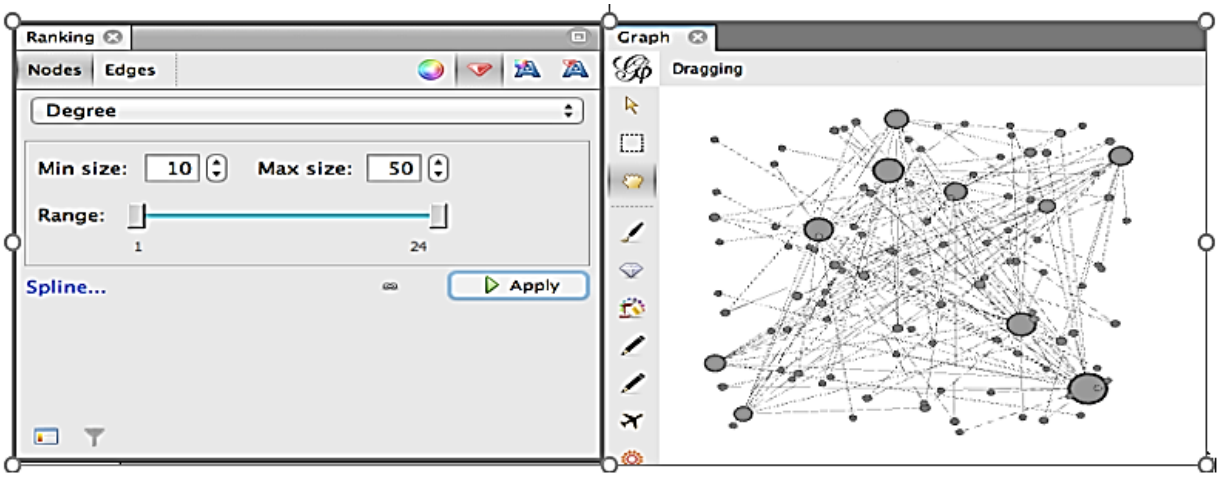

Рис. 2 – Граф онтології використання та узгодженої циркуляції даних системи роботи андеррайтингу страхової організації.

Математичну модель процесів страхової організації, яка дозволила андеррайтеру враховувати та порівнювати тарифні ставки страхових компаній із середньо ринковою ставкою по сегменту ринку, а потім змінювати їх ставки з урахуванням інтенсивності конкуренції та конкурентного ефекту поточного періоду, було використано для розробки автономного інтелектуального модуля автоматизації процесів андеррайтингу страхової організації.

Процес тестування синтезу параметрів та конструктивних змін у системі роботи андеррайтингу, реалізованих в розробленій інформаційній технології , показала адекватність та коректність розрахунків тарифної ставки під час експериментальних досліджень. Результати комп'ютерної симуляції роботи автономного інтелектуального модуля андеррайтингу страхової організації показали позитивний вплив на її фінансовий стан за рахунок вдосконалення точного вибору величини навантаження тарифної ставки та можливостей коригування кількісних і якісних показників за допомогою прогнозного рівня циклу андеррайтингу.

Експериментальні прогони моделей підтверджують ефективність розробленого програмного модуля системи автономного інтелектуального андеррайтингу базової для досліджень страхової організації.

Список посилань

1. Прагья Сінгх, Педро Кустодіо, Томаш Собчак, Блог Findability, Building a chatbot – that actually works, 2020, [Електронний ресурс]. – Режим доступу: https://findwise.com/blog/category/findability/

2. Павленко П.М. Управління ефективністю промислового виробництва / П.М. Павленко // Стратегія соціально-економічного розвитку України: зб. наук. пр. / заг. ред. Степанова О.П. – К.: КНУКіМ, 2015. – Ч. 2. – С. 81–98.

УДК 651.012.12

Кондратюк С.С., аспірант
Державний торговельно-економічний університет, м. Київ

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Все більше компаній переходять на електронний документообіг, особливо в умовах воєнного часу.

Оскільки документи несуть в собі в тому числі і комерційну цінність, то захист документів зараз актуальний як ніколи. Якщо говорити про паперові примірники, то захистити документи практично неможливо.

Проте і для електронних документів є вимоги щодо безпеки.. Зокрема, безпека електронних документів залежить від того, на якій платформі в організації реалізовано електронний документообіг.

Існує декілька факторів, на які слід звертати увагу при реалізації системи для електронного документообігу.

1. Резервне копіювання. Система електронного документообігу повинна володіти інструментом для створення резервних копій інформації. Має бути передбачена можливість як зберігання резервних копій всередині системи, так і можливість вивантаження резервних копій на з'ємний носій або у хмарне сховище з можливістю зберігати такі копії у кількох дата центрах. Оскільки резервна копія передбачає вивантаження усієї інформації в системі разом з усіма налаштуваннями, то не завжди в цьому може виникати необхідність. Тому в системі для електронного документообігу має бути передбачена можливість створення архівів електронних документів з подальшим їх вивантаженням. Документам, що зберігаються на локальних комп'ютерах загрожує потенційно більша небезпека, ніж документам, що зберігаються в централізованих захищених сховищах, в тому числі хмарних сховищах з використанням брандмауерів та інших інструментів кібербезпеки, що дозволяють уникнути злому інформації, наприклад, таких як Microsoft Azure чи GigaCloud. Часто такі інструменти бекапів застосовуються у хмарних рішеннях для реалізації електронного документообігу.

2. Контроль доступу до документів. В системах для електронного документообігу має бути передбачено розмежування прав доступу до документів. Тобто, наприклад, працівник, який відповідає за внесення у програму даних про надходження товару від постачальників, не повинен мати доступу до розрахунку зарплат чи форм бухгалтерської звітності. Тому розмежування доступу до функціонала дозволяє розподілити ролі співробітників відповідно до їхніх посадових обов'язків і забезпечити конфіденційність інформації в системі. Окрім того, кожен користувач системи повинен пройти процедуру автентифікації. Це може бути реалізовано введенням паролю до свого облікового запису, використанням токену, або може бути застосована і багатоетапна автентифікація.

3. Використання кваліфікованого електронного підпису. Використання КЕП в системі для електронного документообігу забезпечить достовірність та конфіденційність інформації. Зрозуміти, що документ є дійсним і що саме цей документ підписувався конкретною відповідальною особою допоможе саме електронний підпис. Конфіденційність інформації при обміні електронними документами забезпечується їх шифруванням за допомогою криптографічного алгоритму, затвердженого державою (ДСТУ ГОСТ 28147:2009). Формат зашифрованих повідомлень повинен відповідати вимогам наказу Державної служби спеціального зв'язку та захисту інформації № 739 від 18.12.2012 р. У відповідності до даного наказу для шифрування інформації використовується свій окремий сертифікат відкритого ключа шифрування, який не використовується для накладання електронного підпису. Використання КЕП має надважливе значення саме в системах для зовнішнього електронного документообігу, тобто при обміні документами між контрагентами, проте варто подбати про такий спосіб аутентифікації в тому числі і при реалізації внутрішньої системи обміну документами, наприклад, при візуванні документів за допомогою електронного підпису всередині підприємства.

4. Захист визнаний на державному рівні. Ознакою технічно захищеної системи електронного документообігу є відповідний документ, визнаний на державному рівні Державною службою спеціального зв'язку та захисту інформації. Ця інформація має бути відображена у експертному висновку. Вважається, що якщо система відповідає національним стандартам Г-2, то її можна вважати надійною, хоча найвищим рівнем захисту програмного забезпечення, визнаним на державному рівні вважається рівень гарантій Г-3. Такий рівень безпеки означатиме, що система електронного документообігу

працює виключно по надійним каналам зв'язку SSL, з використанням міжнародних та національних електронних підписів для підтвердження авторства від підміни та захисту модулів програмного продукту, без підвищених привілеїв щодо використання прав користувачів операційної системи, зі схваленням від Microsoft, вираженим у Windows 10 Ready. Критерієм довіри до системи електронного документообігу в контексті безпеки може бути і документ від спеціалізованої компанії, що займається тестуванням програмного забезпечення на предмет злому, так звані «білі капелюхи». Вони проводять penetration test – спробу злому системи за різноманітними сценаріями хакерських атак. Якщо система може показати документ про успішне проходження такого тесту, то цей продукт вартий уваги.

Реалізація зазначених у статті інструментів захисту інформації в системах електронного документообігу зробить систему повноцінною та захищеною при роботі з електронними документами. Якщо хоча б один з цих інструментів не буде застосований в системі, то це знизить рівень довіри до програмного продукту.

Список посилань

1. Выбор системы электронного документооборота [Електронний ресурс]. – Режим доступу: https://fossdoc/vybor-sed
2. Свистунов В. Методика выбора оптимальной СЭД - наш опыт [Електронний ресурс]. – Режим доступу: http://itdirector.org.ua/