкурентоспроможності та підвищенні ефективності діяльності на страховому ринку;

2) неготовність персоналу страховика до зміни принципів роботи з клієнтами;

3) відсутність фінансових можливостей для переоснащення базових інформаційних систем [1];

4) відсутність чіткої формалізованої методики оцінки та прогнозу ефективності впровадження систем CRM, яка могла б служити надійним інструментом підтримки прийняття рішення про інвестиції в реалізацію проектів [1].

Отже, нормативне підґрунтя механізмів електронного надання документаційного забезпечення у Товаристві з додатковою відповідальністю страхова компанія «Ю.Ес.Ай.» складається із дотримання положень закону України «Про страхування», внутрішньої політики страхової компанії, здатності її працівників переорієнтовуватися відповідно до викликів часу, професійності та клієнтоорієнтованості.

2.2. Функціональні можливості системи внутрішнього електронного документаційного забезпечення структурних підрозділів Товариства з додатковою відповідальністю страхова компанія «Ю.Ес.Ай»

Власне система внутрішнього е-документаційного забезпечення установ різних типів власності - це «сукупність процесів створення, оброблення, правлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконують із застосуванням перевірки цілісності та за потреби з підтвердженням факту одержання таких документів» [12]. Складовою е-документаційного забезпечення є е-документообіг. Порядок електронного документообігу визначено державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності згідно з законодавством. Таке визначення та тлумачення електронного документообігу визначено статтею 9 Закону України «Про електронні документи та електронний документообіг» від 22.05.2003 № 851-IV [50].

Електронний документообіг — це переведені в цифровий формат усі процеси по роботі з документами установи. Замість паперів формату А4 - файли та цифрові таблиці, замість підписів і чорнильних печаток - електронний підпис та інші інструменти верифікації [12]. У сучасній страховій компанії фахівці кожного структурного підрозділу мають справу із великою кількістю документів, певну частину з яких необхідно час від часу переглядати та коригувати, іншу частину - передавати посадовим особам, державним

службам, партнерам, контрагентам. За паервого документообігу, для цього документ необхідно було надрукувати, узгодити, можливо, внести правки, потім відправити на підпис відповідальній посадовій особі, поставити печатку та провести цю ж процедуру з іншою стороною. Електронний документообіг дозволив перенести весь цей бізнес-процес у цифровий вимір, відмовитися від паперу та заощадити величезну кількість часу та ресурсів [12].

На думку фахівців, електронний документообіг – «закономірний етап розвитку, частина цифрової трансформації світу в цілому. Колись усі документи писалися вручну майстрами каліграфії, це було не дуже швидко та зручно. Потім з'явилися друкарські машинки — писати стало набагато швидше та зручніше. Комп'ютери дали можливість змінювати документи та створювати необмежену кількість копій без особливих зусиль. Але в будь-якому випадку все зводилося до роботи з паперами: від печатки та підпису до відправки. Зараз, в еру діджиталізації, Інтернету, електронних підписів, електронних баз даних, програмні рішення повністю замінили паперові носії та створили системні процеси е-документообігу» [35].

За теорією сучасного документознавства [38, с.234], внутрішній е-документообіг страхової компанії «Ю.Ес.Ай.» - це все, що пов'язано з проведенням документів всередині Компанії. Об'єм е-внутрішнього документообігу складається з вхідних, вихідних та власне внутрішніх документів, що оброблені за період одного календарного року. Основними етапами е-внутрішнього документообігу Компанії є: робота із вхідною е-кореспонденцією; обробка та реєстрація е-документів; контроль над виконанням е-документів; обробка та відправлення вихідної е-кореспонденції. Загальна кількість документів кожного потоку за певний період часу (місяць, квартал, рік) становить обсяг е-документообігу.

Так, протягом 2023 року відповідальними посадовими особами Компанії було оброблено більше, ніж 61 тисячі вхідних документів; більше, ніж 40 тисяч вихідних документів; щорічний темп приросту оброблених документів сягає 30%. На нашу думку перевагами електронного документообігу є:

- однократна реєстрація документа;

- паралельне виконання різних операцій з метою скорочення часу руху документів і підвищення оперативності їхнього виконання;

- безперервність руху документа;

- єдина база документарної інформації для централізованого зберігання документів, що виключає дублювання документів;

- ефективно організована система пошуку документа [37].

У Компанії структурні підрозділи планомірно перейшли на електронні системи, впроваджено діджиталізацію сервісів, отримано широке поширення електронних поліс ОСЦПВ, у повну силу працює електронний європротокол. Кілька місяців тому розпочав функціонування електронний кабінет отримувача виплат. Основна мета запровадження електронних систем - покращення взаємодії страхувальників, страховиків та власне Компанії. Робота документообігу в електронному режимі дозволила скоротити час та зменшити затрачені ресурси для реалізації бізнес-процесів та завдань, поставлених перед Компанією [37]. Система електронного внутрішнього документообігу Компанії базується на програмному продукті компанії INBASE, яка давно займається інсталяцією та супроводом систем електронного документообігу.

Перехід на електронні документи уможливив Компанії вирішити такі завдання:

- оцифрування 100% вхідних документів;

- скорочення на 50% витрат часу на контроль обробки документів;

- скорочення на 50% витрат часу на пошук документів в системі;

- скорочення на 30% витрат часу на реєстрацію документів в системі;

- виключення ризику втрати документів;

- скорочення на 100% часу для логістики документів між підрозділами Компанії [37].

Перехід на електронну систему внутрішнього документообігу розпочався з автоматизації діловодства, архівування, управління нормативною

та розпорядчою документацією. Після переведення цих бізнес-процесів, діджиталізація торкнулася інших сторін діяльності Компанії. Спочатку було автоматизовано:

- обробку вхідної та вихідної документації;
- створення, узгодження та затвердження документів;
- накладення резолюцій;
- сканування та збереження електронних копій документів [37].

Активне сприяння запровадження діджитальних рішень у сфері ОСЦПВ - одне з важливих завдань, що ставило перед собою керівництво Компанії. Окрім того, на сьогодні у сфері страхових послуг Компанія – сучасна технологічна установа, що використовує можливості та переваги, що дають ІТ-технологій. Електронний обіг документообіг дозволив швидше обслуговувати отримувачів регламентних виплат, налагодив максимально оперативну та ефективну взаємодію з страховиками, у тому числі із застосування електронного підпису. Протягом 2019 року у Компанії було оброблено: більше, ніж 61 тисячі вхідних документів; більше, ніж 40 тисяч вихідних документів; щорічний темп приросту оброблених документів сягає 30% [37].

Зокрема, найбільш затребуваними сервісами електронного документообігу у царині страхових компаній в Україні такі:

- Сервіс «Paperless». «Paperless» - сервіс для компаній та підприємців з обміну документами між собою в електронній формі. Це безкоштовний сервіс, який працює коректно з електронним підписом усіх основних АЦСК України, включаючи ключі, видані Державною фіскальною службою України, Міністерством юстиції тощо. Для користування ним не потрібно встановлювати додаткове програмне забезпечення. Щоб коректно використовувати його, необхідно лише встановити додаток для браузера та зареєструватися [37].

Усі документи зберігаються в трьох екземплярах на незалежних серверах, що фактично є стовідсотковою гарантією того, що з цими

документами нічого не трапиться. Окрім цього, для додаткового страхування є можливість завантажувати документи на комп'ютер. Також заплановано найближчим часом додати функцію синхронізації документів із сервісами Dropbox та GoogleDrive [37].

- Сервіс «Document.Online». На відміну від попереднього, сервіс «Document.Online» є умовно безкоштовним. Це означає, що є тариф, який дозволяє користуватися сервісом безкоштовно, але він має обмеження щодо кількості документів, якими можна користуватися протягом місяця. Цей сервіс дозволяє завантажувати документи, створювати шаблони для подальшого використання, обмінюватись документами або направляти їх декільком отримувачам. «Document.Online» підтримує роботу з усіма акредитованими центрами сертифікації ключів України. «Document.Online» можна встановити на будь-який стаціонарний чи мобільний пристрій, що має доступ до Інтернету, незалежно від операційної системи, встановленої на нього [37].

Документи зберігаються на серверах Microsoft Azure. Доступ до документів гарантується на рівні 99.98%. Це означає, що тільки 5 хвилин на місяць існує перерва у доступі до даних. Між серверами Microsoft Azure автоматично підтримується зв'язок. Завдяки багаторазовому копіюванню даних імовірність втрати їх у разі виходу з ладу одного з серверів незначна. Навіть у разі фізичного руйнування носія дані буде відновлено протягом години [37].

- «ІІТ Користувач ЦСК-1». Частковий функціонал для здійснення електронного документообігу надає програма «ІІТ Користувач ЦСК-1», розроблена на замовлення Державної фіскальної служби України. Цей сервіс відрізняється більш інтуїтивно зрозумілим інтерфейсом та спеціалізацією саме на роботі з електронним підписом. Програма надає такий функціонал:

- накладення кваліфікованого електронного підпису чи печатки на будь-яку інформацію в електронному вигляді (текстові, відео-, аудіо- файли, файли баз даних тощо), а також для криптографічного захисту інформації шляхом її направленого шифрування;

- генерацію ключів заявників кваліфікованого надавача ЕДП ІДД ДПС, резервне копіювання особистого ключа з одного носія ключової інформації на інший, знищення особистого ключа [49];

- перевірку сертифіката користувача;

- формування та передачу до кваліфікованого надавача ЕДП ІДД ДПС запиту на блокування / скасування сертифіката користувача;

- доступ до сертифікатів кваліфікованого надавача ЕДП ІДД ДПС, серверів кваліфікованого надавача ЕДП ІДД ДПС, сертифікатів інших користувачів та списку відкликаних сертифікатів з метою перегляду, пошуку сертифікатів користувачів у файловому сховищі, визначення статусу сертифікатів користувачів, перевірку цілісності сертифікатів [49].

Зараз у Компанії при е-документообігу існує програма для внутрішніх документів та окрема для зовнішніх. Ведення Загальним відділом Компанії реєстру всіх е-документів з їхнім описом уможливив повернути або відновити документи у випадку втрати чи вилучення. Е-внутрішні документи щоквартально аналізуються, дані про них доповідаються уповноваженою посадовою особою Загального відділу керівництву для прийняття управлінських рішень щодо вдосконалення роботи з е-внутрішніми документами. Підрахунок документів із метою визначення обсягу е-внутрішнього документообігу у Компанії фіксується по кожному з документопотоків загалом (вхідний, вихідний, внутрішній) в обліковій таблиці в розрізі видів е-документів та груп, а також структурних підрозділів Компанії [37].

Кількість е-внутрішніх документів обчислюється у вигляді дробу, чисельник якого означає кількість е-документів, а знаменник - кількість електронних примірників (е-копій) документа. Усі операції, здійснювані фахівцями Компанії у процесі е-внутрішнього документообігу, є складовою спеціальної управлінської функції, е-діловодства, або е-документаційного забезпеченням. Ці операції об’єднують численні дії, пов’язані зі створенням та оформленням е-внутрішніх документів Компанії, їхнім обліком, реєстрацією,

контролем за виконанням, формуванням у справи, підготовкою до архівного зберігання тощо.

Для оптимальної організації е-внутрішнього документообігу Компанії на сервері створено базу даних, в якій зберігаються всі створені е-документи. Доступ до бази даних здійснюється через браузер, підтримка якого відбувається через інтерфейс Компанії. (як правило, підтримку браузера визначає розробник створеного інтерфейсу) [37]. Е-внутрішні документи зберігаються або завантажуються в певні виділені каталоги Компанії. Каталоги розподілені відповідно до ієрархічної структури підрозділів. .

За внутрішньою посадовою інструкцією, що створена на основі Типової інструкції з діловодства створювати, модифікувати, видаляти е-внутрішні документи має право особа, наділена відповідними правами. Е-внутрішні документи Компанії конкретизують статут, регулюють сфери її діяльності, які ще вимагають обов'язкового письмового закріплення, формалізують взаємовідносини між штатними працівниками, дають керівництву Компанії можливість встановити систему штрафів та заохочень [37].

Саме за допомогою е-внутрішніх документів можна у формі, що максимально відповідає баченню керівництва та інтересам Компанії, встановлено межу відповідальності кожного співробітника. Наявність деяких із нижченаведених документів прямо передбачена чинним законодавством України, наявність інших витікає з типового документообігу, притаманного якісному та безпечному веденню бізнесу в Україні. Найбільш поширеними внутрішніми документами Компанії є:

- правила внутрішнього розпорядку;
- посадові інструкції;
- положення (про оплату праці, про відпустки, про дивіденди, про бухгалтерію та ін.) ;
- інструкція про печатки та штампи;
- колективний договір;
- пакети документів у сфері інформаційної безпеки підприємства;

- пакети документів у сфері охорони праці, пожежної безпеки [37].

Так, колективний договір - угода, яка укладається між власником Компанії на представництво трудовим колективом органами. Колективний договір є результатом соціального партнерства та діалогу на локальному рівні. Колективний договір укладається відповідно до чинного законодавства (ст. 10-20 Закону України «Про колективні договори і угоди») [56] узятих сторонами зобов'язань і має на меті регулювання виробничих, трудових і соціально-економічних відносин, а також узгодження інтересів власників. Маємо наголосити, що колективний договір укладається на підприємствах, в установах, організаціях незалежно від форм власності і господарювання, які використовують найману працю і мають права юридичної особи, а також у структурних підрозділах підприємства, установи, організації в межах компетенції цих підрозділів.

У нашому випадку, зміст колективного договору Компанії визначають сторони. У ньому передбачені взаємні зобов'язання сторін щодо регулювання виробничих, трудових, соціально-економічних відносин, зокрема:

- зміни в умовах праці;
- забезпечення продуктивної зайнятості;
- нормування оплати праці;
- встановлення форм, системи, розмірів заробітної плати та інших видів трудових виплат (премій, доплат, надбавок та інші);
- встановлення гарантій, компенсацій, пільг [56];
- участь трудового колективу у формуванні, розподілі і використанні прибутку Компанії;
- встановлення режиму роботи, тривалості робочого часу і відпочинку;
- умов з охорони праці;
- забезпечення житлово-побутового, культурного, медичного обслуговування, організації оздоровлення і відпочинку працівників Компанії;
- умов регулювання фондів оплати праці та встановлення міжкваліфікаційних (міжпосадових) співвідношень в оплаті праці;

- забезпечення рівних прав та можливостей жінок і чоловіків [56];
- заборона дискримінації.

У колективному договорі Компанії передбачено додаткові порівняно з чинним законодавством і угодами гарантії, соціально-побутові пільги. Колективний договір підлягає реєстрації місцевими органами державної виконавчої влади, порядок якої визначається Кабінетом Міністрів України [37]. Колективний договір набрав чинності від дня підписання сторонами або від дня, зазначеного в ньому, і діє до часу укладання нового або перегляду чинного, якщо інше не передбачено договором. Наприклад, за умови, що установа є новоствореною, організація колективного договору укладається у тримісячний строк після реєстрації або після рішення про заснування, якщо реєстрація не передбачена.

Колективний договір поширюється на всіх працівників незалежно від того, чи є вони членами профспілки, і обов'язковий як для власника або уповноваженого ним органу, так і для працівників. Щорічно в строки, передбачені колективним договором, сторони, що його підписали, звітують про його виконання [37]. Контроль за виконанням колективного договору здійснюється безпосередньо сторонами, які його уклали, або уповноваженими ними. Маємо наголосити, що як такої, юридичної відповідальності за неукладення колективного договору не встановлено, однак передбачено адміністративну відповідальність за ухилення від участі у колективних переговорах та за невиконання колективного договору, який вже укладено. Проте відсутність колективного договору на підприємстві, яке використовує найману працю, у деяких випадках може бути кваліфіковане як порушення законодавства про працю.

Отже, внутрішня система е-документаційного забезпечення Компанії відповідає сучасним вимогам і значно спростила роботу з документами, що створюються між структурними підрозділами.

2.3. Зовнішня система електронного документаційного забезпечення структурних підрозділів Товариства з додатковою відповідальністю страхова компанія «Ю.Ес.Ай»

Зовнішня система е-докуменатційного забезпечення Компанії призначена для роботи із установами, підприємствами, профільними відомствами, клієнтами та страховиками. У теорії сучасного документознавства, зовнішніми документи розуміються як ті, що надходять від інших підприємств, організацій, тобто, складаються за межами даного підприємства [11, с.125]. До них належать виписки банку, рахунки постачальників та ін. Так, обов'язковим для Компанії є розміщення на сайті зовнішніх документів, що підтверджують право надати послуги, наприклад, ліцензії, вказують на платоспроможність, зокрема, фінансові звіти, нормативні документи, що регулюють діяльність «Ю.Ес.Ай.» [37].

Так, страхова ліцензія як зовнішній документ – це ліцензія на провадження страхової діяльності — документ, що «засвідчує право її власника на проведення страхової діяльності на території України при дотриманні ним умов та вимог, обумовлених при видачі ліцензії» [35]. В Україні ліцензія на проведення страхової діяльності не має обмежень по терміну дії. Ліцензії видаються на проведення добровільного та обов'язкового особистого, майнового страхування, а також страхування відповідальності і перестрахування. Кабінет Міністрів України встановлює розмір плати за видачу ліцензій на проведення конкретних видів страхування.

Для ліцензування страхової діяльності необхідні такі документи: заяву на отримання ліцензії; копії установчих документів та копія свідоцтва про реєстрацію; довідки банків або висновки аудиторських фірм (аудиторів), що підтверджують розмір сплаченого статутного фонду; довідка про фінансовий стан засновників страховика, підтверджена аудитором(аудиторською фірмою), якщо страховик створений у формі повного чи командитного товариства або товариства з додатковою відповідальністю; правила (умови)

страхування; економічне обґрунтування запланованої страхової (перестрахувальної) діяльності; інформація про учасників страховика, голову виконавчого органу та його заступників, копія диплома голови виконавчого органу страховика або його першого заступника про вищу економічну або юридичну освіту, копія диплома головного бухгалтера страховика про вищу економічну освіту, інформація про наявність відповідних сертифікатів у випадках, передбачених Уповноваженим органом [26, с.178].

Уповноважений орган зобов'язаний розглянути заяву страховика про видачу йому ліцензії у строк, що не перевищує 30 календарних днів з часу одержання всіх необхідних документів [63].

У свою чергу, фінансовий звіт як зведений обліковий документ повинен мати такі обов’язкові реквізити: назву документа (форми); дату складання; назву підприємства, від імені якого складено документ; зміст та обсяг господарської операції, одиницю виміру господарської операції; посади осіб, відповідальних за здійснення господарської операції і правильність її оформлення; особистий підпис або інші дані, що дають змогу ідентифікувати особу, яка брала участь у здійсненні господарської операції. Первинні документи, складені відповідними структурними підрозділами Компанії в електронній формі, застосовуються у бухгалтерському обліку за умови дотримання вимог законодавства про електронні документи та електронний документообіг. Інформація, що міститься у прийнятих до обліку первинних документах, систематизується на рахунках бухгалтерського обліку в регістрах синтетичного та аналітичного обліку шляхом подвійного запису їх на взаємопов’язаних рахунках бухгалтерського обліку. Операції в іноземній валюті відображаються також у валюті розрахунків та платежів по кожній іноземній валюті окремо [63].

Дані аналітичних рахунків повинні бути тотожні відповідним рахункам синтетичного обліку на кінець останнього дня кожного місяця. Господарські операції повинні бути відображені в облікових регістрах у тому звітному періоді, в якому вони були здійснені. У разі складання та зберігання первинних

документів і регістрів бухгалтерського обліку з використанням електронних засобів оброблення інформації підприємство зобов'язане за свій рахунок виготовити їх копії на паперових носіях на вимогу інших учасників господарських операцій, а також правоохоронних органів та відповідних органів у межах їх повноважень, передбачених законами. Відповідальність за несвоєчасне складання первинних документів і регістрів бухгалтерського обліку та недостовірність відображених у них даних несуть особи, які склали та підписали ці документи [40, с.178].

Фінансова звітність підписується директором Компанії та бухгалтером. Склад та форми фінансової звітності установлені центральним органом виконавчої влади, що забезпечує формування та реалізує державну політику у сфері бухгалтерського обліку, за погодженням із центральним органом виконавчої влади, що реалізує державну політику у сфері статистики. Фінансова звітність за міжнародними стандартами складається у Компанії на підставі таксономії фінансової звітності за міжнародними стандартами. Для складання фінансової звітності застосовуються міжнародні стандарти, які викладені державною мовою та офіційно оприлюднені на вебсторінці центрального органу виконавчої влади, що забезпечує формування та реалізує державну політику у сфері бухгалтерського обліку. Фінансовий звіт Компанії складається на кінець останнього дня звітного періоду. Річний фінансовий звіт складається станом на кінець дня 31 грудня. Місячні (на останню дату місяця) і квартальні форми (станом на 31 березня, 30 червня, 30 вересня та 31 грудня) [40, с.179].

Окрім вищеперерахованих зовнішніми страховими документами також є:

- страховий поліс - документ, що видається страховиком, який підтверджує договір страхування та містить умови укладеного договору, в якому страховик зобов'язується за конкретну плату відшкодувати страхувальнику збитки, пов'язані з ризиками та нещасними випадками, зазначеними у договорі. Страховий поліс видається страховим товариством

страхувальнику після сплати ним страхової премії. Існують страхові поліси різних видів та різних назв залежно від порядку оформлення страхування та характеру ризику [74, с.178].

За рейсовим полісом об'єкт страхування страхується на певний період. За змішаним полісом об'єкт страхується як на певний рейс, так і на певний строк. Рейсовий страховий поліс оформляється на бланках страхового товариства та підписується страховиком і страхувальником або його експедитором у порту відвантаження товарів. Рейсовий страховий поліс містить такі основні дані: назву страхувальника, умови страхування , розмір страхової суми (тобто розмір відшкодування, що сплачує страховик у випадку загибелі або пошкодження застрахованого товару), розмір страхової премії, яка вноситься страхувальником як оплата за страхування [74, с.179];

- генеральний поліс - це договір тривалого характеру між страхувальником та страховиком. У ньому зазначається строк його дії, обсяг та границі відповідальності страховика, строки платежу страхової премії та інші спеціальні умови і застереження;

- страховий сертифікат - документ, котрий видається страховим товариством страхувальнику, який засвідчує, що страхування було здійснено і що був виданий поліс. Такий сертифікат на конкретний вантаж використовується в основному у тому випадку, якщо товари застраховані відповідно до умов генерального або невалютного полісу. На вимогу страхувальника він може обмінюватися па страховий поліс, оскільки у багатьох країнах законодавство визнає як судовий доказ тільки страховий поліс [74, с.180];

- страхове оголошення (декларація) - документ, який використовується, якщо страхувальник повідомляє своєму страховику докладні відомості про окремі відправлення, на які поширюється договір страхування або генеральний поліс, укладений між сторонами.

Також, суто специфічними документами, наявними у страховій діяльності, також, є:

- рахунок страховика - документ, що видається страховиком із зазначенням суми виконаного страхування з вимогою оплати цієї суми;

- коверкот - документ, який видається страховиком (страховим маклером, агентом тощо) для повідомлення страхувальника про те, що його інструкції щодо страхування виконані, або в засвідчення здійсненого агентом страхування на користь страхувальника;

- абандон - відмова вантажо- або судновласника від своїх прав на застраховане майно на користь страховика при зобов'язанні останнього сплатити страхувальнику повну страхову суму [74, с.181];

- договір страхування - угода між страхувальником та страховиком, що регулює їх взаємні зобов'язання відповідно до умов даного виду страхування, або угода, за якою одна сторона (страховик) бере на себе зобов'язання за обумовлену винагороду (страхова премія) відшкодувати збитки іншій стороні (страхувальнику), які виникли внаслідок передбачених у страховому договорі випадковостей (страхового випадку);

- поліс валютований - поліс по морському страхуванню, в якому зазначена страхова сума;

- претензія - вимога, що пред'являється страхувальником страховику у зв’язку з настанням страхового випадку, який мав місце внаслідок випадковостей, закладених в умовах страхування [74, с.181].

У свою чергу, франшиза - умови страхового договору, які передбачають звільнення страховика від відшкодування збитків, що не перевищують певного резерву. Страховий платіж (страховий внесок, страхова премія) - плата за страхування, яку страхувальник зобов’язаний внести страховику згідно з договором страхування. Страховий тариф - ставка страхового внеску з одиниці страхової суми за визначений період страхування. Страхові тарифи при добровільній формі страхування обчислюються страховиком актуарно (математично) на підставі відповідної статистики настання страхових випадків, а за договорами страхування життя - також з урахуванням величини інвестиційного доходу, яка повинна зазначатися у договорі страхування.

Конкретний розмір страхового тарифу визначається в договорі страхування за згодою сторін [74, с.182].

Актуарними розрахунками можуть займатися особи, які мають відповідну кваліфікацію згідно з вимогами, встановленими Уповноваженим органом, яка підтверджується відповідним свідоцтвом. Правила страхування розробляються страховиком для кожного виду страхування окремо і підлягають реєстрації в Уповноваженому органі при видачі ліцензії на право здійснення відповідного виду страхування.

Правила страхування повинні містити: предмет договору страхування; порядок визначення розмірів страхових сум та (або) розмірів страхових виплат; страхові ризики; виключення із страхових випадків і обмеження страхування; строк та місце дії договору страхування; порядок укладення договору страхування; права та обов'язки сторін; дії страхувальника у разі настання страхового випадку [74, с.183]; перелік документів, що підтверджують настання страхового випадку та розмір збитків; порядок і умови здійснення страхових виплат; строк прийняття рішення про здійснення або відмову в здійсненні страхових виплат; причини відмови у страховій виплаті або виплаті страхового відшкодування; умови припинення договору страхування; порядок вирішення спорів; страхові тарифи за договорами страхування іншими, ніж договори страхування життя; страхові тарифи та методику їх розрахунку за договорами страхування життя; особливі умови.

У разі, якщо страховик запроваджує нові правила страхування чи коли до правил страхування вносяться зміни та (або) доповнення, страховик повинен подати ці нові правила, зміни та (або) доповнення для реєстрації до Уповноваженого органу. Уповноважений орган має право відмовити у видачі ліцензії та реєстрації правил чи змін та (або) доповнень до них, якщо подані правила страхування або зміни чи доповнення до них суперечать чинному законодавству, порушують чи обмежують права страхувальника або не відповідають вимогам чинного законодавства [74, с.183]. Для укладання договору страхування страхувальник подає страховику письмову заяву за

формою, встановленою страховиком, або іншим чином заявляє про свій намір укласти договір страхування. При укладанні договору страхування страховик має право запросити у страхувальника баланс або довідку про фінансовий стан, підтверджені аудитором (аудиторською фірмою), та інші документи, необхідні для оцінки страховиком страхового ризику.

Договори обов'язкового страхування цивільно-правової відповідальності власників наземних транспортних засобів, що підлягають обов'язковому технічному контролю відповідно до Закону України «Про дорожній рух» [47], укладаються страховиками за умови проходження транспортними засобами обов'язкового технічного контролю, якщо вони згідно з протоколом перевірки технічного стану визнані технічно справними. Договори обов'язкового страхування цивільно-правової відповідальності власників наземних транспортних засобів укладаються на строк, що не перевищує строку чергового проходження транспортним засобом обов'язкового технічного контролю відповідно до вимог Закону України «Про дорожній рух» [47]. Факт укладання договору страхування може посвідчуватися страховим свідоцтвом (полісом, сертифікатом), що є формою договору страхування. Договір страхування набирає чинності з моменту внесення першого страхового платежу, якщо інше не передбачено договором страхування.

Договір страхування життя може бути укладений як шляхом складання одного документа (договору страхування), підписаного сторонами, так і шляхом обміну листами, документами, підписаними стороною, яка їх надсилає. У разі надання страхувальником письмової заяви за формою, встановленою страховиком, що виражає намір укласти договір страхування, такий договір може бути укладений шляхом надіслання страхувальнику копії правил страхування та видачі страхувальнику страхового свідоцтва (поліса), який не містить розбіжностей з поданою заявою. Заява складається у двох примірниках, копія заяви надсилається страхувальнику з відміткою

страховика або його уповноваженого представника про прийняття запропонованих умов страхування [63].

Отже, система е-зовнішнього документаційного забезпечення компанії «Ю.Ес.Ай.» відповідає профілю діяльності і укладена відповідно до чинного нормативного законодавства. У цілому, складовими системи електронного надання документаційного забезпечення Товариства з додатковою відповідальність страхова компанія «Ю.Ес.Ай.» є зовнішній та внутрішній е-документообіги, робота з фаховими е-страховими документами.

РОЗДІЛ ІІІ. ШЛЯХИ УДОСКОНАЛЕННЯ МЕХАНІЗМІВ НАДАННЯ ДОКУМЕНТАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СУЧАСНОЇ УСТАНОВИ (НА ПРИКЛАДІ ТОВАРИСТВА З ДОДАТКОВОЮ ВІДПОВІДАЛЬНІСТЮ СТРАХОВА КОМПАНІЯ «Ю.Ес.Ай.»)

3.1. Посилення безпеки контролю з витоком інформації із електронної системи звіту та аналітичної обробки даних Товариства з додатковою відповідальністю страхова компанія «Ю.Ес.Ай.»

У роботі страхових компаній важливою складовою є робота ІТ-відділів, скерована на посилення захисту інформаційних продуктів та послуг від стороннього втручання. Фахівці ІТ-відділу страхової компанія «Ю.Ес.Ай.» постійно працюють над удосконаленням вже існуючих антивірусних програм та створенням нових. Саме сучасні антивірусні спеціалізовані програми убезпечують комп'ютери співробітників різних структурних підрозділів Компанії від небажаних чи шкідливих програм загалом, можуть відновлювати заражені чи модифіковані такими програмами файли, власне, є профілактичним засобом, що запобігає зараженню (модифікації) файлів чи операційної системи Компанії шкідливим кодом [37]. Основні завдання з посилення безпеки контролю з витоком інформації систем звіту та аналітичної обробки даних Компанії ми вбачаємо у тому, щоб:

- удосконалювати сканування файлів і програм у режимі реального часу;
- сканування комп'ютера за потребою;
- сканування Інтернет-трафіку;
- сканування електронної пошти;
- захист від атак ворожих веб-сайтів;
- відновлення пошкоджених файлів [75, с.347].

Надважливим у діяльності, наприклад, страхових агентів у системі захисту інформації є слідкування за трафіком, потоком навантаження на

комунікаційну систему Компанії, а саме: звернення, кількість переданих за одиницю часу пакетів або повідомлень у різних системах, мережах, включаючи телекомунікаційні та транспортні мережі, обсяг переданих або прийнятих даних. Відповідно до напрямку транспортування розрізняють: вхідний трафік - визначається обсягом вхідного потоку; вихідний трафік - визначається обсягом вихідного потоку.

У свою чергу, постійний моніторинг над безпекою електронної пошти дозволяє прискорювати зчитування даних, внутрішніх і зовнішніх е-документів тощо. Протокол SMTP має обмежений механізм для відстеження прочитання переданого повідомлення, а також не має функціоналу для перевірки того, чи лист було переглянуто отримувачем [35]. Якщо поштовий сервер повідомляє про помилку доставки, це сигналізує про те, що повідомлення не було доставлене адресату. Щоб виправити це, фахівці ІТ-відділу Компанії розробили систему сповіщень про стан доставки та помилки, проте ця система не є універсальною.

За зауваженням дослідників, ряд провайдерів електронної пошти навмисно не надають звіти про ненадання (NDR) та звіти про доставку повідомлень для боротьби зі спамерами з огляду на те, що:

- звіти про доставку можна використовувати для перевірки існування адреси, і якщо адреса існує, спамер отримує звіт про це [33];

- якщо спамер використовує електронну адресу підробленого відправника (підробка електронної пошти), то на справжню адресу електронної пошти, яку було використано, можуть бути надіслані десятки тисяч звітів про недійсні адреси електронної пошти, які спамер, можливо, намагався надіслати електронною поштою [33].

Для отримання звіту про прочитання співробітників інших підрозділів Компанії (офіс-менеджери, бухгалтерія, відділ кадрів страхові агенти) використовують слідкування за переходами через унікальні посилання або додавання відповідних зображень для тіла листа. Так, маючи внутрішню унікальну адресу для посиланням або віддаленого зображення, поштовий

сервіс відслідковує за тим, чи відкрив отримувач посилання або чи було завантажено зображення, і тим самим отримати звіт про прочитання повідомлення. Перешкодити цьому може відключене завантаження віддалених зображень. Ця функція працює за замовчуванням, наприклад, у службі Gmail [72].

У свою чергу, досить небезпечним на сьогодні є і фішинг - шахрайство для виманювання у користувачів персональних даних. Шахраї змушують користувачів розкривати конфіденційні дані. Один із методів - надсилання електронних листів із пропозиціями підтвердити реєстрацію облікового запису з посиланнями на сайт, зовнішній вигляд якого повністю копіює дизайн ресурсу Компанії. Шахраї використовують електронну пошту Компанії, намагаючися вкрасти паролі, номери банківських рахунків або інші приватні дані. За даними інтернет-центру розгляду скарг ФБР, у США 2019 року об'єм втрат від фішингу склав 57 млн $ [33].

Іншою вагомою складовою удосконалення безпеки розсилки повідомлень є спам - масове розсилання кореспонденції рекламного чи іншого характеру страховим агентам, які не висловили бажання її одержувати. Передусім термін «спам» стосується рекламних електронних листів. За спостереженнями дослідників, 2020 року щодня в Інтернеті надсилалось 14,5 млрд спам-листів, що становить 45 % всіх відправлених електронних листів. Незважаючи на розробку спам-фільтрів для боротьби за спамом, ця проблема досі не є вирішеною [33].

Актуальною складовою захисту системи звітів та аналітичної обробки даних є використання антивірусних продуктів. Фахівці класифікують антивірусні продукти відразу за кількома ознаками, таким, як:

- використовувані технології антивірусного захисту;
- функціонал продуктів;
- цільові платформи.

Із використовуваних технологій ІТ-співробітників Компанії антивірусного захисту є:

- класичні антивірусні продукти (продукти, які застосовують тільки сигнатурний метод детектування) [35];

- продукти проактивного антивірусного захисту, що застосовують лише проактивні технології антивірусного захисту;

- комбіновані продукти, що застосовують як класичні, сигнатурні методи захисту, так і проактивні [35].

За функціоналом продуктів є:

- антивірусні продукти, що забезпечують тільки антивірусний захист;

- комбіновані продукти, що забезпечують не лише захист від шкідливих програм, але і фільтрацію спаму, шифрування та резервне копіювання даних та інші функції).

За цільовими платформами: Windows, NIX (до даного сімейства наледать ОС BSD, Linux, etc), MacOS, для мобільних платформ (Windows, Symbian, iOS, BlackBerry, Android, WindowsPhone та інші). Антивірусні продукти класифікуються за об'єктами захисту: для захисту робочих станцій, для захисту файлових і термінальних серверів, для захисту поштових та Інтернет-шлюзів, для захисту серверів віртуалізації [22].

У цілому, антивірусне програмне забезпечення Компанії складається з комп'ютерних програм, які намагаються знайти, запобігти розмноженню і видалити комп'ютерні віруси та інші шкідливі програми. Антивірусне програмне забезпечення Компаній містить два різних методи для виконання своїх задач:

- перегляд (сканування) файлів для пошуку відомих вірусів, що відповідають визначенню в словнику вірусів;

- знаходження підозрілої поведінки будь-якої із програм, що схожа на поведінку зараженої програми [36, с.145].

Класифікувати антивірусних продуктів фахівцями IT-відділу здійснюється одразу за кількома ознаками: використовувані технології антивірусного захисту, функціонал продуктів, цільові платформи. У такому випадку антивірусна програма під час перегляду файлу звертається до

словника з відомими вірусами, що складений авторами програми-антивірусу Компанії. У разі відповідності якоїсь ділянки коду програми, що проглядається, відомому коду) вірусу в словнику, програма-антивірус може виконувати одну з наступних дій [37]:

- видалити інфікований файл;

- відправити файл у карантин (тобто зробити його недоступним для виконання, з метою недопущення подальшого розповсюдження вірусу);

- намагатися відтворити файл, видаливши сам вірус із тіла файлу.

Фахівці підкреслюють, що «хоча антивірусні програми створені на основі пошуку відповідності визначенню вірусу в словнику, за звичайних обставин, вони можуть досить ефективно перешкоджати збільшенню випадків зараження комп'ютерів, автори вірусів намагаються триматися на півкроку попереду таких програм-антивірусів, створюючи «олігоморфні», «поліморфні» і, найновіші, «метаморфічні» віруси, у яких деякі частини шифруються або спотворюються так, щоб неможливо було знайти спільне з визначенням в словнику вірусів» [30, с.56].

Антивіруси, що використовують метод знаходження підозрілої поведінки програм, не намагаються ідентифікувати відомі віруси, замість цього вони стежать за поведінкою всіх програм. Якщо програма намагається записати якісь дані в файл, що виконується (exe-файл), програма-антивірус може зробити помітку цього файлу, попередити користувача і спитати, що треба зробити. На відміну від методу відповідності визначенню вірусів в словнику, метод знаходження підозрілої поведінки дає захист від абсолютно нових вірусів, яких ще немає в жодному словнику вірусів. Однак треба враховувати, що програми, побудовані на цьому методі, видають також велику кількість помилкових попереджень. Програми класу Firewall давно мали в своєму складі модуль знаходження підозрілої поведінки програм [31, с.89].

Ряд програм-антивірусів намагаються імітувати початок виконання коду кожної нової програми, що викликається для виконання, перед тим, як передати їй керування. Якщо програма використовує код, що змінюється

самостійно, або проявляє себе як вірус (тобто починає шукати інші exe-файли, наприклад), тоді програма буде вважатися шкідливою (здатною нашкодити іншим файлам). Однак цей метод також має велику кількість помилкових попереджень [31, с.71].

Основні можливості ряду програм такі: захист від вірусів, черв'яків, троянів та інших шкідливих програм; захист від шпигунських та рекламних програм; захист від несанкціонованого доступу до приватної інформації; функція стеження в режимі реального часу («Вартовий»); вбудований алгоритм евристичного аналізу; перевірка файлів, що завантажуються на комп'ютер із мережі Інтернет; поштовий фільтр; перевірка офісних документів.

Для оптимізації роботи з вірусами, що можуть перешкоджати роботі із аналітичними даними та звітами у Компанії використовується антивірусна програма Zillya! Оновлення антивірусних баз на комп'ютерах Компанії відбувається централізовано та не потребує підключення окремих ПК до мережі Інтернет. Відповідальний адміністратор мережі має змогу відслідковувати стан захисту системи в режимі он-лайн. Усі події, пов'язані із виявленням вірусних загроз на ПК, що знаходяться у мережі, фіксуються антивірусом та відображаються в адміністративній панелі у вигляді повідомлень.

За допомогою Коду активації з 32-х символів, через мережу Інтернет здійснюється централізоване оновлення антивірусних баз на комп'ютерах Компанії [69]. Антивірус виявляє та знешкоджує шкідливе програмне забезпечення на комп'ютері співробітників Компанії. Об'єкти, що перевіряються такі: файли на жорсткому диску, USB-накопичувачах, оперативній пам'яті, електронна пошта.

У стані «захист у нормі» антивірус має унікальний вигляд - лише одна кнопка, що сповіщає співробітника Компанії, що система в нормі. Співробітник повинен застосовувати будь-які дії лише у випадку, якщо

антивірус не має змоги діяти без втручання ІТ-спеціаліста. Антивірус захищає ПК співробітників Компанії від вірусів за допомогою:

- щоденних оновлень антивірусних баз в автоматичному режимі;

- вбудованого модуля евристичного аналізу, який дозволяє виявляти та нейтралізувати шкідливі програми на основі аналізу їх коду [69];

- повна база загроз, яким протидіє антивірус, складає більше 5 млн. вірусів.

Цікавим є і «Вартовий» - це система перевірки файлів у реальному часі, що виявляє віруси та інші шкідливі програми, які намагаються проникнути на комп'ютери співробітників Компанії. «Вартовий» відстежує запущені процеси, файли, що створюються і відкриваються, ефективно блокує і видаляє загрози «на випередження». Поштовий фільтр перевіряє всі вхідні і вихідні поштові повідомлення на наявність шкідливих об'єктів, не допускаючи можливості для проникнення в систему загроз разом з електронним листом [69].

Різноманітні архіви. включаючи поштові бази, ISO-образи, скануються, але вибір дій обмежується командою «Ігнорувати». Такі файли не поміщаються ні в активні загрози, ні в карантин, і тим більше не видаляються. Співробітник Компанії лише отримує повідомлення про те, що в архіві знайдено вірус. Фахівці наголошують, що «файли у архівах не становлять загрози для користувача до тих пір, поки вони не будуть витягнуті користувачем з архіву, але в цей момент вони будуть виявлені і нейтралізовані «Вартовим» [69].

Zillya! Антивірус містить функцію «Планувальник» - сканування персонального комп'ютера, яку можна налаштувати так, як буде найбільш зручно. Співробітник Компанії може налаштувати автоматичне сканування одноразово, щодня, погодинно, щотижня або щомісяця. Основа захисту даних від усіх типів шкідливих програм базується на використанні актуальної вірусної бази, яка вміщує 15 млн вірусних сигнатур та сучасного модулю проактивного захисту. Комплексність Інтернет захисту реалізується за

допомогою потужного брандмауера та WEB-фільтра, здатних на сучасному рівні перевіряти дані, які потрапляють на ПК співробітника Компанії , блокувати сайти, на яких виявлені загрози [69].

У такому випадку, утиліти не будуть перевантажувати комп'ютер, оскільки антивірус споживатиме не більше 150 Мб оперативної пам'яті ПК. Програма містить вбудовану базу даних, що містить усі необхідні правила дозволу або блокування (за бажанням співробітника Компанії) стандартних системних сервісів або протоколів (NetBIOS, DHCP, DNS та інших) для роботи з мережею. За їхньою допомогою співробітник Компанії може дозволяти або забороняти мережеву активність за такими протоколами та не розбиратися у тонкощах їхньої роботи. У Zillya! Internet Security є можливість встановлювати загальні налаштування для всіх додатків. Для цього достатньо було IT-співробітникам Компанії в налаштуваннях прописати правило, яке дозволяє доступ до певної IP-адреси через певний порт [69].

Деякі сайти додаються до бази Zillya! Internet Security як підозрілі, або як сайти, що мають шкідливий контент. Якщо сайт знаходиться в такому списку, співробітник Компанії має змогу його відвідувати, переглядати сторінки, зображення, але не має змогу завантажити з цього ресурсу програми, архіви, документи та інші файли, які потенційно можуть нести загрозу вашому комп'ютеру. У WEB-фільтрі окрім вбудованої бази сайтів, що блокуються, створено власний список таких сайтів, які співробітник Компанії за певних причин вважає шкідливими.

Також, для співробітників Компанії створено спеціальну програму, яка дозволяє максимально надійно видаляти непотрібні конфіденційні файли, без можливості їх відновлення [69]. Принцип роботи програм-шредерів полягає в тому, що файл, який планується видалити, піддається багатопрохідному затиранню. Видалити файли можна або безпосередньо з меню антивірусу (вкладка Інструменти) або ж за допомогою контекстного меню, клікнувши правою кнопкою миші на будь-якому файлі та обрати в спливаючому меню пункт «Wipe files by Zillya! Internet Security». Інтерфейс виконаний в

плитковому дизайні забезпечує доступ до основних модулів та функцій антивірусу в один клік. Основа захисту даних від усіх типів шкідливих програм базується на використанні актуальної вірусної бази, яка вміщує 15 млн вірусних сигнатур та сучасного модулю проактивного захисту. Оновлення сигнатурних баз відбувається щоденно.

Утиліти не будуть перевантажувати комп'ютер, оскільки антивірус споживатиме не більше 512 Мб оперативної пам'яті ПК. Основні модулі та функції захисту:

- поведінковий аналізатор HIPS - сканування і аналіз програм, на предмет їх можливої шкідливої поведінки. Функція самозахисту - можливість відключення захисту ПК співробітника Компанії внаслідок примусової зупинки за допомогою «Диспетчера завдань» [69].

- використання технології евристичного аналізу. Евристичний аналізатор перевіряє файли за схожими характеристиками. При виявленні певної кількості схожих даних у файлі він приймає рішення, що дана програма схожа на шкідливу.

Поштовий фільтр перевіряє всі вхідні і вихідні поштові повідомлення на наявність шкідливих об'єктів, не допускаючи таким можливості для проникнення в систему загроз разом із електронним листом. Функція сканування – перевірка файлів на предмет наявності вірусів чи шкідливих програм.

Файловий шредер - спеціальна програма, яка дозволила максимально надійно видаляти непотрібні конфіденційні файли, без можливості їх нього відновлення. Принцип роботи програм-шредерів полягає в тому, що файл, який планується видалити, піддається багатопрохідному затиранню. Видалити файли можна або безпосередньо з меню антивірусу (вкладка Інструменти) або ж за допомогою контекстного меню, клікнувши правою кнопкою миші на будь-якому файлі та обрати в спливаючому меню пункт «Wipe files by Zillya! Internet Security» [69].

Отже, використання та постійне удосконалення сучасних комп'ютерних програм ІТ-спеціалістами Страхової компанії «Ю.Ес.Ай.» дозволяє піти на випередження співробітникам структурних підрозділів під час роботи із аналітичними обробками даних та системою звітів.

3.2. Удосконалення механізмів ідентифікації електронного довірчого підпису фахівців Товариства з додатковою відповідальністю страхова компанія «Ю.Ес.Ай.»

Робота із е-документаційним забезпеченням у Компанії включає і використання електронного довірчого підпису, що теж потребує час від часу удосконалення та захисту. За чинними нормативно-правовим документами, в Україні з 7 листопада 2018 року, відповідно до закону «Про електронні довірчі послуги» [49] електронний підпис може бути трьох категорій:

- простий електронний підпис та печатка – низький рівень довіри;
- удосконалений електронний підпис та печатка – середній рівень довіри;
- кваліфікований електронний підпис та печатка – високий рівень довіри.

Саме та лише кваліфікований електронний підпис (тобто, підпис з високим рівнем довіри) прирівнюється до власноручного (частина 4 статті 18 Закону про ЕДП) [49]. Електронний підпис - це електронні дані, які забезпечують цілісність документів та ідентифікують особу. У співробітників Компанії електронний підпис може зберігатися у вигляді MobileID, підпису на ID-картці, підпису на «токені» чи захищеному носії інформації. За допомогою електронного підпису уповноважені посадові особи Компанії, наприклад, страхові агенти, підписують електронні документи, користуються електронними послугами, реєструються на державних порталах тощо. Страхові документи із цим підписом мають таку саму юридичну силу, як і документи, підписані власноруч [49].

Так, Mobile ID – зручний і надійний засіб для електронної автентифікації та електронного підпису. Mobile ID допомагає співробітникам Компанії оперативно вирішувати питання за допомогою доступних електронних сервісів. Також, співробітники можуть віддалено підписувати договори в системах електронного документообігу Компанії, підтверджувати особистість на державних веб-ресурсах, отримувати адміністративні послуги. Mobile ID - це персональний кваліфікований підпис та засіб електронної ідентифікації, який зберігається на SIM-карті мобільного телефона уповноваженого співробітника Компанії. Електронна ідентифікація на державних та електронних ресурсах з підтримкою сервісу MobileID здійснюється через [33]:

- системи державних адміністративних послуг (понад 118 електронних послуг (наприклад, Державний портал адміністративних послуг, ЦНАП міста, Головний сервісний центр МВС України, Кабінет водія та інші).

- системи електронної звітності (кабінет платника податків: ідентифікація на ресурсі та доступ до усіх сервісів Державної фіскальної служби).

- системи е-документаційного забезпечення Компанії, коли є потреба підписувати договори, акти, накладні в електронній формі (ведення електронного документообігу в системах Star.Docs, Deals, Megapolis.DocNet, Document.Online, EDIN, Вчасно, АСКОД, SmartSign) [33].

Удосконалення користування електронним підписом здійснюється і через розуміння того, що, за чинним законодавством, кваліфіковані надавачі електронних довірчих послуг мають право: надавати електронні довірчі послуги з дотриманням вимог Закону України «Про електроні довірчі послуги»; отримувати документи, необхідні для ідентифікації особи, ідентифікаційні дані якої міститимуться у сертифікаті відкритого ключа; отримувати консультації від центрального засвідчувального органу або засвідчувального центру з питань, пов’язаних з наданням електронних довірчих послуг; звертатися до органів з оцінки відповідності для отримання документів про відповідність; звертатися із заявою про скасування,

блокування або поновлення сформованих у центральному засвідчувальному органі або засвідчувальному центрі кваліфікованих сертифікатів відкритих ключів [33].

У свою чергу, уповноважені співробітники Компанії як кваліфіковані надавачі електронних довірчих послуг зобов'язані забезпечити: захист персональних даних користувачів електронних довірчих послуг відповідно до вимог законодавства; функціонування програмно-технічного комплексу, що ними використовується, та захист інформації, що в ньому обробляється, відповідно до вимог законодавства; створення та функціонування свого веб-сайту; впровадження, підтримання в актуальному стані та публікацію на своєму веб-сайті реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів; можливість цілодобового доступу до реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів та до інформації про статус сертифікатів відкритих ключів через телекомунікаційні мережі загального користування; цілодобовий прийом та перевірку заяв підписувачів та створювачів електронних печаток про скасування, блокування та поновлення їхніх сертифікатів відкритих ключів [33].

Електронна ідентифікація співробітників Компанії здійснюється «за допомогою засобів електронної ідентифікації, що підпадають під схему електронної ідентифікації, затверджену Кабінетом Міністрів України» [51]. Міжнародні договори Компанії щодо електронних довірчих послуг передбачають порядок подання повідомлень та визнання схем електронної ідентифікації (із зазначенням рівня довіри для засобів електронної ідентифікації). Схема електронної ідентифікації співробітників Компанії встановлюють високий, середній або низький рівні довіри до засобів електронної ідентифікації, що використовуються в них. «Схема електронної ідентифікації визначається Кабінетом Міністрів України» [51].

Низький, середній та високий рівні довіри до засобів електронної ідентифікації повинні відповідати таким критеріям:

- низький рівень довіри до засобів електронної ідентифікації характеризує засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує обмежений ступінь довіри до заявлених або затверджених ідентифікаційних даних і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї відносяться, включаючи технічні засоби контролю, призначенням яких є зниження ризику зловживання або спростування ідентичності;

- середній рівень довіри до засобів електронної ідентифікації характеризує засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує суттєвий ступінь довіри до заявлених або затверджених ідентифікаційних даних і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї відносяться, включаючи технічні засоби контролю, призначенням яких є істотне зниження ризику зловживання або спростування ідентичності [51];

- високий рівень довіри до засобів електронної ідентифікації характеризує засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує найвищий ступінь довіри до заявлених ідентифікаційних даних особи і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї відносяться, включаючи технічні засоби контролю, призначенням яких є запобігання зловживанню повноваженнями або підміні особи.

Використання кваліфікованих електронних підписів та печаток у Компанії забезпечує високий рівень довіри до схем електронної ідентифікації. Використання удосконалених електронних підписів та печаток забезпечує середній рівень довіри до схем електронної ідентифікації. Маємо наголосити, що електронні довірчі послуги надаються уповноваженими співробітниками Компанії, як правило, на договірних засадах надавачами електронних довірчих послуг. До переліку електронних довірчих послуг входять:

- створення, перевірка та підтвердження удосконаленого електронного підпису чи печатки;

- формування, перевірка та підтвердження чинності сертифіката електронного підпису чи печатки [51];

- формування, перевірка та підтвердження чинності сертифіката автентифікації веб -сайту;

- формування, перевірка та підтвердження електронної позначки часу;

- реєстрована електронна доставка;

- зберігання удосконалених електронних підписів, печаток, електронних позначок часу та сертифікатів, пов'язаних з цими послугами [51].

Кожна послуга, що входить до складу електронних довірчих послуг, може надаватися як окремо, так і в сукупності. Діяльність кваліфікованих надавачів електронних довірчих послуг здійснюється за умови внесення коштів на поточний рахунок із спеціальним режимом використання у банку (рахунок в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхування цивільно-правової відповідальності для забезпечення відшкодування шкоди, яка може бути завдана користувачам таких послуг чи третім особам [49]. Розмір внеску на поточному рахунку із спеціальним режимом використання у банку (рахунку в органі, що здійснює казначейське обслуговування бюджетних коштів) або страхової суми не може становити менш як 1000 мінімальних розмірів заробітної плати.

Розподіл ризиків збитків, що можуть бути заподіяні користувачам електронних довірчих послуг та третім особам фізичними або юридичними особами, не внесеними центральним засвідчувальним органом до Довірчого списку, визначається суб'єктами правових відносин на договірних засадах. Електронна взаємодія фізичних та юридичних осіб, яка потребує відправлення, отримання, використання та постійного зберігання за участю третіх осіб електронних даних, аналоги яких на паперових носіях не повинні містити власноручний підпис відповідно до законодавства, а також автентифікація в інформаційних системах, в яких здійснюється обробка таких електронних даних, можуть здійснюватися з використанням електронних довірчих послуг або без отримання таких послуг, за умови попередньої

домовленості між учасниками взаємодії щодо порядку електронної ідентифікації учасників таких правових відносин [49].

Електронна взаємодія фізичних та юридичних осіб, яка потребує відправлення, отримання, використання та постійного зберігання за участю третіх осіб електронних даних, аналоги яких на паперових носіях повинні містити власноручний підпис відповідно до законодавства, а також автентифікація в складових частинах інформаційних систем, в яких здійснюється обробка таких електронних даних та володільцями інформації в яких є органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності, повинні здійснюватися з використанням кваліфікованих електронних довірчих послуг [49].

Уповноважені фахівці Компанії для засвідчення чинності відкритого ключа використовують лише кваліфікований сертифікат відкритого ключа, а для реалізації повноважень, спрямованих на набуття, зміну чи припинення прав та/або обов'язків фізичної або юридичної особи відповідно до закону [37], застосовують виключно засоби кваліфікованого електронного підпису чи печатки, які мають вбудовані апаратно-програмні засоби, що забезпечують захист записаних на них даних від несанкціонованого доступу, від безпосереднього ознайомлення із значенням параметрів особистих ключів та їх копіювання.

Порядок використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності встановлюється Кабінетом Міністрів України. Також, співробітники Компанії знають про те, що «використання електронних довірчих послуг не змінює порядку вчинення правочинів, встановленого законом. Правочини, що підлягають нотаріальному посвідченню та/або державній реєстрації у випадках, встановлених законом, вчиняються в електронній формі виключно із застосуванням кваліфікованих електронних довірчих послуг та у встановленому порядку» [49].

Кваліфікована електронна довірча послуга створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки надається кваліфікованим постачальником електронних довірчих послуг та включає:

- надання користувачам електронних довірчих послуг засобів кваліфікованого електронного підпису чи печатки для генерації пар ключів та/або створення кваліфікованих електронних підписів чи печаток, та/або перевірки кваліфікованих електронних підписів чи печаток, та/або зберігання особистого ключа кваліфікованого електронного підпису чи печатки;

- технічну підтримку та обслуговування наданих засобів кваліфікованого електронного підпису чи печатки [49].

Електронний підпис чи печатка співробітника Компанії не можуть бути визнані недійсними та позбавлені можливості розглядатися як доказ у судових справах виключно на тій підставі, що вони мають електронний вигляд або не відповідають вимогам до кваліфікованого електронного підпису чи печатки. 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 [53].

Обов’язкові вимоги до надання кваліфікованої електронної довірчої послуги створення, перевірки та підтвердження кваліфікованих електронних підписів чи печаток, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України. Випуск та обіг засобів електронної ідентифікації з функціями кваліфікованого електронного підпису як документів, що посвідчують особу, регулюються законодавством. Вимоги до кваліфікованих електронних довірчих послуг, які надаються з використанням засобів електронної ідентифікації з функціями кваліфікованого електронного підпису як документів, що посвідчують особу, встановлюються цим Законом та іншими актами законодавства.

Засоби кваліфікованого електронного підпису чи печатки повинні забезпечувати: належний рівень унікальності пари ключів, що ними генеруються; конфіденційність особистих ключів під час їх генерації, зберігання та створення кваліфікованого електронного підпису чи печатки; захист від доступу до особистих ключів сторонніх осіб. Засоби кваліфікованого електронного підпису чи печатки не повинні змінювати електронні дані, з якими пов'язаний цей кваліфікований електронний підпис чи печатка, або перешкоджати доступу до них підписувача чи створювача (уповноваженого представника створювача) електронної печатки [49].

Засоби кваліфікованого електронного підпису чи печатки під час перевірки кваліфікованого електронного підпису чи печатки надаються співробітнику Компанії як представнику електронних довірчих послуг у результаті процесу перевірки. Вимоги до засобів кваліфікованого електронного підпису чи печатки встановлюються Кабінетом Міністрів України. «Відповідність засобів кваліфікованого електронного підпису чи печатки зазначеним вимогам підтверджується документами про відповідність або позитивними експертними висновками за результатами їх державної експертизи у сфері криптографічного захисту інформації» [49]. Встановлення обов'язкових вимог до засобів кваліфікованого електронного підпису чи печатки, а також перевірка їх дотримання здійснюються відповідно до вимог, установлених Кабінетом Міністрів України.

Кваліфікована електронна довірча послуга формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки включає: створення умов для генерації пари ключів особисто підписувачем чи створювачем (уповноваженим представником створювача) електронної печатки за допомогою засобу кваліфікованого електронного підпису чи печатки; формування кваліфікованих сертифікатів електронного підпису чи печатки, що відповідають вимогам цього Закону, та видачу їх користувачу електронної довірчої послуги; скасування, блокування та поновлення кваліфікованих сертифікатів електронного підпису чи печатки у

випадках, передбачених Законом України «Про електронні довірчі послуги»; перевірку та підтвердження чинності кваліфікованих сертифікатів електронного підпису чи печатки шляхом надання третім особам інформації про їхній статус та відповідність вимогам чинного національного законодавства [49].

Надання доступу до сформованих кваліфікованих сертифікатів електронних підписів та печаток шляхом їх розміщення на офіційному веб-сайті кваліфікованого надавача електронних довірчих послуг, за умови згоди підписувача чи створювача електронної печатки на публікацію кваліфікованого сертифіката електронного підпису чи печатки. Формування та видача кваліфікованих сертифікатів електронного підпису чи печатки, що не відповідають вимогам Закону, заборонені. Обов'язкові вимоги до кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованого сертифіката електронного підпису чи печатки, а також порядок перевірки їх дотримання встановлюються Кабінетом Міністрів України [49].

Отже, робота уповноважених співробітників страхової компанії «Ю.Ес.Ай.» із електронними підписами та електронними печатками потребує не лише дотримання статей Закону України «Про електронні довірчі послуги», а й постійного удосконалення засобу від злому та е-крадіжки чи підробки.

3.3. «Хмарні» технології та їхня роль у збереженні інформації у структурних підрозділах Товариства з додатковою відповідальністю страхова компанія «Ю.Ес.Ай.»

Однією із важливих складових, пов'язаної із життєвим циклом е-документаційного забезпечення, є «хмарні» технології. Від часу своєї появи і на сьогодні «хмарні» технології удосконалюються відповідно до потреб сучасного постінформаційного суспільства. Так, одним із продуктів, що забезпечує у страховій компанії систему захисту і збереження е-

документаційної інформації, є Microsoft Office 365. Це – платний хмарний Інтернет-сервіс і програмне забезпечення компанії Microsoft, що розповсюджується за схемою «програмне забезпечення + послуги». «Хмарний» формат означає, що дані Компанії зберігаються в центрі обробки даних, а не на комп'ютерах співробітників, що забезпечує доступ до е-документів і даних через браузер із різних пристроїв з можливістю виходу в Інтернет [72].

Сервіс Office 365 був анонсований в жовтні 2010 року, публічне бета-тестування розпочалося у квітні 2011. Світова прем'єра відбулася 28 червня 2011 року, коли корпорація Microsoft запустила сервіс Office 365 у 40 країнах світу. Пакет був призначений для використання в компаніях від малого бізнесу до великих підприємств. «Хмарний» офісний пакет послуг Microsoft Office 365 у Компанії включає в себе:

- Microsoft Office Professional Plus, що забезпечує можливість роботи з е-документами в знайомому інтерфейсі за стосунків Office на комп'ютері, телефоні або через веб-браузер [72];

- Exchange Online, що дозволяє розгорнути співробітникам Компанії у «хмарі» сервіси електронної пошти Outlook, календаря і контактів і забезпечує захист від вірусів і спаму;

- SharePoint Online, що був використаний під час створення вебсайту Компанії і внутрішньої соціальної мережі для спілкування та взаємодії її співробітників;

- Lync Online для організації відео- і голосових конференцій з колегами і партнерами, а також можливість налаштування та використання програм обміну миттєвими повідомленнями. Сервіс може інтегруватися з корпоративними ERP і CRM-системами [72].

Office 365, встановлений у Компанії, доступний з багатьма різноманітними пакетами, що спрямовані на різні цілі та сегменти ринку та забезпечують різні потреби з різними варіаціями цін. Вони включають:

- Personal: включає доступ до Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft OneNote, Microsoft Outlook, Microsoft Publisher & Microsoft Access для домашнього/некомерційного використання (PC чи Mac), а також доступ до преміум-можливостей на одному планшеті (Android, iOS чи Windows RT) або телефоні. Додатково до цього є можливість користуватись 1 ТВ сховища на OneDrive і 60 хвилин міжнародних дзвінків у Skype [72].

- Business Essentials (раніше Small Business) використовується у доступі до гостьових Exchange, SharePoint і Lync сервісів.

- ProPlus: надає доступ до програм Office 2016 Professional Plus для 25 користувачів із 5 пристроями

На зауваження фахівців, «на сучасному ринку «хмарних» послуг найближчим конкурентом Office 365 є сервіси Google Docs/Google Apps, які Google пропонує з 2006 року. За даними самої Google, на червень 2011 ним користуються понад 3 млн компаній. Іншими конкурентами є рішення Zoho та ThinkFree» [72].

У «хмаро» орієнтованому середовищі співробітники Компанії використовують популярну поштову програму-клієнт Outlook (рис. 3.1.). Microsoft OneDrive - файл-хостинг, що базується у «хмаро» орієнтованому середовищі. Для всіх папок і файлів уповноваженим фахівцем Компанії присвоєно рівень доступу: від виключно персонального до публічного. Office Online дозволив завантажувати, створювати, редагувати і обмінюватися документами Microsoft Office Word, Excel, PowerPoint і OneNote просто у браузері і не тільки [72].

OneDrive підтримує перегляд формату pdf, а також стандарту odf. Функція пошуку OneDrive не підтримує пошук документів у форматі pdf, однак підтримується пошук форматів із пакету Microsoft Office: doc, docx, ppt, pptx, xls і xlsx. До сховища папку можна завантажити одним архівом, розмір якого не перевищує 4 ГБ. Основні види роботи з сервісом OneDrive:

- доступ до сховища файлів OneDrive,

- завантаження документів до сховища з комп’ютера або флешносія,

- створення файлів і папок у сховищі OneDrive он-лайн,

- забезпечення чи обмеження доступу до файлів і папок OneDrive,

- надання доступу до файлу конкретному користувачеві та оповіщення його про отримання такого доступу.

Основні види роботи з файлами в OneDrive:

- змінити назву,

- редагувати онлайн,

- забирати на редагування (при цьому обмежується доступ до документа, інші користувачі не зможуть з ним працювати),

- переглядати попередні версії файлів,

- завантажувати копію,

- стежити за внесеними змінами в документ іншими колегами тощо [72].

Рис. 3.1. Поштова програма-клієнт Outlook

Маємо наголосити, що перехід Компанії від стандартної локальної інфраструктури до «хмари» значно зменшив капітальні витрати не тільки на обладнання [37], а й на експлуатаційні витрати, пов’язані із технічним обслуговування, уможливив використання необхідних ресурсів. Тому, ще одна платформа, на якій зберігається інформація з е-докуемнтаційного забезпечення страхової компанії «Ю,Ес.Ай.» - Microsoft Azure. Microsoft Azure

«хмарна» платформа з широким спектром ресурсів та послуг, які дозволяють співробітникам Компанії швидко створювати, розгортати і керувати сервісами. Microsoft Azure повністю реалізує дві хмарні моделі — платформи як сервісу (Platform as a Service, PaaS) та інфраструктури як сервісу (Infrastructure as a Service, IaaS) і поширюється за принципом «Pay only for what you use», що дозволяє повністю контролювати свої витрати. Але Microsoft Azure не зосереджується тільки на хмарних ЦОД, підтримка гібридного формату інфраструктури надає співробітникам Компанії засоби для розширення можливостей зберігання, архівування та відновлення даних в максимально ефективному та економічному вигляді [37].

На сьогодні служби Azure доступні в 22 регіонах по всьому світу і забезпечують максимальну продуктивність у збереженні даних. Серед всіх служб та сервісів є основні, які задіяні майже у всіх сценаріях вирішення задач. Ним є сервіс віртуальних машин Azure, що дозволив співробітникам Компанії створювати і використовувати віртуальні машини в «хмарі», надає гнучкі можливості віртуалізації без необхідності купувати і обслуговувати фізичне обладнання. Хоча обслуговувати віртуальну машину — налаштовувати її, встановлювати виправлення і обслуговувати програмне забезпечення, яке працює на віртуальній машині, співробітнику Компанії доводиться самому, проте це значно спрощує процес володіння обчислювальною потужністю і дозволяє контролювати витрати на утримання. Використовуваний в технології для віртуальних машин підхід IaaS, дозволяє застосовувати її різними способами [72].

Деякі додатки вигідно виконувати в хмарному сервісі з економічних міркувань. Поширеним прикладом є додаток зі значними піками навантаження через велику кількість запитів у певний час, тоді варто обладнати свій центр обробки даних достатньою кількістю обладнання для обробки цих піків, але більшість із цього обладнання, швидше за все, буде простоювати. Виконання цієї програми в Azure дозволяє тримати додаткові віртуальні машини і запускати їх тільки в разі потреби та завершувати роботу після використання.

Похвилинна тарифікація дає можливість оплачувати тільки ті ресурси та час, якими дійсно користувались у Компанії [37].

При використанні аварійного відновлення в IaaS, замість утримання резервного центру обробки, який майже не використовується, у Компанії сплачують лише потрібні обчислювальні ресурси у випадку дійсної необхідності. Наприклад, якщо на основному центрі обробки даних виникає збій, можна створити в Azure віртуальні машини для виконання найбільш важливих додатків, а потім, коли необхідність в них зникне, завершити їх роботу [72].

За фахівцями, групи розробників часто використовують віртуальні машини, оскільки вони забезпечують швидкий і простий спосіб створення комп'ютера з певними конфігураціями, необхідними для написання коду і тестування програми. Віртуальні машини Azure пропонують раціональний і економічний спосіб створення віртуальних машин з подальшим видаленням тих, що вже не потрібні [72].

За допомогою технологій віртуальної мережі Azure у Компанії створено можна мережу (VNET), яка є частиною локальної її мережі. Це уможливило виконання на віртуальній машині Azure таких додатків як SharePoint, SQL Server і т.д. У свою чергу, віртуальна машина в Azure – це класична віртуальна машина з операційною системою, місцем для зберігання даних, можливістю підключення в мережу та з підтримкою виконання найрізноманітніших додатків (рисунок 3.2.) [72].

Рис. 3.2. Віртуальна мереаі Azure

Управління віртуальними машинами здійснюється за допомогою порталу через веб-браузер, через команди Powershell із підтримкою створення сценаріїв або безпосередньо за допомогою REST API. У діяльності Компанії залежно від виду потреб використовують віртуальні машини різного розміру. Так, віртуальними машинами серії A можна розгортати з використанням обладнання і процесорів різних типів. Розмір регулюється в залежності від обладнання, щоб забезпечити узгоджені показники продуктивності процесора для виконуваного екземпляра (незалежно від пристрою, на якому виконується розгортання) [72].

Віртуальні машини серії D призначені для додатків, яким необхідні великі обчислювальні потужності і високопродуктивні тимчасові диски. Віртуальні машини серії D відрізняються більш швидкими процесорами, більш високим співвідношенням «пам'ять — ядро» і твердотільним накопичувачем (SSD) в якості тимчасового диска.

Серія Dv2, наступне покоління серії D, відрізняється більш потужним ЦП. Процесор серії Dv2 приблизно на 35% швидше, ніж процесор серії D. Мається на увазі використання процесорів серії Intel Xeon® E5-2673 v3 (Haswell) з тактовою частотою 2,4 ГГц, а завдяки технології Intel Turbo Boost версії 2.0 може досягати 3, 2 ГГц. Серія Dv2 має такі ж конфігурації пам'яті та диска, як і серія D [72]. Віртуальні машини серії G відрізняються максимальним об'ємом пам'яті і працюють на серверах з процесорами сімейства Intel Xeon E5 V3. Для віртуальних машин серій DS, DSv2 і *GS* доступне високопродуктивне сховище Premium з мінімальною затримкою, призначене для робочих навантажень з високою інтенсивністю операцій вводу-виводу. Для розміщення дисків віртуальних машин використовуються твердотільні накопичувачі, а також надається локальний кеш SSD [72].

Власне сховище Azure це – «хмарне» рішення для зберігання сучасних додатків, що забезпечило у Компанії високу доступність і масштабованість для задоволення актуальних потреб. Сервіс збереження в Azure має високий ступінь масштабованості, дозволяючи зберігати і обробляти сотні терабайт

даних для підтримки сценаріїв з даними великого розміру, які необхідні для дослідницьких, аналітичних фінансових і мультимедійних додатків співробітникам Компанії. Також, можна зберігати і невеликі обсяги даних, необхідні, наприклад, для вебсайту Компанії [37].

Сховище Azure доступне з будь-якої точки світу і з програми будь-якого типу, незалежно від того, де воно виконується: в хмарі, на робочому столі, локальному сервері чи на мобільному пристрої. Сервіс гнучкий і дозволяє проєктувати програмні додатки для великої кількості користувачів Компанії, а потім масштабувати їх при необхідності як в плані обсягу сховища, так і за кількістю необхідних транзакцій. Тарифікуються тільки ті ресурси, які використовуються, і тільки тоді, коли використовуються. У сервісі збереження Azure застосовується система автоматичного розбиття, яка автоматично балансує навантаження, виходячи з трафіку даних. Це означає, що в міру зростання потреб вашого застосування сховище Azure автоматично виділяє відповідні ресурси [72].

Доступна служба збереження Azure Premium, коли потрібне сховище з високою продуктивністю, низькою затримкою для дискових операцій та високонавантажених робочих операцій, що виконуються на віртуальних машинах Azure. За допомогою служби сховища Azure Premium в якому використовуються SSD-диски, можливо підключення до віртуальної машини безліч постійних дисків з даними для забезпечення високої продуктивності операцій вводу-виводу. Сервіс збереження даних в Azure включає сховище BLOB-об’єктів, а також сховища таблиць, черг і файлове [72].

Всі BLOB-об’єкти організовані в контейнери, які надають зручний спосіб призначення політик безпеки групам об’єктів. Обліковий запис містить будь-яку кількість контейнерів, а контейнер містить будь-яку кількість BLOB-об’єктів. Ємність облікового запису для зберігання обмежена до 500 ТБ. Сервіс сховища типу «таблиці» для сучасних додатків, яким потрібні сховища даних з більшим ступенем масштабованості і гнучкості, ніж попереднім поколінням програмного забезпечення. Табличне сховище пропонує високу

ступінь доступності і масштабованості, дозволяючи додаткам автоматично здійснювати масштабування відповідно до запиту користувача. Таке NoSQL сховище типу «ключ-атрибут» немає схеми конструкції, на відміну від традиційних реляційних баз даних [72].

При розробці додатків для масштабування, компоненти програми часто не пов'язані між собою, так що вони можуть змінюватись незалежно один від одного. Сховище черг забезпечує надійне рішення по обміну повідомленнями для асинхронної взаємодії між компонентами програми, незалежно від того, де вони виконуються: в хмарі, на робочому столі, локальному сервері або мобільному пристрої. Сховище черг також підтримує управління асинхронними завданнями і побудову робочих процесів. Обліковий запис може містити будь-яку кількість черг. Черга може містити будь-яку кількість повідомлень в межах ємності облікового запису зберігання.

Файлове сховище, в якому доступні загальні папки з файлами SMB розташовані в хмарі, завдяки чому швидко і без додаткових затрат співробітники Компанії виконують перенесення додатків попередніх версій, зв'язаних із загальними папками. Завдяки файловому сховищу Azure програми, що працюють на віртуальних машинах Azure або хмарних службах, можуть підключити загальну папку в хмарі, по типу локального додатку при підключенні звичайної загальної папки SMB. Будь-яка кількість компонентів цих додатків, може одночасно підключатися і отримувати доступ до ресурсів сховища [72].

Отже, як показує досвід страхової компанії «Ю.Ес.Ай.» задля оптимізації життєвого циклу сучасного е-страхового документаційного забезпечення можливе використання двох «хмарних» сервісів. У цілому, шляхи удосконалення механізмів е-документаційного забезпечення аналізованої нами страхової компанії «Ю.Ес.Ай.» скеровані на оптимальну роботу співробітників, на можливість зосередитись саме на процесах страхування, а не паперовій бюрократичній роботі.

ВИСНОВКИ

Дослідження теми магістерської кваліфікаційної роботи «Механізми електронного надання документаційного забезпечення сучасної установи» уможливили зробити такі висновки, відповідно до поставлених завдань:

1. З'ясовано законодавчо-правові основи електронного надання документаційного забезпечення сучасної установи, підгруням для яких є Конституція України, Цивільний процесуальний кодекс України, закони України «Про інформацію», «Про захист інформації в автоматизованих системах», «Про державну таємницю», «Про телекомунікації», «Про обов'язковий примірник документів», «Про Національний архівний фонд та архівні установи», Закон України «Про електронні документи та електронний документообіг», ДСТУ 4163:22020, інші нормативно-правові акти.

2. Аналіз організації електронного документаційного забезпечення сучасної установи довів, що організація е-документаційного забезпечення здійснюється на таких принципах: рух документів повинен мати мінімальну кількість повернень на попередні етапи; документи повинні спрямовуватись виконавцям у відповідності з їх обов'язками, щоб уникнути дублювання операцій. Е-документаційне забезпечення охоплює три основні завдання стосовно програмних засобів автоматизації: документування (створення документів, які підтримують і реєструють управлінську діяльність, тобто їх підготовку, оформлення, узгодження та виготовлення); організація документообігу (забезпечення руху, пошуку, зберігання і використання документів); систематизація архівного зберігання документів. Етапи переведення документа в електронну форму такі:

1. Сканування документа і створення його електронної копії у вигляді зображення (образ документа). У процесі сканування виконується візуальний контроль якості.

2. Розпізнавання сканованих документів - переведення зображення у текстовий документ. З точки зору переведення документа у електронний вид

їх умовно поділяють на кілька типів. Переведення кожного із видів документів у електронну форму має такі особливості:

- для фотографій достатньо їх електронного зображення;

- при переведенні текстів - їх необхідно розпізнати, можливо, відновити форматування:

- при введенні анкет, бюлетенів для голосування та ін., зазвичай, не потрібно зображення власне документа, а достатньо лише інформації про те, за кого віддано голос.

3. Аналіз системи захисту інформації в електронному документообігу уможливив висновки про те, що захист інформації в системі діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі; комплексна система захисту інформації – взаємопов’язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації. Суб'єктами відносин, пов’язаних із захистом інформації в системах, є: володільці інформації; власники системи; користувачі; спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв’язку та захисту інформації і підпорядковані йому регіональні органи. Одним із видів захисту інформації є криптографічний захист, за якого відбувається перетворення інформації із використанням спеціальних даних з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо. Для забезпечення захисту інформації у системі створюється комплексна система захисту інформації, яка призначається для захисту інформації від:

- витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;

- несанкціонованих дій з інформацією, у тому числі з використанням комп’ютерних вірусів;

- спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування.

4. Дослідження нормативного підґрунтя механізмів електронного надання документаційного забезпечення у Товаристві з додатковою відповідальністю страхова компанія «Ю.Ес.Ай.» довело, що основні вимоги до змісту та порядку укладання договорів страхування, права та обов'язки сторін визначені в Законі України «Про страхування». Договір страхування повинен містити: назву документа; назву та адресу страховика; прізвище, ім’я, по батькові або назву страхувальника і його адресу; зазначення об’єкта страхування; розмір страхової суми; перелік страхових випадків; визначення розміру тарифу, розмір страхових внесків і терміни їх сплати; термін дії договору; порядок зміни і припинення дії договору; права та обов’язки сторін і відповідальність за невиконання або неналежне виконання умов договору; інші умови за згодою сторін; підписи сторін.

5. Системи внутрішнього та зовнішнього документаційного забезпечення структурних підрозділів Товариства з додатковою відповідальністю страхова компанія «Ю.Ес.Ай.» взаємодіють відповідно до типового документообігу, притаманного якісному та безпечному веденню бізнесу в Україні. Найбільш поширеними внутрішніми документами Страхової компанії є: правила внутрішнього розпорядку; посадові інструкції; положення (про оплату праці, про відпустки, про дивіденди, про бухгалтерію та ін.); інструкція про печатки та штампи; колективний договір; пакети документів у сфері інформаційної безпеки підприємства; пакети документів у сфері охорони праці, пожежної безпеки.

Суто специфічними документами, наявними у страховій діяльності, також, є: рахунок страховика; коверкот; абандон; договір страхування; поліс валютований; претензія; франшиза.

6. Шляхи удосконалення механізмів надання документаційного забезпечення Товариства з додатковою відповідальністю страхова компанія

«Ю.Ес.Ай.» були нами визначення як такі, що сприяють безпеці системи захисту інформації, слідкують за трафіком, потоком навантаження на комунікаційну систему Страхової компанії, а саме: звернення, кількість переданих за одиницю часу пакетів або повідомлень у різних системах, мережах, включаючи телекомунікаційні та транспортні мережі, обсяг переданих або прийнятих даних. Відповідно до напрямку транспортування розрізняють: вхідний трафік - визначається обсягом вхідного потоку; вихідний трафік - визначається обсягом вихідного потоку. У свою чергу, постійний моніторинг над безпекою електронної пошти дозволяє прискорювати зчитування даних, внутрішніх і зовнішніх е-документів тощо.

Постійного удосконалення потребують і кваліфіковані електронні підписи та печатки, що забезпечують у Страховій компанії високий рівень довіри до схем електронної ідентифікації. Використання удосконалених електронних підписів та печаток забезпечує середній рівень довіри до схем електронної ідентифікації. У «хмаро» орієнтованому середовищі співробітники Страхової компанії задля посилення безпеки інформації використовують популярну поштову програму-клієнт Outlook. Microsoft OneDrive - файл-хостинг, що базується у «хмаро» орієнтованому середовищі. Для всіх папок і файлів уповноваженим фахівцем Компанії присвоєно рівень доступу: від виключно персонального до публічного. Office Online дозволив завантажувати, створювати, редагувати і обмінюватися документами Microsoft Office Word, Excel, PowerPoint і OneNote просто у браузері і не тільки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бебик В.М. Інформаційно-комунікаційний менеджмент у глобальному суспільстві: навч. посібн. URL: http://books.br.com.ua/themes/185/221

2. Безкровний М. Ф., Кропивка М.Ф., Палеха Ю.І., Іщенко Т.Д. Загальне діловодство: теорія та практика керування документацією із загальних питань. Київ: «Ліра-К», 2014. 456 с.

3. Блощинська В. Сучасне діловодство: Навчальний посібник. Київ: Центр навчальної літератури, 2005. 319 с.

4. Булава М. CRM – перспективний напрямок розвитку будь-якої компанії. Страхова справа. 2003. №3. С. 86–87.

5. Вимоги до форматів криптографічних повідомлень: Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України від 18.12.2012 № 739; станом на 02. 06. 2020 р. URL: https://zakon.rada.gov.ua

6. Вимоги до структури та змісту XML-схеми метаданих електронного примірника описів справ постійного зберігання: метод. рекомендації / Держ. арх. служба України, УНДІАСД; уклад.: Гаранін О. Я., Купрунець Т. Я. Київ, 2015. 28 с.

7. Вимоги щодо найменування файлів електронних примірників описів справ постійного зберігання: Наказ Міністерства юстиції України від 11. 11. 2014 р. № 1886/5. URL: https://zakon.rada.gov.ua

8. Віднесення електронних інформаційних ресурсів до Національного архівного фонду. Аналітичний огляд / Держ. архівна служба України; Укроку наук.-досл. ін-т архів. справи та документознавства; уклад.: Т. М. Ковтанюк, Н. М. Христова. Київ, 2012. 33 с.

9. Гаманкова О.О. Ринок страхових послуг України. Теорія, методологія, практика: Монографія. Київ: КНЕУ, 2009. 135 с.

10. Демидов Д. Швидкі CRM-проекти: за і проти. Страхова справа. 2011. № 3. С. 47–49.

11. Діденко А. Сучасне діловодство. Київ: Либідь, 2004. 383 с.

12. ДСТУ 4163:2020. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів. URL: https://undiasd.archives.gov.ua/

13. ДСТУ ISO 9001-2015. Системи управління якістю настанови щодо поліпшення діяльності (34051). URL: https://dnaop.com/html/34051

14. ISO 15489-1:2016. Інформація та документація. Управління документами. Частина 1. Поняття та принципи. URL**:** https:// archives.gov.ua/

15. Електронний архів. URL: http://www.archives.gov.ua

16. Єдиний державний реєстр підприємств та організацій України (ЄДРПОУ) (ведення ЄДРПОУ здійснює Державний комітет статистики України). URL: https://usr.minjust.gov.ua/ua/freesearch

17. Єжова Л. Ф. Інформаційний маркетинг. Київ: КНЕУ, 2012. 560 с.

18. Жук О.О. Зарубіжний досвід у сфері страхування та можливості його використання. Зовнішня торгівля: економіка, фінанси, право, 2014 URL: irbis-nbuv.gov.ua

19. Загорецька, О.М . Службові документи сучасної організації. Київ, 2005. 120 с.

20. Заруба О. Д. Основи страхування: посібник. Київ: Українсько-фінський інститут менеджменту і бізнесу, 1995. 180 с.

21. Інтернет-ресурс: URL: https://insuranceukraine.online/

22. Інтернет-ресурс: URL: https://uk.wikipedia.org/wik

23. Інтернет-ресурс: Список законодавчої термінології. URL: https://uk.wikipedia.org

24. Карпенко С. Г., Попов В.В., Тарнавський Ю.А., Шпортюк Г.А. Інформаційні системи і технології: Навч. посіб. для студ. вищ. навч. закл. Київ: МАУП, 2004. 192 с.

25. Кислюк В. Спеціальне документознавство. Київ: Кондор, 2011. 192 с.

26. Кінащук Л. Л. Страхове право: підручник. Київ: Атіка, 2007. 256 с

27. Конституція України. URL: https://zakon.rada.gov.ua

28. Концепція планування життєвого циклу електронних документів / Держ. архівна служба України; Центральний державний електронний архів України; уклад.: Ковтанюк Ю. С., Забенько Ю. І. Київ, 2011. 60 с

29. Ланге Д. Управління взаємовідносинами з клієнтами – нова стратегія в роботі страхових компаній. Страхова справа. № 2(10). С. 58–65.

30. Литвинова С.Г., Спірін О.М., Анікіна Л.П. Хмарні сервіси Office 365: навчальний посібник. Київ: Компринт, 2015. 170 с.

31. Матвієнко О., Цивін М. Основи організації електронного документообігу: Навчальний посібник. Київ: Центр учбової літератури, 2008.112 с.

32. Міністерство цифрової трансформації. URL: https://thedigital.gov.ua/

33. Моргун К. Інформаційне забезпечення інноваційної діяльності страхових компаній. Львів, 2013. URL: http://kerivnyk.info/2013/01/morgun.html

34. Нечипорук Л.В. Страховий ринок: закономірності становлення та розвитку в умовах глобалізації: Монографія. Харків: Право, 2010. 345 с.

35. Нєізвєстна О.В. Інформаційне забезпечення менеджменту страхової діяльності. Мукачів, 2017. URL: ile:///C:/Users/1/Downloads/110.pdf

36. Новаківський І.І. Інформаційні системи в менеджменті: системний підхід. Навчальний посібник. Львів: Вид-во «Національний університет Львівська політехніка», 2010. 202 с.

37. Офіційний сайт Товариства з додатковою відповідальністю страхова компанія «Ю.Ес.Ай». URL: https://usi.net.ua/

38. Палеха Ю. Управлінське документування: У 2 ч. ч. 1. Київ: Вид-во Європ. ун-ту, 2003. 383 с.

39. Перелік форматів даних електронних документів постійного і тривалого (понад 10 років) зберігання / Держ. архів. служба України, УНДІАСД; авт.: П. М. Марченко, Ю. С. Ковтанюк. Київ, 2011. 10 с

40. Піратовський Г. Л. Страховий бізнес: управління розвитком: монографія. Київ: КНТЕУ, 2006. 253 с.

41. Правила організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях: Наказ Міністерства юстиції України від 18.06.2015 № 1000/5 станом на 07. 11. 2018 р. URL: http://zakon.rada.gov.ua

42. Про бухгалтерський облік та фінансову звітність в Україні: Закон України станом на 17. 06. 2020 р. URL: http://zakon.rada.gov.ua/laws

43. Про внесення змін до Положення про Єдиний державний реєстр підприємств та організацій України: Постанова Кабінету Міністрів України від 22 червня 2005 р. № 499 URL: http://zakon.rada.gov.ua

44. Про господарські товариства: Закон України станом на 03.07.2020 р. URL: https://zakon.rada.gov.ua/

45. Про державну службу: Закон України станом на 23. 07. 2020 URL: https://zakon.rada.gov.ua/laws

46. Про державну таємницю: Закон України. Відомості Верховної Ради України. 1994. N 16. Ст. 93.

47. Про дорожній рух: Закон України станом на 16. 10. 2020 р. URL: https://zakon.rada.gov.ua/laws

48. Про доступ до публічної інформації: Закон України станом на 14. 09. 2019 р. URL: https://zakon.rada.gov.ua/laws

49. Про електронні довірчі послуги: Закон України станом на 07. 11. 2018 р. URL: https://zakon.rada.gov.ua/

50. Про електронні документи та електронний документообіг: Закон України станом на 17. 11. 2018 р. URL: https://zakon.rada.gov.ua/

51. Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації:

Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141; станом на 01. 02. 2016. URL: http://zakon.rada.gov.ua

52. Про захист інформації в автоматизованих системах: Закон України станом на 10. 11. 2016 р. URL: https://zakon.rada.gov.ua

53. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України станом на 04. 07. 2020 р. URL: https://zakon.rada.gov.ua/laws

54. Про захист персональних даних: Закон України станом на 12. 11. 2018 р. URL: https://zakon.rada.gov.ua

55. Про інформацію: Закон України станом на 12. 10. 2018 р. URL: https://zakon.rada.gov.ua

56. Про колективні договори і угоди: Закону України станом на 27. 12. 2019 р. URL: https://zakon.rada.gov.ua/laws

57. Про криптографічний та технічний захист інформації: Закон України. URL: https://www.president.gov.ua/documents/2594-iv-2760

58. Про мови в Українській РСР: Закон УРСР. Відомості Верховної Ради УРСР. 1989. N 45. Ст. 631.

59. Про Національний архівний фонд та архівні установи: Закон України станом на 16. 10. 2020 р. URL: https://zakon.rada.gov.ua/laws

60. Про обов'язковий примірник документів: Закон України станом на 22. 08. 2020. URL: http://zakon.rada.gov.ua/laws/

61. Про санкції: Закон України станом на 15. 08. 2020. URL: http://zakon.rada.gov.ua/

62. Про Стратегію сталого розвитку «Україна—2020»: Указ Президента України від 12 січня 2015 р. № 5. URL: https://zakon.rada.gov.ua/

63. Про страхування: Закон України станом на 21. 11. 2017. URL: http://zakon.rada.gov.ua/

64. Про схвалення Концепції розвитку електронного урядування в Україні: Розпорядження КМУ від 20 вересня 2017 р. № 649-р URL: https://www.kmu.gov.ua/npas/250287124

65. Про фінансові послуги та державне регулювання ринків фінансових послуг: Закон України станом на 21.12.2017. URL: http://zakon.rada.gov.ua/

66. Ротова Т. А. Страхування: Навч. посіб. Київ: Київ. нац. торг.-екон. ун-т, 2006. 400 с

67. Стислий опис системи е-документообігу АСКОД. URL: http://www.docflow.ua/products/ackod.pdf

68. Страхування: підручник / керівник авт. кол. і наук. ред. С. С. Осадець. Вид. 3-тє, без змін. Київ: КНЕУ, 2006. 599 с.

69. Сучасні антивірусні програми. URL: http://antivirus.pp.ua/

70. Типова інструкція з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві: Постанова від 17 січня 2018 р. № 55 станом на 15. 09. 2020 URL: http://zakon.rada.gov.ua

71. Ткаченко Н. В. Управління взаємовідносинами з клієнтами - фактор успішної діяльності страховика. Вісник Української академії банківської справи № 2(35) 2013 р. URL: VUABS_2013_2_20.pdf

72. Хмарні рішення Microsoft Azure URL: http://integritysys.com.ua/solutions/privatecloud-solution-azure/

73. Цивільний процесуальний кодекс України. URL: http://zakon.rada.gov.ua

74. Шумелда Я. П. Страхування. Тернопіль: Джура, 2006. 296 с

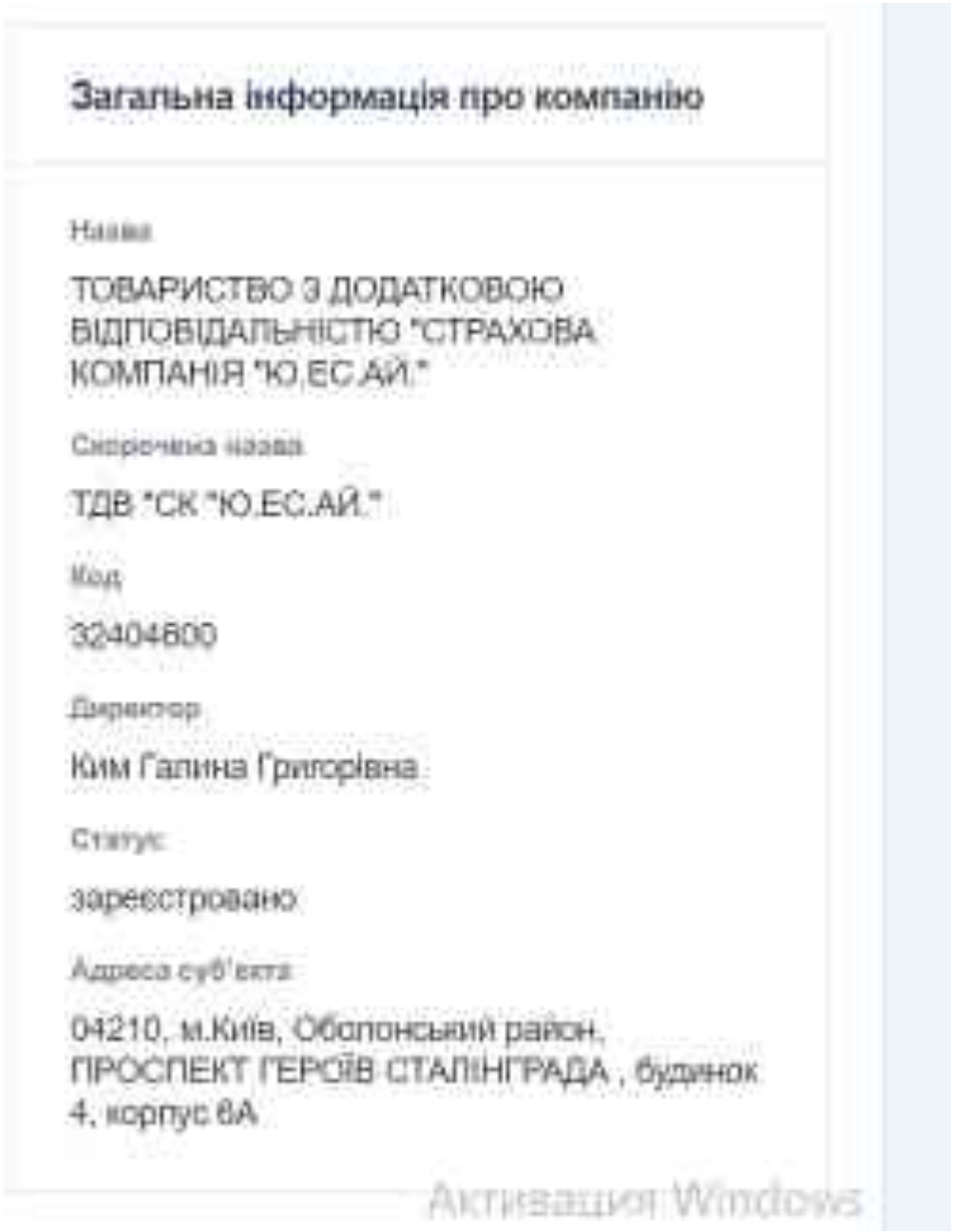
75. Щедріна Олена Іванівна. Нові інформаційні технології: Навч. Посібник. Київ: КНЕУ, 2005. 445 с.

76. Яворська Т. В. Страхові послуги: навч. посіб. Київ: Знання, 2008. 350 с.

ДОДАТКИ

Додаток А

Загальні відомості про страхову компанію «Ю.Ес.Ай.»
(джерело: Інспекційний портал)



Загальна інформація про компанію

Назва

ТОВАРИСТВО З ДОДАТКОВОЮ ВІДПОВІДАЛЬНІСТЮ "СТРАХОВА КОМПАНІЯ "Ю.ЕС.АЙ."

Скорочена назва

ТДВ "СК "Ю.ЕС.АЙ."

Код

32404600

Директор

Ким Галина Григорівна

Статус

зареєстровано

Адреса суб'єкта

04210, м.Київ, Оболонський район, ПРОСПЕКТ ГЕРОЇВ СТАЛІНГРАДА , будинок 4, корпус 6А

Додаток Б

Супровідне документаційне забезпечення страхової компанії «Ю.Ес.Ай»

(джерело: офіційний сайт Кмопанії)

ДЕРЖАВНА АВІАЦІЙНА СЛУЖБА УКРАЇНИ

[redacted]

ТДВ «Страхова компанія «Ю.ЕС.АЙ.»

Відповідно до вимог п. 59 Ліцензійних умов провадження господарської діяльності з надання фінансових послуг (крім професійної діяльності на ринку цінних паперів), затверджених постановою Кабінету Міністрів України від 07 грудня 2016 року № 913, на підставі наказу Державіаслужби від 17.01.2017 № 21 «Про реєстрацію страховиків, які мають дозвіл на обов'язкове авіаційне страхування цивільної авіації» та звернення страхової компанії, ідентифікованої як товариство з додатковою відповідальністю «Страхова компанія «Ю.ЕС.АЙ.», яке має дозвіл на обов'язкове авіаційне страхування цивільної авіації, 11.06.2020 зареєстровано в Державіаслужбі та внесено до Реєстру страховиків за порядковим номером 63.

Голова Олександр БІЛЬЧУК

МІНІСТЕРСТВО РЕГІОНАЛЬНОГО РОЗВИТКУ, БУДІВНИЦТВА ТА ЖИТЛОВО-КОМУНАЛЬНОГО ГОСПОДАРСТВА УКРАЇНИ

АТЕСТАЦІЙНА АРХІТЕКТУРНО-БУДІВЕЛЬНА КОМІСІЯ

Серія АЕ № 002805

КВАЛІФІКАЦІЙНИЙ СЕРТИФІКАТ

відповідального виконавця окремих видів робіт (послуг), пов'язаних із створенням об'єкта архітектури

Експерт
(найменування професії)

Виданий про те, що Каліченко Сергій Євгенович
(прізвище, ім'я, по батькові)

пройшов(ла) професійну атестацію, що підтверджує його (її) відповідність кваліфікаційним вимогам у сфері діяльності, пов'язаної із створенням об'єктів архітектури, професійну спеціалізацію, необхідний рівень кваліфікації і знань.

Категорія: Експерт

Кваліфікаційний сертифікат видано згідно з рішенням Атестаційної архітектурно-будівельної комісії (далі - Комісія) від _____ № _____

(рішенням відповідної секції Комісії від 09.10.2013 № 38, затвердженим президією Комісії 10.10.2013 № 38-Е).

Зареєстрований у реєстрі атестованих осіб 10.10 2013 року за № 2685.

Роботи (послуги), пов'язані із створенням об'єктів архітектури, спроможність виконання яких визначено кваліфікаційним сертифікатом: Технічне обстеження будівель і споруд.

Дата видачі 10.10 2013 року

(Голова, заступник голови) Атестаційної архітектурно-будівельної комісії Барзилович Д.В.
(прізвище, ім'я, по батькові)

Згідно з оригіналом

Додаток В

Схема структура е-документаційного забезпечення установи

(за В. Петровою)

Додаток Г

Схема е-документаційного забезпечення сучасної установи

(за М. Цивіним)