УДК 004+655.5+621.391

ОСНОВИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ РЕДАКЦІЙНО-ВИДАВНИЧИХ БІЗНЕС-ПРОЦЕСІВ

Р. О. Козак[1], Н. В. Загородна[1], В. М. Сеньківський[2]

[1]Тернопільський національний технічний університет імені Івана Пулюя, вул. Руська, 56, Тернопіль, 46001, Україна

[2]Українська академія друкарства, вул. Під Голоском, 19, Львів, 79020, Україна

Актуалізовано проблему захисту інформації в редакційно-видавничих процесах. Розглянуто методологічні основи побудови та впровадження системи управління інформаційною безпекою видавничої діяльності. Ґрунтуючись на міжнародних стандартах і практиках, запропоновано ключові етапи створення системи управління інформаційною безпекою видавничих бізнес-процесів.

Ключові слова: *мультимедійне видання, інформаційна безпека, система управління інформаційною безпекою, захист даних, безпека редакційно-видавничих процесів.*

Постановка проблеми. Розвиток інформаційних технологій привніс суттєві зміни в процеси створення і розповсюдження видань. Зокрема стало можливим залучення до процесу створення інформаційного продукту, крім фахівців, широкого кола людей, а видання може бути створене, передане та відтворене практично на будь-якій програмно-апаратній платформі. «Відсторонення» через цифрових посередників створює нову комунікативну ситуацію у редакційно-видавничій справі, змінює форми її функціонування.

Стрімкі технологічні трансформації у видавничих бізнес-процесах неминуче призводять до виникнення нових ризиків, серед яких на перший план виходять ризики інформаційної безпеки (ІБ). Витік персональних даних працівників організації, зараження шкідливим програмним забезпеченням корпоративних систем, втручання в роботу автоматизованих систем управління технологічними процесами — аж ніяк не повна і сьогодні добре відома низка проблем, яка не лише може завдати удару по іміджу видавництва та спричинити фінансові збитки, а й викликати інтерес відомств та служб, що регулюють ці питання. У видавничій справі проблематика постає особливо гостро, оскільки видання, в тій чи іншій його формі, є виробничим ресурсом. Тому йдеться не лише про захист конфіденційної інформації, що циркулює в редакції, а про ІБ видання (мультимедійного видання) на усіх стадіях його життєвого циклу.

Досвід свідчить, що заходи і засоби захисту виявляються більш ефективними та економічно доцільними, якщо вони інтегровані у технологічні процеси чи сервіси

на стадіях вивчення вимог і проектування. Чим раніше організація впровадить заходи щодо захисту своїх інформаційних систем (продуктів), тим дешевшими та ефективнішими вони згодом будуть для неї.

Управління інформаційною безпекою набуває все більшого значення у міру прагнення видавничого бізнесу до зростання і просування продукції на нові ринки, використовуючи нові технології: користувачам важливо знати, що дотримується конфіденційність їх персональних і ділових даних; інвесторам необхідна впевненість у захищеності інформаційних активів; користувачі очікують, що сервіси (наприклад, онлайн видання) будуть функціонувати без збоїв, які можуть бути викликані помилками в роботі інформаційних систем, навмисними або ненавмисними діями персоналу, шкідливим програмним забезпеченням чи іншими факторами.

Зазвичай головними перешкодами на шляху забезпечення інформаційної безпеки є її невисока пріоритетність під час розподілу ресурсів і бюджетні обмеження. Компанії нерідко виділяють єдиний бюджет на задоволення всіх потреб з інформаційних систем (апаратне і програмне забезпечення, зарплата, консультанти), що сприяє розвитку тенденції виділяти основну частину коштів на підвищення продуктивності. За такої умови нерідко питання інформаційної безпеки залишаються без належної уваги.

Вибіркова і безсистемна реалізація засобів безпеки не зможе забезпечити необхідного рівня захисту. Тому для захисту чутливої інформації в процесах створення, представлення та дистрибуції видань необхідно інтегрувати питання фізичної та інформаційної безпеки в єдиний для всієї організації процес — процес управління інформаційною безпекою підприємства. Отже, розроблення та впровадження системи управління інформаційною безпекою (СУІБ) редакційно-видавничої діяльності є актуальною проблемою.

Аналіз останніх досліджень та публікацій. Міжнародні організації та інститути, що спеціалізуються у вирішенні комплексних проблем інформаційної безпеки, запропонували концепції проведення аудиту та управління інформаційними ризиками у вигляді міжнародних та національних стандартів: ISO 15408, ISO 270xx, COBIT, PCI DSS, SAC, COSO та ін. [1, 2]. Зокрема сімейство стандартів ISO 27000 продовжує активно розвиватися та містить стандарти, що визначають вимоги до СУІБ, систему управління ризиками, метрики і вимірювання ефективності механізмів контролю, а також інструкції щодо впровадження. (В Україні прийнята серія міжнародних стандартів управління інформаційною безпекою ДСТУ ISO/IEC 27000:2015).

Стандарт визначає інформаційну безпеку як «збереження конфіденційності, цілісності та доступності інформації; крім того, можуть бути включені й інші властивості, такі як автентичність, неможливість відмови від авторства, достовірність».

Конфіденційність — забезпечення доступу до інформації тільки для тих, хто має відповідні повноваження (авторизовані користувачі). Цілісність — забезпечення точності і повноти інформації, а також методів її опрацювання. Доступність — забезпечення доступу до інформації авторизованим користувачам, коли це необхідно (на вимогу) [3].

Стандарт є робочим інструментом для впровадження СУІБ в організації, а також для проведення аудиту з підтвердження того, що засоби управління безпеки функціонують відповідно до вимог стандарту. Стандарт описує СУІБ як всеохоплюючу систему менеджменту, побудовану на принципах бізнес-ризиків, для впровадження, експлуатації, моніторингу та підтримки системи менеджменту безпеки [4].

Згідно з ISO 27001, система управління інформаційною безпекою — це «та частина загальної системи управління організації, заснованої на оцінці бізнес-ризиків, яка створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід і вдосконалення інформаційної безпеки». Система управління містить структуру організації, політики, планування, посадові обов'язки, практики, процедури, процеси і ресурси. Створення та експлуатація СУІБ вимагає застосування такого ж підходу, як і будь-яка інша система управління.

Варто окремо вказати на стратегічні переваги, які може отримати видавничий бізнес від сертифікації згідно із стандартом ISO 27001 [5]:

- побудова надійної структури інформаційної безпеки;
- захист даних та інтелектуальної власності;
- створення нових можливостей (наприклад, співпраця з фінансовими компаніями);
- підвищення лояльності клієнтів;
- уникнення фінансових і репутаційних втрат, пов'язаних з дискредитацією даних;
- зростання довіри інвесторів;
- запобігання кібератакам і витоку даних;
- отримання конкурентної переваги на ринку.

Використовувана в ISO 27001 для опису СУІБ процесна модель передбачає безперервний цикл заходів PDCA (Plan-Do-Check-Act): планування, виконання, перевірка, вплив (управління, коригування) [6], відомий як цикл Шухарта-Демінга (рис. 1, табл. 1).

Рис. 1. Модель PDCA для впровадження СУІБ

Таблиця 1

Опис циклу PDCA для впровадження СУІБ

PDCA	Опис
Планування	Розроблення політики безпеки, визначення мети, процесів та процедур, пов'язаних з управлінням ризиками та підвищенням інформаційної безпеки для досягнення результатів відповідно до загальної політики та цілей організації
Виконання	Впровадження та використання політики безпеки, елементів керування, процесів та процедур, механізмів контролю
Перевірка	Оцінювання та вимірювання ефективності роботи відповідно до політики безпеки, цілей та практичного досвіду, а також підготовка звіту про результати для керівництва з метою подальшого аналізу й аудиту
Вплив (управління, коригування)	Застосування коригувальних та профілактичних заходів з метою досягнення постійного вдосконалення СУІБ на основі результатів аналізу; перегляд політики безпеки; підвищення поінформованості персоналу

Мета статті. Аналіз відкритих публікацій вказує на те, що проблема захисту даних, зокрема, в мультимедійних виданнях та в мультимедіа загалом, є добре висвітленою та теоретично обґрунтованою [7–9]. Однак актуальним залишається питання ефективності та економічної доцільності застосування того чи іншого засобу захисту для інформаційного продукту. Адже очевидно, що управління інформаційною безпекою у окремій інформаційній системі підприємства повинно здійснюватися у контексті його діяльності: з урахуванням технології виробництва, специфіки ринків збуту, а також фактичної ситуації, що складається в ринковій конкурентній боротьбі, державній політиці, розвитку правової системи, рівня розвитку окремих використовуваних інформаційних та телекомунікаційних технологій.

Тому, з огляду на тенденції стрімкого розвитку ІТ та одночасного з цим безсистемного реагування на існуючі загрози, видається доцільним адаптувати існуючі та розробити нові концептуальні засади побудови системи управління інформаційною безпекою видавничої діяльності. Для створення методологічної бази варто опиратися на аналіз рекомендацій міжнародних стандартів, врахування особливостей редакційно-видавничих процесів, форм представлення видання, розподіленої архітектури мережі збуту та маркетингу, інтерактивної природи мультимедійного видання. При правильному використанні система має забезпечити ефективне управління і захист цінних даних, активів видавництва та авторських прав, дати змогу мінімізувати ризики і надати клієнтам і зацікавленим сторонам впевненість у тому, що компанія управляє цими ризиками.

Виклад основного матеріалу дослідження. Побудова системи управління інформаційною безпекою — це комплексний процес, направлений на мінімізацію зовнішніх і внутрішніх загроз із врахуванням обмежень на ресурси і час. Для побудови ефективної системи інформаційної безпеки необхідно спочатку описати процеси діяльності, потім визначити поріг ризику, тобто рівень загрози, при якому вона потрапляє в процес управління ризиками. Отже, потрібно побудувати таку систему інформаційної безпеки, яка забезпечить досягнення заданого рівня ризику.

Зважаючи на сукупність видавничих бізнес-процесів [10], специфіку інформаційного продукту — переважно мультимедійного видання, — з методологічного погляду [11] створення СУІБ може бути реалізовано в такі шість етапів (рис. 2), а з позиції процесного підходу систему інформаційної безпеки можна представити як процес управління ризиками (рис. 3), — як ключового етапу управління ІБ.

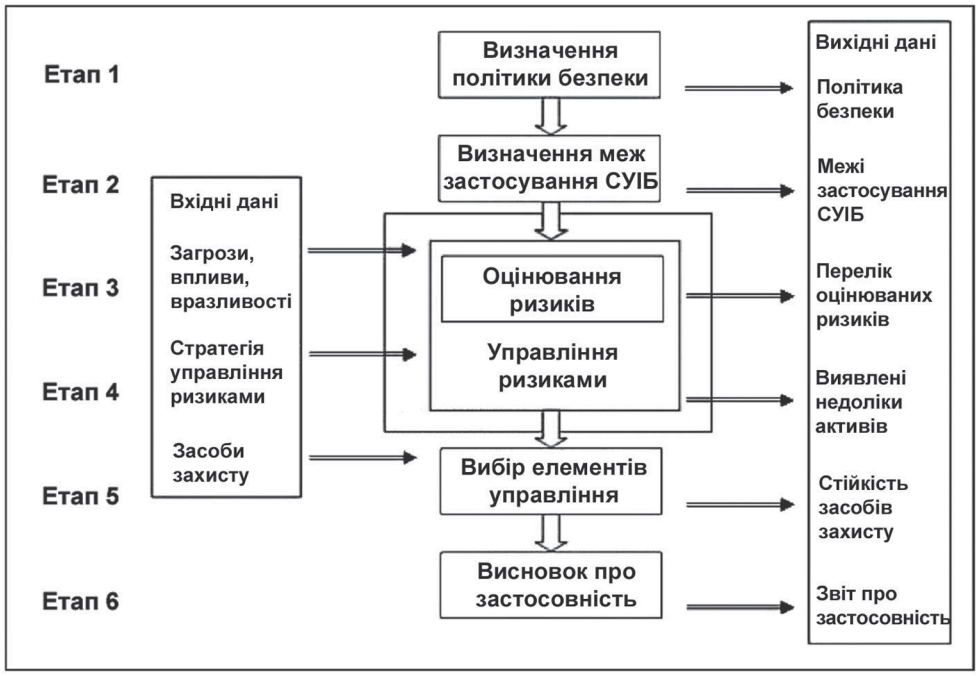

Рис. 2. Етапи процесу створення СУІБ

Етапи 3 і 4 утворюють основу СУІБ видавництва і є процесами, які трансформують принципи політики безпеки організації, а також перетворюють цілі СУІБ в конкретні плани щодо впровадження механізмів керування і захисту, спрямованих на мінімізацію загроз і вразливостей.

Процедури та дії на етапах 5 та 6 не стосуються інформаційних ризиків. Вони радше пов'язані з оперативними діями, необхідними для технічної реалізації, обслуговування і управління, оцінюванням рівня безпеки. Відповідні засоби контролю можна отримати з існуючих наборів засобів чи механізмів, які зазвичай містяться в стандартах та керівних положеннях інформаційної безпеки,

або як результат поєднання чи адаптації пропонованих засобів до конкретних вимог організації та експлуатаційних характеристик. В обох випадках етап 6 є задокументованим відображенням виявлених ризиків в умовах конкретного редакційно-видавничого процесу, що містить технічну реалізацію механізмів безпеки, які планують застосувати. Незважаючи на те, що УІБ є циклічним процесом, у більшості компаніях етапи 1 та 2 повторюватимуться рідше, ніж етапи 3, 4, 5 та 6. Це пов'язано з тим, що створення політики безпеки та визначення меж СУІБ є управлінськими та стратегічними питаннями, тоді як процес управління ризиками — це щоденна операційна проблема.

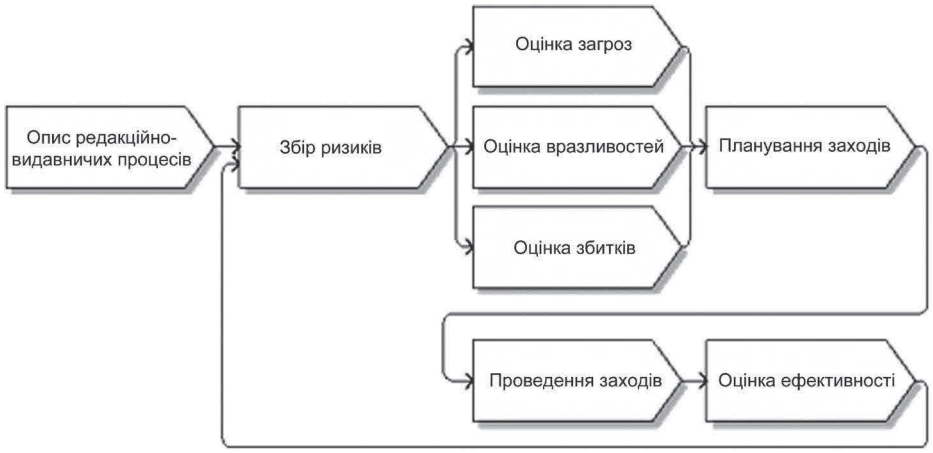

Рис. 3. Модель системи управління ризиками для СУІБ

Аналіз моделі управління ризиками потребує розгляду в рамках узагальненої моделі системи інформаційної безпеки видавництва, із розкриттям таких понять як об'єкт захисту, види і модель загроз, модель порушника, а тому буде висвітлено в подальших дослідженнях.

Висновки. Застосування засобів захисту інформації в редакційно-видавничих процесах є ситуативним і, зазвичай, безпека мультимедійного продукту забезпечується сучасними і дорогими рішеннями, проте не є комплексною. Запровадження системи управління інформаційною безпекою у видавничу діяльність має низку переваг, ключовою з яких виступає стійкість (неперервність) бізнесу перед новими загрозами, пов'язаними із прогресом в ІТ. У роботі запропоновано концептуальні засади побудови СУІБ на основі міжнародних практик із врахуванням специфіки видавничих бізнес-процесів. Власне питання управління інформаційною безпекою, яке традиційно розглядається в структурі управління всією компанією, є циклічним процесом, що включає усвідомлення керівництвом необхідності захисту інформації, аналіз стану інформаційної безпеки в організації; оцінку інформаційних ризиків, впровадження відповідних механізмів контролю, моніторинг функціонування механізмів захисту, та ін., в умовах видавничої галузі потребує нових досліджень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27000 family — Information security management systems [Electronic resource]. URL: https://www.iso.org/isoiec-27001-information-security.html.
2. ДСТУ ISO/IEC 27000:2015 (ISO/IEC 27000:2014, IDT) Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник [Електронний ресурс]. URL: http://document.ua/informaciini-tehnologiyi_-metodi-zahistu_-sistema-upravlinnj-std32008.html.
3. Домарев В. В. Безопасность информационных технологий. Системный подход. Киев: Издательство «Диасофт», 2004. 992 с.
4. Шахалов И. Ю., Дорофеев А. В. Основы управления информационной безопасностью современной организации [Електронний ресурс]. URL: https://cyberleninka.ru/article/n/osnovy-upravleniya-informatsionnoy-bezopasnostyu-sovremennoy-organizatsii.
5. Cheol Soon Park. A Study of Effect of Information Security Management System [ISMS] Certification on Organization Performance. [Electronic resource]. URL: http://paper.ijcsns.org/07_book/201003/20100303.pdf.
6. Calder A. Implementing Information Security based on ISO 27001/ISO 27002. A Management Guide. Van Haren, 2011. P. 90.
7. Zhaopin Su, Guofu Zhang and Jianguo Jiang. Multimedia Security: A Survey of Chaos-Based Encryption Technology [Electronic resource]. URL: https://www.intechopen.com/ books/multimedia-a-multidisciplinary-approach-to-complex-issues/multimedia-security-a-survey-of-chaos-based-encryption-technology.
8. Furht B., Kirovski D. Multimedia Security Handbook. CRC Press, 2004, 832 pp.
9. Multimedia Security: Open Problems and Solutions. Voloshynovskiy S. etc. [Electronic resource]. URL: http://citeseerx.ist.psu.edu/viewdoc/download? doi=10.1.1.71.1389&rep=rep1&type=pdf.
10. Белоусова Н. М. Бизнес-процессы в издательской деятельности и их классификация [Електронний ресурс]. URL: https://cyberleninka.ru/search?q=% D0%91%D0%B5%D0%BB%D0%BE%D1%83%D1%81%D0%BE%D0%B2%D0%B0%20%D0%9D.%D0%9C.
11. M. Gheorghe de Studii, Boldeanu A., Bucureti D. Economice. Information security management system, 2017.

REFERENCES

1. ISO/IEC 27000 family — Information security management systems. Retrieved from https://www.iso.org/isoiec-27001-information-security.html (in English).
2. DSTU ISO/IEC 27000:2015 (ISO/IEC 27000:2014, IDT) Informatsiini tekhnolohii. Metody zakhystu. Systema upravlinnia informatsiinoiu bezpekoiu. Ohliad i slovnyk. Retrieved from http://document.ua/informaciini-tehnologiyi_-metodi-zahistu_-sistema-upravlinnj-std32008.html. (in Ukrainian).
3. Domarev, V. V. (2004). Bezopasnost informatcionnykh tekhnologii. Sistemnyi podkhod. Kiev: Izdatelstvo «Diasoft» (in Russian).
4. Shakhalov, I. Iu., & Dorofeev, A. V. Osnovy upravleniia informatcionnoi bezopasnostiu sovremennoi organizatcii. Retrieved from https://cyberleninka.ru/article/n/osnovy-upravleniya-informatsionnoy-bezopasnostyu-sovremennoy-organizatsii (in Russian).

5. Cheol Soon Park. A Study of Effect of Information Security Management System [ISMS] Certification on Organization Performance. Retrieved from http://paper.ijcsns.org/07_book/201003/20100303.pdf (in English).
6. Calder, A. (2011). Implementing Information Security based on ISO 27001/ISO 27002. A Management Guide. Van Haren (in English).
7. Zhaopin, Su, Guofu, Zhang, & Jianguo, Jiang. Multimedia Security: A Survey of Chaos-Based Encryption Technology. Retrieved from https://www.intechopen.com/ books/multimedia-a-multidisciplinary-approach-to-complex-issues/multimedia-security-a-survey-of-chaos-based-encryption-technology (in English).
8. Furht, B., & Kirovski, D. (2004). Multimedia Security Handbook. CRC Press (in English).
9. Voloshynovskiy, S., Koval, O., & Deguillaume, F., Pun, T. Multimedia Security: Open Problems and Solutions. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download? doi=10.1.1.71.1389&rep=rep1&type=pdf. (in English).
10. Belousova, N. M. Biznes-protcessy v izdatelskoi deiatelnosti i ikh klassifikatciia. Retrieved from https://cyberleninka.ru/search?q=% D0%91%D0%B5%D0%BB%D0%BE%D1%83%D1%81%D0%BE%D0%B2%D0%B0%20%D0%9D.%D0%9C. (in Russian).
11. M. Gheorghe de Studii, Boldeanu, A., & Bucureti, D. (2017). Economice. Information security management system (in English).

BASES OF INFORMATION SECURITY MANAGEMENT IN THE EDITORIAL AND PUBLISHING BUSINESS PROCESSES

R. O. Kozak[1], N. V. Zahorodna[1], V. M. Senkivskiy[2]

[1]Ternopil Ivan Puluj National Technical University,
56, Ruska St., Ternopil, 46001, Ukraine

[2]Ukrainian Academy of Printing,
19, Pid Holoskom St., Lviv, 79020, Ukraine
ruslan.o.kozak@gmail.com

The problem of information security in the editorial and publishing processes has been actualized. The methodological foundations of the construction and implementation of the information security management system for publishing activities have been considered. Based on international standards and practices, key steps in the development of information security management system for publishing business processes have been suggested.

Keywords: *multimedia publication, information security, information security management system, data protection, security of editorial and publishing processes.*

Стаття надійшла до редакції 20.02.2017.
Received 20.02.2017.