2. Системний аналіз: підручник / А. В. Катренко. — Л. : Новий Світ — 2000, 2011. — 396 с. — (Комп'ютинг). https://nubip.edu.ua/sites/default/files/u214/sistemniy_analiz_ki_2021.pdf

УДК 004.056.5:002

Шафранова Д.Д., здобувач
Зелінська О. В., к.т.н., доцент, доцент кафедри інформаційних технологій

ІНФОРМАЦІЙНА БЕЗПЕКА ДОКУМЕНТІВ

Донецький національний університет імені Василя Стуса, м. Вінниця

Вступ. У сучасному світі суспільство все частіше використовує і розробляє різні технології які спрощують життя. Сьогодні більшість організацій, підприємств, фірм переходять на електронний документообіг, тому що це зручно і безпечно. Але при роботі з електронними документами постає питання безпеки: як захистити від різних ушкоджень, зломів і зберегти інформацію від небажаних користувачів? Зараз у воєнний час безпека документів стала більш актуальною, ніж раніше. Оскільки документи відіграють значну роль в житті людини та в різних організаціях. Без них неможливо довести існування чогось або когось.

Актуальність. Зараз тема «Інформаційна безпека документів» привертає до себе значну увагу. Через війну в Україні багато різних підприємств були змушені покинути своє звичне місце роботи й переїхати на безпечну територію нашої держави або виїхати за кордон. Тим самим зберегти в цілісності усі важливі документи, а також не дати змоги ворогу доступу до приватної інформації.

Аналіз останніх досліджень. Питання інформаційної безпеки досліджувалось різними науковцями: В. Пилипчуком, В. Брижком, М. Зубком, Б. Кормичем, В. Цимбалюком, Я. Жарковим.

Мета роботи – дослідити та проаналізувати роль інформаційної безпеки документів в Україні.

Викладення основного матеріалу. Сьогодні інформаційні системи підтримують різні сервери та переносять велику кількість різних даних, що важко було уявити ще декілька років тому. Це необхідно для багатьох інфраструктур, наприклад для державних органів влади, електронних мереж обслуговування населення, навчання. Тому безпека та розвиток інформаційних систем – актуальне питання. Для кожного випадку визначення безпеки означає специфікацію політики безпеки, тобто безлічі бажаних цілей. Наприклад, електронна система голосування повинна бути встановлена таким чином, щоб голосувати могли тільки зареєстровані виборці, доступ до веб-сервера повинен здійснюватися аутентифікованими користувачами, тільки авторизовані користувачі повинні підключатися до банківської системи [1].

Для документа, як носія інформації, характерними властивостями є: цінність, достовірність, актуальність, конфіденційність, цілісність, доступність, спостережність.

Як вже зазначалось вище, більшість різних організацій намагаються перейти з паперової на електрону форму документів. Але в кожного фактора є свої плюси й мінуси. Як приклад, електрону форму можна зламати, загроза конфіденційності, збій у роботі серверу електронного документообігу, також в процесі роботи виникають різні технічні проблеми, чим можуть зробити різну шкоду документам. Але і паперова форма документів теж не ідеальна, її набагато легше можна позбутись, ніж електронної. Наприклад, різні незвичайні ситуації, які можуть виникати на підприємствах, також паперовий варіант його легше загубити.

Але якщо у мирний час робота з паперовими документами була зрозумілою і передбачуваною, могла тривати кілька днів чи тижнів і навіть місяців, то з моменту 24 лютого з початку повномасштабної війни в Україні, реальність непередбачувана і велика кількість підприємств, незалежно від їх розміру та організаційно правової форми — ТОВ, ПП, ДП — чи ФОП втратили (повністю або частково) свої приміщення, майно, а з ними й документи. Для підприємця, офіси якого опинились в зоні бойових дій, це створює додаткові проблеми, вирішення яких зараз ускладнює діяльність [2].

По-перше, це величезне фінансове навантаження для підприємства і додаткова робота для усіх працівників організації, адже відновлення втрачених документів потребує часу та зусиль. А за вимогами законодавства на відновлення втрачених, знищених документів бізнес має 90 днів. Тому електронний варіант в такому випадку більш надійний, ніж паперовий [2].

По-друге, як приклад, можна навести ситуацію магазину «Кейс ТМ Novus». 20 березня вщент згорів його головний офіс. У приміщенні знаходились усі паперові документи, які дали змогу розгорітися пожежі ще більше та були знищені. Але документи за короткий проміжок часу вдалось відновити у електронному вигляді. Тисячі документів для репарації у цифровому форматі організація спромоглась підготувати за кілька днів, що було б просто неможливим з використанням паперу. Ці документи неможливо знищити, вони легітимні та мають юридичну силу. В умовах війни перехід на е-документи є зручнішим та безпечнішим для бізнесу і не тільки [2].

Сьогодні таких прикладів можна наводити безліч, тому що такі ситуації трапляються кожного дня і не по одному разу. Також шкоди зазнали деякі відомі торгівельні марки:

- Мережа супермаркетів АТБ за час війни втратила кілька розподільчих центрів, зокрема, був повністю знищений центр у Київській області площею у 25 000 кв м, ще один зруйнований наполовину.
- Ракетного удару зазнав магазин Auchan в Одесі, також частково постраждав Auchan у Харкові.

- 59 торгових об'єктів Fozzy Group були частково або повністю зруйновані, ще 40 об'єктів знаходяться у зоні бойових дій [3].

100% безпеку електронного документообігу теж не можна забезпечити. Але існують деякі правила для підприємств, які можна використати і це потребує не великих фінансових затрат.

1. Ознайомлення усіх найманих працівників з документами в яких зазначена політика компанії й отримання розписки.
2. Використати ретельний контроль за персоналом.
3. Блокування усіх документів, які стосуються організації чи підприємства.
4. Підвищення рівня фізичного захисту.
5. Непомітна перевірка послужного списку найманого працівника.

Сьогодні 8 місяців як в Україні триває повномасштабна війна і ворог не тільки знищує міста та населені пункти, але до його рук потрапляє безліч документів різних організацій і підприємств. В такому випадку потрібно вживати такі заходи:

1. Документи основного виду підприємства і персональні дані потрібно постаратись зберегти та вивезти їх у безпечне місце, якщо така можливість відсутня, то забезпечити зберігання у закритому приміщені або в укритті цього приміщення. Але, якщо існує потенційна загроза життю людей лишити усі документи у приміщені [4].
2. Якщо документ має обмежений доступ або державну таємницю його потрібно знищити. При такому знищенні необхідні оформити відповідні акти, дотримуючись вимог нормативно-правових актів, які це регулюють. Водночас матеріали з основної діяльності знищувати не потрібно, передбачаючи можливість повернення населеного пункту під контроль органів влади України або подальшу передачу [4].
3. Якщо документи знаходяться на ПК чи серверах потрібно заздалегідь скопіювати вміст серверів та необхідну інформацію про працівників на персональні носії і обов'язково вивезти їх. Перед тим, як залишити приміщення, необхідно унеможливити доступ із технічних засобів до реєстрів [4].

Висновки. Кожне підприємство чи організація вправі самі вирішувати для себе який формат документації вести. Хтось веде тільки електронну чи паперову форму, а хтось навпаки паперову та електрону. Але зараз у нашій країні нестабільний час і електронний документообіг в такій ситуації переважає. Створення електронних архівів на підприємстві це не тільки економія часу і зручність, а і гарантована безпека для організацій.

Список використаних джерел

1. *Інформаційна безпека. Навчальний посібник. Ч. 2 / С. В.Кавун, В. В. Носов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2008. – 8 с.*

2. *Втрачені первинні документи під час війни: що необхідно знати? [Електронний ресурс]. – Режим доступу: https://medoc.ua/news/vtrachen-pervinn-dokumenti-pd-chas-vjni-shho-neobhdno-znati*
3. *Електронні документи – це безпека для бізнесу під час війни. [Електронний ресурс]. – Режим доступу: https://news.dtkt.ua/debet-kredit/partner-news/78266-elektronni-dokumenti-ce-bezpeka-dlya-biznesu-pid-cas-viini*
4. *Кадровик – 01. [Електронний ресурс]. – Режим доступу: https://prokadry.com.ua/news/7686-yak-buti-z-kadrovimi-buhgalterskimi-ta-nshimi-dokumentami-u-raz-zagrozi-zahoplennya*

УДК 004.01

Шафорост В. В., Корнієнко К. К.,
здобувачі 3 курсу спеціальності 122
«Комп'ютерні науки»
Ніколюк П. К.,професор, доктор
фізико-математичних наук.

МОДЕЛЮВАННЯ ІННОВАЦІЙНИХ ПРОЦЕСІВ ДЛЯ РОЗВИТКУ ЕКОНОМІКИ УКРАЇНИ

Донецький національний університет імені Василя Стуса

В умовах реалізації моделі інноваційного розвитку національна економічна стратегія спрямована на посилення інноваційного процесу, зміну характеру і співвідношення елементів екстенсивного та інтенсивного розвитку та характеру інноваційного процесу. У зв'язку з цим основною метою та призначенням стратегії економічного розвитку є встановлення спрямованості інновацій та розвиток і формулювання відповідних заходів та дій.

В інноваційному процесі доцільно будувати сценарії майбутніх подій і моделювати абстрактно-логічну структуру інноваційних зв'язків. Діагностика інноваційних можливостей і встановлення моделей є важливими етапами стратегічного управління інноваційним процесом. Політика, заснована на моделі, і дослідження потреб груп інтересів допомагають розробити цільові системи та надають мети інноваційному процесу.

Для прогнозування в економічній, соціальній, політичній та інших сферах вчені виділяють такі основні методи:

- метод екстраполяції, що встановлює застосування минулих і дійсних подій, зв'язків і поєднань на майбутнє;
- метод інтерполяції − формулювання перехідних значень функції, враховуючи відомі її значення;
- метод побудови сценаріїв − застосування систематичної послідовності явищ для встановлення варіантів розвитку об'єкта;
- статистичне моделювання − створення і розгляд моделей, математичних рівнянь, які розкривають взаємозв'язки, структурні і