„Studia Archiwalne", t. 9, 2022
ISSN 1734-7513

Michał Zawada
(Archiwum Państwowe w Lublinie)

Wrażliwość informacyjna i bezpieczeństwo informacji w działalności archiwalnej

ZARYS TREŚCI: Bezpieczeństwo informacji przenika niemal wszystkie aspekty działalności archiwalnej. Zapewnienie poufności, integralności i dostępności informacji, dla których źródłem są materiały archiwalne, realizowane jest na poziomie regulacji prawnych i techniczno-organizacyjnych już na etapie ich wytwarzania w jednostkach objętych nadzorem archiwalnym. Bezpieczeństwo informacji zaczyna się jednak jeszcze wcześniej, na poziomie pojedynczego pracownika (urzędnika, archiwisty), który realizuje wspomniane regulacje. Wrażliwość informacyjna, czyli troska o wytwarzanie kompletnych, czytelnych, zrozumiałych, a przede wszystkim prawdziwych informacji, to kompetencja, która jest niezbędna urzędnikom i archiwistom w procesie ich tworzenia.

SŁOWA KLUCZOWE: bezpieczeństwo informacji, poufność, integralność, dostępność, kostka McCumbera.

ABSTRACT: Information security permeats almost every aspect of archival activities. In order to guarantee confidentiality, integrity and availability of information stored in archival materials, legal, technical and organizational regulations are executed from the very first stage of their creation in organizational entities under archival supervision. However, information security begins at even earlier stage, at the level of single worker (clerk, archivist), who fulfills all those regulation mentioned above. Informational sensitivity, which is care about creating complete, readable, intelligible, and most of all true information, de-

picts a personal competence that is essential for clerks and archivists in process of its creation.

KEYWORDS: information security, confidentiality, integrity, availability, McCumber cube.

Wstęp

Archiwa, bez względu na swoją genezę i rodzaj przechowywanych w nich zbiorów (państwowe, społeczne, rodzinne, prywatne), mają u podstaw swego istnienia zapewnienie bezpieczeństwa zgromadzonych w nich informacji. Niemalże wszystkie działania na archiwaliach, począwszy od ich zgromadzenia i opisania, poprzez różnego rodzaju systemy ewidencji i opracowania, na przechowywaniu oraz korzystaniu z nich skończywszy, mają za swój motyw bezpieczeństwo informacji. Malowanie go jako tło dla szerokiej działalności archiwalnej wydaje się być na pierwszy rzut oka nieco przesadzone, zwłaszcza jeżeli bezpieczeństwo informacji utożsamia się z ich poufnością lub, szerzej, ograniczeniem dostępu do nich[1]. Warto zatem na początku precyzyjnie określić, czym jest bezpieczeństwo informacji, gdyż jego zakres bezpośrednio wpływa na to, co jest przedmiotem niniejszego artykułu, czyli na wrażliwość informacyjną.

> Bezpieczeństwo informacji to stan i proces, w ramach którego zapewnia się w całym cyklu życia informacji (powstanie, przekazanie, przetworzenie, kopiowanie, wykorzystywanie, przechowywanie, gromadzenie, niszczenie) osiąganie i utrzymywanie z uwzględnieniem obowiązujących standardów bezpieczeństwa na pożądanym przez dany podmiot poziomie takich jej fundamentalnych właściwości, jak: dostępność, użyteczność, integralność i poufność[2].

Z przywołanych wyżej właściwości informacji poufność wydaje się być na pierwszym miejscu, gdy myślimy o bezpieczeństwie informacji w archiwach, jednakże po bardziej wnikliwym zastanowieniu się nad informacją samą w sobie, pozostałe jej właściwości, tj. integralność i poufność, grają równorzędne role. Mówiąc o integralności należy mieć tu na uwadze to, iż „informacje integralne to takie,

[1] Por. W. Fehler, *O pojęciu bezpieczeństwa informacyjnego*, [w:] *Bezpieczeństwo informacyjne w XXI wieku*, red. M. Kubiak, S. Topolewski, Siedlce–Warszawa 2016, s. 26–28.

[2] Ibidem. s. 30.

które poprawnie oddają istotę danego stanu rzeczy oraz nie zostały naruszone w drodze od wytwórcy (źródła) do odbiorcy – to informacje, które nie zostały poddane manipulacji"[3]. Świadomie pomijam tutaj użyteczność informacji, jako że wychodzę z milczącego założenia, iż w archiwach przechowuje się tylko te archiwalia, które zostały uprzednio zakwalifikowane w taki czy inny sposób jako zawierające użyteczne dla kogoś informacje. Założenie to zostało nadbudowane na rozumianej „archiwistycznie" infologicznej teorii informacji, zgodnie z którą „informacją są takie komunikaty lub kombinacje komunikatów, które umożliwiają ich rzeczywistym lub potencjalnym odbiorcom (użytkownikom informacji), zaspokojenie potrzeb informacyjnych, tzn. zmniejszenie stopnia niewiedzy o danym zjawisku (stopień nieokreśloności), pozwalając tym samym na polepszenie znajomości otoczenia i sprawniejsze przeprowadzenie celowych działań"[4]. Zaspokojenie potrzeb informacyjnych jest motywem przewodnim tworzenia i zachowywania wytworzonej informacji w ogóle, bez względu na to, czy informacja ta wykorzystywana jest w bieżącej działalności czy też ponownie użytkowana w dalszej przyszłości jako informacja archiwalna. To tutaj, w zaspokojeniu potrzeb informacyjnych, ujawnia się najsilniej konieczność uwzględniania integralności i dostępności informacji jako właściwości równie istotnych jak poufność. Co więcej, „pewne informacje spożytkowujemy na bieżąco, w innych zaś dostrzegamy cechy, które mogą uczynić je użytecznymi dopiero w jakiejś perspektywie czasowej"[5]. Ta potencjalnie rosnąca wartość informacji w czasie sprawia, że niszczenie informacji nieużytecznej z teraźniejszego punktu widzenia (np. brakowanie dokumentacji niearchiwalnej) musi przewidywać, na ile jest to możliwe, przyszłe zapotrzebowanie na tę informację. Nie jest to jednak temat niniejszego artykułu, zatem pozwolę sobie pozostawić powyższą myśl w pewnym zawieszeniu.

Bezpieczeństwo informacji w archiwach państwowych

Zarysowana we wstępie koncepcja bezpieczeństwa informacji, czyli zapewnienie w całym cyklu jej życia nienaruszonych właściwości poufności, integralności i dostępności, odciska się jak pełna detali pieczęć na laku ustawowej działalno-

[3] Ibidem, s. 31–32.

[4] M. Cieślarczyk, *Psychospołeczne i prakseologiczne aspekty bezpieczeństwa informacyjnego,* [w:] *Bezpieczeństwo informacyjne w XXI wieku*, red. M. Kubiak, S. Topolewski, Siedlce–Warszawa 2016, s. 52.

[5] W. Fehler, op. cit., s. 30.

ści archiwalnej archiwów państwowych. Jako przykład realizacji przez archiwa państwowe bezpieczeństwa informacji na poziomie prawnym można podać następujące zapisy ustawy archiwalnej[6]:

a) poufność, czyli ograniczenie dostępu do informacji wyłącznie do kręgu osób uprawnionych, reguluje art. 16b ust. 1 unza[7], wskazując na zasady prawnego ograniczenia dostępu do informacji ze względu na ich charakter (informacje niejawne, dane osobowe), ochronę dóbr osobistych lub bezpieczeństwo zasobu archiwalnego;
b) integralność, czyli zapewnienie kompletności informacji zawartych w materiałach archiwalnych, opisuje m. in. art. 12 i 12a unza[8], w którym na aktotwórców i przechowawców nałożone zostały obowiązki zapewnienia należytego przechowywania materiałów archiwalnych, ochrony przed zniszczeniem oraz poddania niezbędnej konserwacji. Ponadto, art. 52, 53 i 54 unza[9] wskazują na konsekwencje prawne uszkodzenia, zniszczenia, wywozu lub innej formy „defragmentacji" materiałów archiwalnych;
c) dostępność, rozumiana jako dostęp do informacji, dla których źródłem są archiwalia, została ogólnie opisana w art. 2 ust. 1[10] oraz art. 16a ust. 1 unza[11]. Zaznaczono tam, iż materiały archiwalne są dostępne dla każdego, a sam zasób służy celom naukowym, kulturalnym, gospodarczym oraz potrzebom obywateli.

Powyższe przykłady, które rzecz jasna nie tworzą listy zamkniętej, nie tylko obrazują podejście archiwów do bezpieczeństwa informacji zawartych w narodowym zasobie archiwalnym, ale także wskazują na wzajemne powiązanie właściwości informacji, inaczej mówiąc, na ich swoistą nierozłączność. Tak oto dostępność informacji (art. 2 ust. 1 i art. 16a ust. 1 unza) może być ograniczona zachowaniem jej poufności (art. 16b ust. 1 unza) lub naruszeniem jej integralności (art. 52 ust. 1, art. 53 ust. 1, art. 54 ust. 1 unza).

Poziom techniczno-organizacyjny bezpieczeństwa informacji w archiwach państwowych, stanowiący praktyczną realizację przepisów prawnych, obfituje

---

[6] Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (tekst jedn. Dz. U. z 2020 r., poz. 164), dalej: unza.

[7] Zob. M. Konstankiewicz, A. Niewęgłowski, *Narodowy zasób archiwalny i archiwa. Komentarz*, Warszawa 2016, s. 224–232 (dalej: Komentarz).

[8] Ibidem, s. 157–163.

[9] Ibidem, s. 677–690.

[10] Ibidem, s. 36–37.

[11] Ibidem. s. 217-218.

w przykłady rozwiązań, które jeszcze bardziej uświadamiają ważność wszystkich wspomnianych właściwości informacji. Jako przykłady takich rozwiązań można podać:

a) poufność
   - uprawnienia pracowników do dostępu, np. do magazynów archiwalnych,
   - poziomy uprawnień dostępu do systemu EZD, ZoSIA, dedykowanych baz danych,
   - zabezpieczenia dostępu, jak np. zamykane szafy, ewidencja pobranych kluczy,
   - zabezpieczenia infrastruktury informatycznej;
b) integralność
   - system przechowywania materiałów archiwalnych w magazynach,
   - dbałość o kompletność wytwarzanej w archiwum dokumentacji,
   - dbałość o bieżącą aktualizację informacji, np. danych użytkowników;
c) dostępność
   - procedury udostępniania bezpośredniego i pośredniego materiałów archiwalnych użytkownikom,
   - digitalizacja materiałów archiwalnych oraz ich publikacja np. w serwisie szukajwarchiwach.gov.pl,
   - promocja i popularyzacja zasobu archiwalnego.

Rozwiązania techniczno-organizacyjne można jeszcze uzupełnić o różne polityki i procedury wdrożone w archiwach państwowych, których zadaniem jest zapewnienie poufności, integralności i dostępności przetwarzanych w nich informacji. Począwszy od normatywów kancelaryjnych, poprzez politykę ochrony danych osobowych, dokumentację systemu zarządzania bezpieczeństwem informacji, na wewnętrznych przepisach szczegółowych skończywszy, pamięć o zapewnieniu bezpieczeństwa informacji jest stale obecna w archiwach i kształtuje charakter pracy archiwistów.

Przytoczone do tej pory przykłady realizacji bezpieczeństwa informacji w archiwach, choć w pełni prawdziwe i skuteczne, wskazują na pewną „ukrytą" cechę niemalże wszystkich, a przynajmniej zdecydowanej części, rozwiązań prawnych i techniczno-organizacyjnych w tej dziedzinie. Cechą tą jest zastosowanie tychże rozwiązań do informacji już wytworzonej, informacji, której kształt został już nadany u, szeroko pojętego, aktotwórcy, informacji, której za-

kres, sposób przedstawienia i użyteczność zostały zdeterminowane w przeszłości. Rzec można, że w takim przypadku mamy do czynienia z zapewnieniem „wtórnego" bezpieczeństwa informacji, z zapewnieniem go już zapisanej informacji, która w trakcie tworzenia i zapisywania (bez względu na zastosowany nośnik informacji) mogła ulec zniekształceniu, niekompletności, albo, co gorsza, sfałszowaniu. Gdzie zatem tak naprawdę zaczyna się bezpieczeństwo informacji, zwłaszcza tych zawartych w materiałach archiwalnych, nad którymi nadzór sprawują archiwa państwowe?

Wrażliwość informacyjna

Archiwa państwowe sprawują czujną straż nad informacjami zawartymi w materiałach archiwalnych. Dotyczy to zarówno materiałów przechowywanych w magazynach archiwalnych po ustawowym ich przejęciu do zasobu, jak również tych materiałów, które nie zostały jeszcze przejęte, a nad którymi pieczę roztacza, używając potocznego sformułowania, nadzór archiwalny. Zbliżamy się tutaj do istoty niniejszego artykułu, czyli przywołanej w tytule wrażliwości informacyjnej. Jest ona związana z drugą ze wspomnianych wyżej sytuacji „sprawowania straży" nad informacjami zawartymi w materiałach archiwalnych, czyli tych znajdujących się w jednostkach nadzorowanych przez archiwa państwowe. Jako myśl przewodnią kolejnych rozważań, która tak na marginesie była jedną z inspiracji do powstania tego artykułu w ogóle, pozwolę sobie przytoczyć słowa profesora Roberta Degena:

> (…) archiwa aktywnie funkcjonują na tzw. przedpolu archiwalnym i kształtują zasób narastający w registraturach. Realizując swoje kompetencje w tym zakresie, archiwa państwowe kontrolują stan dokumentacji przechowywanej w archiwach zakładowych, sprawdzają poprawność wydzielania materiałów przeznaczonych do zniszczenia, wydają zgodę na ich brakowanie oraz mają możliwość ingerowania w **mechanizmy pracy biurowej**. (…) Ingerencja ta jest zrozumiała, o ile jej celem jest dążenie do **zapewnienia bezpieczeństwa materiałom archiwalnym**[12] (pogrubienia tekstu – M. Z.).

[12] R. Degen, *Kancelarie i archiwiści. Garść uwag na temat wpływu pracowników archiwów państwowych na mechanizmy pracy biurowej administracji w Polsce po 1918 roku*,

Rozwijając powyższą myśl profesor wskazuje dalej, iż ingerencja archiwistów w pracę biurową pracowników nadzorowanej instytucji może obejmować nawet początkowe etapy wszczynania i załatwiania spraw, jakimi są przyjęcie i rejestracja korespondencji wpływającej. Jest to o tyle istotne, że kultura pracy biurowej jest, mimo pewnych elementów wspólnych dla całej administracji, indywidualną cechą każdej instytucji[13].

Podkreślone przeze mnie „mechanizmy pracy biurowej" oraz „zapewnienie bezpieczeństwa materiałom archiwalnym" są tą przestrzenią działalności instytucji, a precyzyjniej mówiąc działalności każdego z pracowników owej instytucji, w której objawia się tytułowa wrażliwość informacyjna. Celem uniknięcia nieporozumień terminologicznych (wrażliwość informacyjna to nie wrażliwość informacji, czyli jej podatność na zagrożenia) pozwolę sobie zdefiniować tutaj wrażliwość informacyjną (uwaga: w kontekście informacji zapisanych w materiałach archiwalnych) jako kompetencję osoby odpowiedzialnej za proces powstania i utrwalenia informacji, dzięki której (kompetencji) osoba ta zapewnia tworzonej i utrwalanej przez siebie informacji taki poziom precyzji i kompletności, aby opisywany przez tę informację zaistniały rzeczywisty stan lub fakt mógł być jednoznacznie zrozumiany przez inne osoby. Przykładem wrażliwości informacyjnej może być spisanie notatki służbowej z rozmowy telefonicznej, w której wskazuje się na datę i godzinę rozmowy, jednoznacznie identyfikuje rozmówców oraz w kompletny, czytelny i zrozumiały sposób informuje o przedmiocie i przebiegu rozmowy.

Wskazanie w powyższej definicji wrażliwości informacyjnej etapu powstania i utrwalenia informacji nie jest przypadkowe. To w tym właśnie momencie następuje przekroczenie granicy między bezpieczeństwem informacji wytwarzanej a bezpieczeństwem informacji już wytworzonej. Chcę przez to powiedzieć, odpowiadając na pytanie z końca poprzedniej części artykułu, że bezpieczeństwo informacji, także tej zawartej w materiałach archiwalnych, rozpoczyna się w momencie jej określenia i transferu z umysłu osoby pracownika, urzędnika, kancelisty na nośnik informacji (papier, plik komputerowy, itp.). Stąd wrażliwość informacyjna jest kompetencją osoby, a nie np. cechą systemu kancelaryjnego, produktem instrukcji kancelaryjnej, bezpośrednim wynikiem przepisów prawnych czy funkcjonalnością systemu klasy EZD. To od każdego indywidu-

[w:] *Dzieje biurokracji na ziemiach polskich,* t. 2, red. A. Górak, D. Magier, Lublin–Siedlce 2009, s. 267–268.

[13] Por. ibidem.

alnego pracownika instytucji, którego obowiązkiem służbowym jest tworzenie i utrwalanie informacji niezbędnych do odzwierciedlenia toku realizacji spraw, a co za tym idzie, gromadzenie i kompletowanie dokumentacji (czyli zbioru powiązanych ze sobą informacji), zależy, czy dana sprawa zostanie jednoznacznie i zrozumiale zachowana na przyszłość. To, że dokumentacja sprawy jest kompletna nie znaczy jeszcze, że poszczególne jej dokumenty zawierają komplet informacji, które powinny się w nich znaleźć. Niejednokrotnie tylko sam prowadzący sprawę jest w stanie wskazać, czy zawarł w dokumentacji wszystkie informacje, w posiadaniu których był, gdy sprawa miała swój bieg. Ponownie pobrzmiewa tutaj echo słów profesora Degena, w których mówił o ingerencji nadzoru archiwalnego w mechanizmy pracy biurowej instytucji wytwarzających materiały archiwalne. W niniejszych rozważaniach schodzimy jednak o poziom niżej od zaznaczonego przez profesora wpływu archiwistów zajmujących się nadzorem archiwalnym na wykonywanie czynności kancelaryjnych. Docieramy do dość subtelnej i prawie nieuchwytnej chwili, w której pracownik tworzący informację, która zaraz przybierze strój dokumentu, decyduje, najpierw w swoim umyśle, a potem za pomocą klawiatury komputera, jakie informacje zawrze oraz czy będą one kompletne i prawdziwe. Jeżeli uznać, że tworzenie informacji to tak naprawdę zmniejszenie chaotyczności danych napływających z jakiegoś stanu lub faktu poprzez ich selekcję i nadanie wyselekcjonowanym danym struktury relacyjnej (powiązanie danych w logiczną i spójną całość), tworzenie informacji w umyśle pracownika ujawnia się jako złożony proces wybrania danych ważnych i odrzucenie nieistotnych. W przytoczonym wyżej przykładzie notatki służbowej zostały wybrane ważne dane (data, termin, rozmówcy, przedmiot i przebieg rozmowy), a odrzucone dane zbędne (marka telefonu, z którego wykonano połączenie, kultura rozmowy i sprawność jej przeprowadzenia, obecność w rozmowie zwrotów grzecznościowych, itp.). Dla uściślenia, ważne dane to dane użyteczne, zgodnie z rozumieniem użyteczności jako właściwości informacji przywołanej w słowach W. Fehlera z początku artykułu.

Wrażliwość informacyjna, czyli umiejętność wytworzenia informacji z dostępnych danych w sposób zapewniający kompletny (trafna selekcja), czytelny (trafne ujęcie relacyjności) i zrozumiały (jasny sposób reprezentacji danych) opis rzeczywistego stanu lub faktu (prawdziwość informacji) to, jak już zostało zaznaczone, pewna kompetencja pracownika. Zapożyczając określenie kompetencji miękkich i twardych, wrażliwość informacyjna plasuje się na ich styku, z niewielkim odchyleniem w stronę kompetencji twardych. Oznacza to, że wrażliwości informacyjnej trzeba od siebie wymagać, oraz że należy się jej nauczyć i ją

rozwijać. Dotyczy to zarówno pracowników jednostek podlegających nadzorowi archiwalnemu, jak również archiwistów, którzy mają możliwość, a nawet obowiązek, „ingerowania w mechanizmy pracy biurowej". Co więcej, dotyczy to również wszystkich pozostałych archiwistów zatrudnionych w archiwach państwowych i wszelkiego personelu archiwalnego wytwarzającego informacje, dla których źródłem są materiały archiwalne. Pracownicy nadzoru archiwalnego, choć nie tylko oni, mają tutaj szerokie pole manewru do wywierania wpływu (ingerencja to może jednak zbyt mocne słowo) na pracowników kontrolowanych jednostek i budzenie w nich świadomości tego, iż bezpieczeństwo informacji tworzących ostatecznie materiały archiwalne, które pozostaną dla przyszłych pokoleń, zaczyna się od nich samych. Sam zakres i mechanizmy wpływu archiwistów zajmujących się nadzorem archiwalnym na czynności kancelaryjne w nadzorowanych jednostkach (z naciskiem na styl wytwarzania przez ich pracowników informacji) to temat na osobny artykuł, jednakże poniżej postaram się choć skrótowo przedstawić kilka myśli w tej materii.

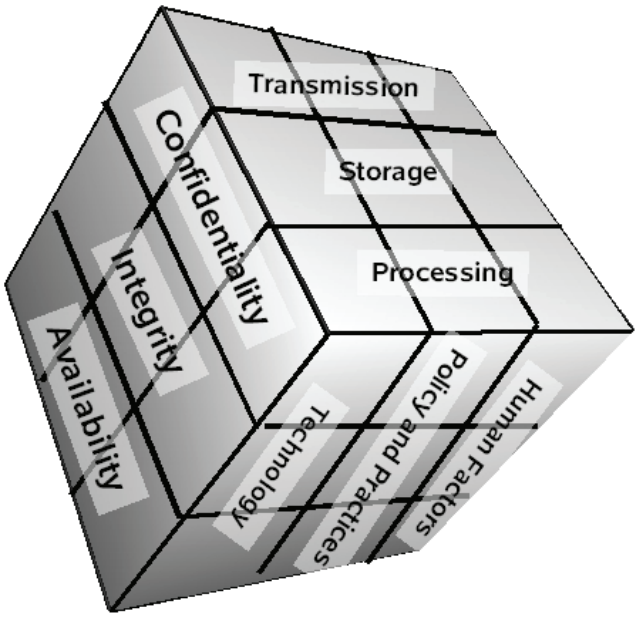
Kostka McCumbera

Wrażliwość informacyjna to fundament wytworzenia i utrwalenia informacji, które odpowiadają temu, co w rzeczywistości się zastało (stan) lub wydarzyło (fakt), czyli mówiąc krótko, informacji prawdziwych i pełnych. Chciałbym w tym miejscu poszerzyć nieco zakres wrażliwości informacyjnej oraz pochylić się nieco nad jej powiązaniem z bezpieczeństwem informacji. Celem takiego zabiegu jest pokazanie, jak założenia bezpieczeństwa realizują się już na poziomie wrażliwości. Spośród zapewne wielu modeli i ujęć umożliwiających uchwycenie ww. powiązań, została wybrana tzw. kostka McCumbera. Jest to model służący do określenia i oceny bezpieczeństwa informacji, stworzony w roku 1991 przez Johna McCumbera, amerykańskiego eksperta w dziedzinie cyberbezpieczeństwa. Model ten określa następujące obszary i elementy bezpieczeństwa informacji:

- atrybuty informacji (poufność, integralność, dostępność),
- stany informacji (transmisja, przechowywanie, przetwarzanie),
- środki bezpieczeństwa (technologia, polityka i procedury, czynniki ludzkie)[14].

[14] Por. J.R. McCumber, *Information Systems Security: A Comprehensive Model*, [in:] *14th National Computer Security Conference*, Washington D.C., 1991, s. 334.

Wybór kostki McCumbera nie jest przypadkowy, a wynika on z elastyczności tego modelu. Jak zauważył J. McCumber, „(…) jej wartość leży w zdolności adaptacji do środowiska informacji bez względu na użyte w nim konkretne technologie. Model jest z konieczności trójwymiarowy, tak aby uchwycić prawdziwą naturę współgrania elementów w systemach bezpieczeństwa informacji (tłumaczenie – M. Z.)”[15]. Ponieważ mowa o wrażliwości informacyjnej w momencie wytwarzania informacji, zastosowanie kostki McCumbera ograniczę do tego właśnie zakresu. Nie mam na celu wskazania wyczerpującej listy „dobrych praktyk”, a jedynie zaznaczenie kilku przykładów obrazujących istnienie bezpieczeństwa informacji na poziomie wrażliwości informacyjnej.



Rys. 1. Kostka McCumbera.
(źródło: <https://en.wikipedia.org/wiki/McCumber_cube#/media/File:McCumber_cube.jpg>)

[15] J. McCumber, *Assessing and Managing Security Risk in IT Systems: A Structured Methodology*, Auerbach 2005, s. 99. Tekst oryginalny: *As with all models, the value lies in its ability to adapt to the information environment irrespective of the specific technologies involved. The model is necessarily three-dimensional to capture the true nature of the interplay of the elements in information systems security.*

Poufność

Wytwarzanie informacji niejawnych wymaga szczególnej dbałości o zapewnienie braku dostępu osób nieuprawnionych do utrwalanych informacji. Poufność we wrażliwości informacyjnej nie ma wprawdzie bezpośredniego wpływu na poufność informacji jako takiej, niemniej jednak warto stosować takie praktyki, jak:

- stosowanie polityki czystego biurka i czystego ekranu, tak aby uniemożliwić osobom nieuprawnionym (współpracownikom niezwiązanym z daną sprawą) poznanie informacji niejawnej;
- zapewnienie tajności odbywanej rozmowy telefonicznej, jeśli jej treść stanowią informacje niejawne;
- niestosowanie w nazwach spraw wyrazów, które naruszają w pewnym znaczeniu poufność dokumentacji, jeżeli dostęp do nazw spraw (np. spis spraw, wyszukiwarka spraw) mogą mieć osoby postronne (dla przykładu: w systemie klasy EZD błędem jest nazwanie sprawy „Postępowanie dyscyplinarne Jan Nowak", ponieważ osoby postronne bez zaglądania do teczki sprawy wiedzą, że Jan Nowak takiemu postępowaniu podlegał; to także naruszenie ochrony danych osobowych).

Integralność

Wytwarzanie kompletnych i prawdziwych informacji jest w rozważanym kontekście sercem triady poufność – integralność – dostępność. Niekompletne albo nieprawdziwe informacje ograniczają przede wszystkim dostępność informacji, ponieważ co nie zostanie zapisane, albo co zostanie zapisane błędnie, już takie zostanie, o ile nie przejdzie kontroli. Nie można mieć dostępu do czegoś, co nie istnieje, stąd nacisk należy położyć ponownie na umiejętność przesiewania napływających danych, tak aby wybrać z nich informacje ważne, tj. użyteczne. Mogą w tym pomóc:

- zapisywanie informacji niezwłocznie po jej otrzymaniu (np. utworzenie notatki służbowej z rozmowy telefonicznej bezpośrednio po jej odbyciu, aby uniknąć zapomnienia jakiejś jej części);
- zapisywanie informacji w sposób ustrukturyzowany i powiązany ze sobą;
- stosowanie zwięzłego stylu i nietworzenie zbędnych odnośników do innych informacji, które zmuszają do dalszych poszukiwań celem zintegrowania informacji.

Dostępność
Podstawowym elementem zapewnienia dostępności informacji jest jej utrwalenie na stałym nośniku, czyli mówiąc potocznie „przeniesienie myśli na papier". Zignorowanie przez pracownika jakiejś ważnej informacji lub pominięcie jej zapisu w dokumentacji sprawy (pamięć o niej tylko w umyśle pracownika odpowiedzialnego za gromadzenie dokumentacji) powoduje, że informacja ta nigdy nie będzie dostępna dla innych użytkowników. Warto także zwrócić tu uwagę na takie zapisywanie informacji, które pozwala na łatwy i szybki do niej dostęp. Jako dobre praktyki można przywołać:

- konsekwentne stosowanie ustalonych zasad nadawania informacjom statusu „ważne" i „nieważne", tak aby w podobnych sprawach można było się spodziewać podobnego zakresu informacji (np. notatek służbowych zapisanych w podobnym formacie);
- stosowanie nazw dokumentów i spraw jasno wskazujących na ich treść;
- unikanie zbyt ogólnych tytułów lub mało różniących się od siebie (np. „Podanie", „Wniosek", „Korespondencja").

Transmisja, przechowywanie, przetwarzanie
Na poziomie wrażliwości informacyjnej wskazane stany informacji są ze sobą na tyle zintegrowane, że trudno jest uchwycić moment przejścia z jednego stanu do drugiego. Odnoszą się one bowiem do procesów myślowych pracownika, który organizuje uzyskane przez siebie dane w informację na poziomie operacji intelektualnych. Zwrot tych operacji jest odwrotny do porządku ich przywołania w podtytule. Pracownik najpierw przetwarza pozyskane dane, następnie przechowuje je w pamięci, ponownie przetwarza, organizuje, by ostatecznie dokonać ich transmisji na nośnik informacji jak papier, plik cyfrowy, itp. Nieraz po transmisji następuje uzupełnienie lub poprawa informacji, czyli ponowne przetwarzanie, przechowywanie, transmisja. Ze względu na stopniowy zanik śladu pamięciowego („zapominanie") należy tutaj pamiętać (*pun intended*) o niezwłoczności „przelania myśli na papier", precyzji i kulturze intelektualnej (dobór informacji i sposobu ich reprezentacji) oraz względzie na to, iż z danej informacji będą korzystać inne osoby niż sam pracownik ją tworzący. Ten ostatni fakt czasami może umknąć uwadze pracownika, dlatego cenną praktyką jest zadawanie sobie przez niego pytania „gdybym to ja miał korzystać z tej informacji, to jak powinna ona wyglądać?".

Technologia
Wykorzystanie dostępnej technologii, rozumianej tu jako metody i środki zapisu informacji, ułatwia pracownikowi spełnienie elementów bezpieczeństwa informacji, o których mowa wyżej. Bez względu na to, czy środkiem tym jest spisanie wstępne informacji „na brudno", system notatek w programie komputerowym, czy korzystanie z gotowych formularzy zawierających pola z autouzupełnieniami dla powtarzalnych dokumentów, wykorzystanie współczesnych zdobyczy technologii cyfrowych w znaczącym stopniu przyczynia się do wsparcia pracownika przy tworzeniu informacji. Żaden z oferowanych środków nie spełni jednak swojej roli, jeżeli nie będzie pracownikowi znany i chętnie wykorzystywany. Ostatecznie jednak to nie korzystanie z takich czy innych narzędzi jest ważne, a kompletność i prawdziwość informacji. Technologia może jedynie pomóc w ich uzyskaniu.

Polityka i procedury
Każda jednostka będąca pod nadzorem archiwalnym posiada szczegółowe regulacje prawne dotyczące mechanizmów pracy biurowej, w tym tworzenia i kompletowania dokumentacji spraw. Przestrzeganie ich zapisów przez pracowników jednostki ma ogromne znaczenie dla zapewnienia poufności, integralności i dostępności informacji w momencie jej tworzenia. Jednakże aby to osiągnąć regulacje te muszą być odpowiednio sprecyzowane, a złożone, wieloetapowe czynności zoperacjonalizowane do postaci algorytmów. Jak zostało to już zaznaczone, niemałą rolę mają tu do odegrania archiwiści zajmujący się nadzorem archiwalnym. Nieraz to ich własna wrażliwość informacyjna decyduje o tym, czy w wewnętrznych regulacjach prawnych jednostki znajdą się zapisy precyzyjnie określające sposób postępowania z informacją od momentu jej odpowiedniego zapisywania w postaci dokumentu. Regulacje te, rzecz jasna, będą uzależnione od specyfiki pracy kancelaryjnej danej jednostki, jednakże pewne dobre praktyki „infotwórcze" znajdą zastosowanie w każdej sytuacji pracy z dokumentacją.

Czynniki ludzkie
Wrażliwość informacyjna to kompetencja każdego pracownika odpowiedzialnego za wytwarzanie informacji, zwłaszcza tych, dla których źródłem są materiały archiwalne. Czynniki ludzkie, choć omówione na końcu, są w przedstawianym modelu bezpieczeństwa informacji najszerszym i najważniejszym aspektem wspomnianej kompetencji. Do czynników tych można zaliczyć m. in.:

- indywidualne cechy osobowościowe pracownika, takie jak precyzja myślenia, bogactwo języka, precyzja i poczucie obowiązku;
- zaangażowanie pracownika w pracę oraz jego motywacja do jej wykonywania;
- zapewnienie pracownikowi odpowiedniego środowiska wykonywania pracy, w tym wyposażenie go w niezbędną wiedzę, umiejętności i środki techniczno-organizacyjne wpływające na jej jakość;
- uwzględnianie takich czynników w pracy pracownika jak: brak odpowiedniej komunikacji i konsultacji w sytuacjach problemowych (brak szukania pomocy u innych w trudnych lub niejednoznacznych przypadkach tworzenia informacji), przecenianie pracownika przez niego samego, roztargnienie i brak uwagi, zmęczenie, presja, stres, brak u pracownika świadomości kontekstu tworzenia informacji, którym jest fakt zawarcia tych informacji w ramach materiałów archiwalnych, czyli dokumentacji przeznaczonej na wieczyste przechowywanie.

Czynniki ludzkie obejmują swym zakresem wszystko to, co wpływa zarówno pozytywnie, jak i negatywnie na proces tworzenia pełnych i prawdziwych informacji przez pracownika. Rozpoznanie i uwzględnienie tych czynników pozwoli na lepszą organizację „mechanizmów pracy biurowej" i umożliwi wypracowywanie coraz lepszych praktyk takiego tworzenia i zapisywania informacji w ramach wytwarzanych materiałów archiwalnych, które zapewnią ich poufność, integralność i dostępność.

Zakończenie

Wrażliwość informacyjna, tak jak została ona przedstawiona w niniejszym artykule, dotyczy niemalże nieuchwytnego momentu, w którym pracownik odpowiedzialny za tworzenie informacji przeznaczonej do wieczystego przechowywania, decyduje do pewnego stopnia o jej treści i kształcie. Nie bez przesady będzie zatem stwierdzenie, iż nie tylko bezpieczeństwo informacji zaczyna się „w głowie" pracownika, ale także kształtowanie narodowego zasobu archiwalnego. Ostatecznie przecież do zasobu archiwalnego trafiają materiały archiwalne o takiej treści i w takim kształcie, jaki został nadany przez aktotwórcę rękami jego pracowników. Obszar nadzoru archiwalnego ma tutaj wielkie (przed)pole do popisu, przede wszystkim poprzez „ludzki" wpływ archiwistów na pracę poszczególnych pracowników. Wrażliwość informacyjna bowiem to nie jest coś, co można do końca zamknąć w sformułowaniach normatywów kancelaryjnych czy innych regulacji wewnętrznych nadzorowanej jednostki wytwarzającej materia-

ły archiwalne. U źródeł materiałów archiwalnych zawsze stoją ludzie z krwi i kości, wraz ze wszystkimi możliwościami i ograniczeniami takiej kondycji. Dzięki temu materiały archiwalne mają swoją niezacieralną, ludzką pieczęć i pięknie wpisują się w dziedzictwo narodowe, które jest niczym innym, jak wyrazem jego kultury duchowo-materialnej.

Summary

Informational sensitivity and information security in archival activities

The paper discussess informational sensitivity in a process of guaranteeing such information properties as confidentiality, integrity and availability. Information security, pivotal factor in archival activities, is one of the most important concern of state archives. Its execution however doesn't start after assumption of archival materials from organizational entities under archival supervision, but during their creation in those entities. Influence, which supervision archivists have on regulations and mechanics of creating information and records in supervised entities is vast, but limited. Informational sensitivity, a personal competence of every single clerk and archivist involved in creation of information, has a fundamental meaning in guaranteeing completeness, readability, intelligibility and authenticity of information during the very moment of their creation. McCumber's cube is a model of information security which is used in this paper to demonstrate interconnection of mentioned security and informational sensitivity. As a human factor, informational sensitivity plays an important role in process of shaping national archival resources.

Bibliografia

Akty prawne

Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (tekst jedn. Dz.U. z 2020 r., poz. 164).

Literatura

Cieślarczyk M., *Psychospołeczne i prakseologiczne aspekty bezpieczeństwa informacyjnego,* [w:] *Bezpieczeństwo informacyjne w XXI wieku*, red. M. Kubiak, S. Topolewski, Siedlce–Warszawa 2016.

Degen R., *Kancelarie i archiwiści. Garść uwag na temat wpływu pracowników archiwów państwowych na mechanizmy pracy biurowej administracji w Polsce po 1918 roku*, [w:] *Dzieje biurokracji na ziemiach polskich*, t. 2, red. A. Górak, D. Magier, Lublin–Siedlce 2009.

Fehler W., *O pojęciu bezpieczeństwa informacyjnego*, [w:] *Bezpieczeństwo informacyjne w XXI wieku,* red. M. Kubiak, S. Topolewski, Siedlce–Warszawa 2016.

Konstankiewicz M., Niewęgłowski A., *Narodowy zasób archiwalny i archiwa. Komentarz*, Warszawa 2016.

McCumber J.R., *Information Systems Security: A Comprehensive Model*, [in:] *14th National Computer Security Conference*, Washington D.C., 1991.

McCumber J., *Assessing and Managing Security Risk in IT Systems: A Structured Methodology*, Auerbach 2005.