Tom LXXI Nr 5 2019 DOI 10.33226/1231-2037.2019.5.34

Łukasz NYSZK
lukasz.nyszk@wat.edu.pl; nr ORCID: 0000-0002-6254-747X
Wojskowa Akademia Techniczna, Wydział Logistyki, Instytut Logistyki

Bezpieczeństwo informacji w logistycznym systemie informatycznym klasy CRM

Security of information in the logistic it system of crm class

Praca dotyczy bezpieczeństwa informacji przetwarzanych w systemie informatycznym CRM, a celem jest scharakteryzowanie istoty oraz podstaw funkcjonowania systemu informatycznego CRM, z uwzględnieniem zasad bezpiecznego zarządzania informacjami zgromadzonymi w CRM. W rezultacie zaprezentowanej analizy wykazano, że CRM to kompleksowe rozwiązanie pozwalające usprawnić procesy zarządzania informacją w firmie. Zapewnienie bezpieczeństwa informacji to najważniejszy warunek wdrożenia i funkcjonowania systemu klasy CRM. W procesie kreowania takiego bezpieczeństwa ważny udział przypada ustawodawcy, który sformułował pewne minimalne standardy ochrony informacji w systemach informatycznych.
Słowa kluczowe: CRM, informacja, system informatyczny, technologia.

The work concerns the security of information processed in the CRM IT system. The aim is to characterize the role and basis of the CRM information system, including the principles of information security management in CRM, which is a comprehensive solution of information management. Ensuring information security is the most important condition for the implementation and functioning of the CRM class system. The legislator formulated minimum standards of information protection in IT systems, which also applies to CRM
Key words: CRM, information, IT system, technology.

WSTĘP

W artykule podjęto problematykę bezpieczeństwa informacji w systemie informatycznym klasy CRM, z uwzględnieniem wybranych podstaw funkcjonowania systemu informatycznego tej klasy oraz zasad ochrony informacji. Problematyka jest aktualna oraz istotna choćby ze względu na wprowadzone w ostatnich latach zmiany prawne w obszarze ochrony informacji gromadzonych i przetwarzanych w systemach informatycznych. Najważniejszą zmianą należy traktować tutaj zaimplementowanie w krajowym porządku prawnym przepisów unijnego tzw. rozporządzenia RODO, czyli rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Ponadto, w ostatnich latach rosło znaczenie systemów informatycznych wykorzystywanych w organizacjach celem poprawy mocnych stron oraz zwiększenia rynkowych szans konkurencyjnych. W praktyce ujawniło się też coraz większe zainteresowanie wdrażaniem rozwiązań klasy CRM.

Celem rozważań o zagadnieniu (problemie) zawartym w tytule artykułu jest scharakteryzowanie istoty oraz podstaw funkcjonowania systemu informatycznego CRM, z uwzględnieniem zwłaszcza zasad bezpiecznego zarządzania informacjami zgromadzonymi w systemie tej klasy. Należy stwierdzić, że wspomniane zasady mają istotne znaczenie, zarówno dla podmiotów, jak i użytkowników systemu, których informacje są w nim zgromadzone (na przykład partnerów biznesowych, dostawców i innych klientów przedsiębiorstwa). W artykule do dociekań przyjęto tezę, zgodnie z którą system informatyczny klasy CRM stanowi doskonalące rozwiązanie wspierające rozwój organizacji, którego efektywne działanie zależy w istotnej mierze od przestrzegania zasad bezpiecznego zarządzania informacjami.

1. SYSTEM INFORMATYCZNY CRM – DEFINICJA, GENEZA, FUNKCJE I ARCHITEKTURA SYSTEMU

Przed określeniem istoty systemu klasy CRM należy wyjaśnić pojęcie systemu informatycznego jako pewnego narzędzia technologicznego pozwalającego na szerzej rozumiane zarządzanie informacjami. Pod tym pojęciem rozumie się wszelkie urządzenia, z których przynajmniej jedno – w oparciu o wcześniej zainstalowane oprogramowanie – ma możliwość automatycznego pozyskiwania, gromadzenia, przetwarzania i przekazywania danych komputerowych oraz innych informacji, przy zapewnieniu odpowiedniego poziomu ochrony takich danych oraz informacji. System informatyczny cechują określone funkcje użyteczne z punktu widzenia zarządzania obiegiem informacji w przedsiębiorstwie.

Z kolei według innej definicji, pod pojęciem systemu informatycznego istnieje „zbiór powiązanych ze sobą elementów sprzętowych, programowych i sieciowych, którego funkcją jest przetwarzanie danych z użyciem technik komputerowych”. Korzyści z przyjęcia systemowych narzędzi zarządzania informacjami w organizacji mogą być widoczne na różnych poziomach takiego zarządzania. Chodzi tu zarówno o tworzenie, zdobywanie, organizowanie obiegu, przechowywanie, dystrybuowanie, jak również wykorzystywanie informacji w praktyce działalności gospodarczej. Możliwość kompleksowego zarządzania informacją na wszystkich tych płaszczyznach stanowi przesłankę wskazującą na silną potrzebę uwzględnienia przez przedsiębiorców szansy wdrożenia określonych systemów informatycznych.

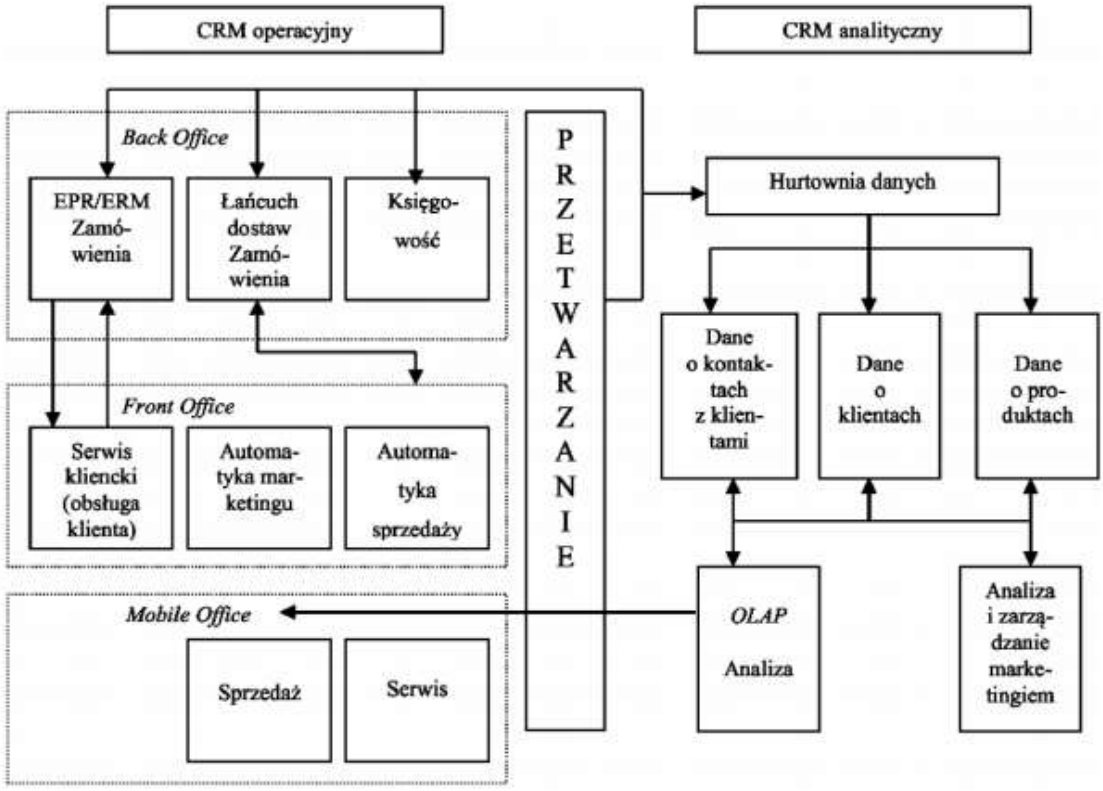
Jednym z praktycznych rozwiązań w dziedzinie zarządzania informacją w firmie jest system informatyczny klasy CRM (z ang. *Customer Relationship Management*), którego istota wyraża się w przyjęciu skutecznych rozwiązań technologicznych w celu obsługi relacji

z klientami przedsiębiorstwa. Istotą systemu CRM jest przyjęcie technologicznych rozwiązań umożliwiających i ułatwiających komunikowanie się przez firmę z klientami. Oprogramowanie wspierające umożliwia tu rejestrację i gromadzenie baz danych o klientach, planowanie rozmaitych interakcji z klientami, czy analizowanie danych w różnych przekrojach w celu dokonywania symulacji przyszłych zmian. Co ważne, system klasy CRM postrzega się nie tylko jako zbiór narzędzi informatycznych, ale przede wszystkim jako trwałą filozofię zarządzania, powiązaną spójnie ze strategią ogólną przedsiębiorstwa. W literaturze zauważono, że sprowadzanie systemu CRM wyłącznie do oprogramowania i aplikacji komputerowych jest błędne, ponieważ jest to cały zbiór technik i strategii rozwijania relacji z klientami. W dalszej części artykułu, ze względu na specyfikę analizowanego problemu, skupiono się jednak na aspekcie technologicznym funkcjonowania systemu informatycznego CRM, ponieważ to właśnie od tego aspektu zależy bezpieczeństwo informacji.

System CRM poprzez organizację i analizę danych umożliwia zarządzanie, a także rozwijanie aktywnych kontaktów z klientami i zarządzanie komunikacją z nimi. Łączy funkcje marketingu i obsługi klienta, zapewniając indywidualne podejście do każdego z nich, jak również oferując przedsiębiorstwu pełną wiedzę o potrzebach klientów. Usługodawcy dostarczający technologię CRM wychodzą z założenia podzielanego przez przedsiębiorców, zgodnie z którym „relacje z klientami stają się dla organizacji najważniejszymi zasobami (najcenniejszymi aktywami)przedsiębiorstwa. Aktywa te muszą być czynnie zarządzane w celu maksymalizacji wartości dodanej organizacji”. Z kolei wśród głównych celów, a zarazem uzasadnień stosowania CRM wymieniono:

- tworzenie trwałych więzi z klientami;
- podwyższanie poziomu satysfakcji nabywców towarów i usług oferowanych przez dane przedsiębiorstwo;
- zwiększenie sprzedaży dóbr producenta;
- maksymalizacja rentowności przedsiębiorstwa;
- możliwość przeprowadzenia zaawansowanej segmentacji klientów, czyli inaczej profilowania rynku ze względu na preferencje, potrzeby, czy wzory zachowań konsumenckich i dopasowania oferty firmy do wyodrębnionych segmentów;
- zmniejszenie kosztów prowadzenia bazy klientów oraz kosztów działalności marketingowej firmy;
- automatyzacja i ułatwienie zarządzania telefonicznymi punktami obsługi klienta oraz działami wsparcia technicznego.

Skupiając się na zarówno na ujęciu technologicznym, jak i biznesowym, na rynku 1 przedstawiono architekturę systemu CRM.



Rysunek 1. Architektura systemu klasy CRM
Źródło: T. Buchwald. T. Guzewski (2014). System zarządzania relacjami z klientem w przedsiębiorstwie międzynarodowym. *Progress in Economic Sciences,* nr 1, 246.

Wynika z analizy rysunku 1, iż architektura systemu informatycznego CRM obejmuje dwie dominujące struktury, tj. CRM operacyjny i CRM analityczny, wykorzystywane wzajemnie do przetwarzania danych zgromadzonych w systemie. Ten pierwszy obejmuje typowe funkcje biznesowe skupione wokół obsługi klienta i dotycz: wystawiania faktur, zarządzania zamówieniami, automatyzacji sprzedaży i marketingu, księgowości, czy serwisu posprzedażowego. Z kolei CRM analityczny wiąże się z efektywnym zarządzaniem przez komputer i oprogramowanie hurtownią danych, w której gromadzi się dane o kontaktach z klientami, dane osobowe samych klientów, czy dane na temat produktów i wyników ich sprzedaży. Opisywana struktura jest zintegrowana z innymi systemami zbierającymi dane wewnątrz organizacji, a zwłaszcza dane w obszarze sprzedaży, logistyki, czy zakupów przedsiębiorstwa. Pozwala to nie tylko identyfikować potrzeby i powtarzające się zachowania nabywcze konsumentów, ale też prognozować te fakty w przyszłości. W literaturze przedmiotu dodano, że proces pozyskiwania wiedzy z hurtowni danych w ramach CRM

składa się z takich etapów, jak konsolidacji danych, ich przekształcania, eksploracji w celu generowania reguł i drzew decyzyjnych, a także interpretacji i wizualizacji wyników. Pozyskana wiedza i wykorzystana wymaga ochrony w celu zachowania bezpieczeństwa konkurencyjnego oraz zapewnienia permanentnego jej rozwoju i przez skuteczną ochronę m.in. informacji w systemie informatycznym CRM. Dlatego w dalszej części artykułu zgłębiane będą zasady ochrony bezpieczeństwa informacji w logistycznym systemie informatycznym klasy CRM.

2. FUNKCJONOWANIE SYSTEMU KLASY CRM W ASPEKCIE BEZPIECZEŃSTWA INFORMACJI W PRZEDSIĘBIORSTWIE

Podstawowym wymogiem wdrożeniowym w przypadku informatycznego systemu klasy CRM jest zwrócenie uwagi w przedsiębiorstwie na przygotowanie systemu pod kątem zabezpieczeń. Uzasadnieniem jest przede wszystkim wrażliwość danych przechowywanych w bazie systemu. Z tego względu CRM powinien posiadać zabezpieczenia wynikające zarówno z obowiązującego stanu prawnego, jak również odpowiadające najlepszym praktykom rynkowym w zakresie funkcjonowania zabezpieczeń systemowych. Monitorowanie CRM pod kątem bezpieczeństwa pozostaje jednym z najważniejszych obowiązków przedsiębiorstwa jako wykonawcy systemu. Co więcej, aplikacja musi posiadać panel logowania, który pozwala na uwierzytelnianie osób decydujących się na korzystanie z CRM w przedsiębiorstwie. Uwierzytelnianie obejmuje wpisanie nazwy użytkownika oraz hasła zapisanego w bazie danych CRM. Dostęp do panelu logowania odbywa się poprzez kanał IP Sec VPN (*Internet Protocol Security, Virtual Private Network*) z wykorzystaniem protokołu L2TP (*Layer 2 Tunneling Protocol*). Zaleca się ponadto stosowanie innych metod uwierzytelniających, jak chociażby schemat SASL (*Simple Authentication and Security Layer*), czy protokół LDAP (*Lightweight Directory Access Protocol*). Rozwiązania te pozwalają skuteczniej zarządzać bezpieczeństwem połączeń i usług katalogowych (danych z takimi obiektami, jak użytkownicy, aplikacje oraz urządzenia sieciowe).

W literaturze przedmiotu podkreśla się, że wśród innych warunków skutecznej ochrony bezpieczeństwa informacji w logistycznym systemie informatycznym CRM należy wymienić odpowiednie przeszkolenie personelu biorącego udział we wdrożeniu i późniejszym obsługiwaniu systemu. Wytworzenie wśród pracowników świadomości odpowiedzialności za bezpieczeństwo informacji to warunek niezbędny do tego, aby móc korzystać z korzyści oferowanych przez to rozwiązanie teleinformatyczne. Co więcej,

ważnym warunkiem jest uczynienie z bezpieczeństwa informacji w CRM wymogu efektywnego zarządzania informacjami w przedsiębiorstwie. Innymi słowy, bezpieczeństwo, o którym mowa, to jedno z kryteriów okresowej oceny funkcjonalności i użyteczności CRM dla podmiotu gospodarczego. Wreszcie, podkreśla się, że w każdej organizacji, w której menedżerowie rozważają możliwość implementacji systemu informatycznego klasy CRM niezbędne jest wykorzystanie takich technologicznych rozwiązań, które są zgodne z ustanowioną w tym podmiocie gospodarczym ogólną polityką bezpieczeństwa. Chodzi tu o zaadaptowanie istniejących rozwiązań wewnątrz firmy do nowych możliwości i funkcji stwarzanych w ramach CRM, nie zaś całkowitą redefinicję zasad polityki bezpieczeństwa uprzednio stosowanej w praktyce organizacyjnej.

W tym miejscu należy wskazać, że istotą pomyślnego wdrożenia i późniejszego funkcjonowania systemu klasy CRM jest zastosowanie podejścia procesowego. Jak zauważono w piśmiennictwie, dotyczy ono tworzenia określonego, zaplanowanego w sposób celowy i racjonalny, a przy tym właściwie zorganizowanego, zbioru działań czy łańcucha wartości w organizacji. Podejście procesowe zakłada realizowanie zadań w sposób fazowy (etapowy), w pełni zaplanowany i zorganizowany, a nie doraźny, czy przypadkowy. Wiąże się ze stosowaniem harmonogramów, procedur oraz standardów pożądanych działań dla realizacji opracowanych wcześniej celów. Podejście to wiąże się ponadto z ciągłością raz podjętych zamierzeń, co ma istotne znaczenie przy okazji wykorzystywania logistycznego systemu informatycznego klasy CRM. Dzieje się tak, dlatego że „w bazach danych systemu CRM są przechowywane informacje o znaczeniu strategicznym dla organizacji, które muszą być chronione przed niepowołanym dostępem”. Podejście procesowe stanowi w związku z powyższym podstawowy wymóg dostosowany do strategicznego zarządzania informacją wewnątrz każdego przedsiębiorstwa zorientowanego technologicznie. Przykładowo, nie wystarczy raz wdrożyć pewnych zabezpieczeń chroniących informacje w systemie informatycznym CRM, ale należy systematycznie kontrolować i monitorować stan tych zabezpieczeń, jak również dokonywać aktualizacji procedur pozwalających na skuteczną ochronę baz danych.

Bezpieczeństwo oraz poufność danych nie tylko stanowi wymóg oceny funkcjonalności systemu informatycznego klasy CRM, ale pojawia się również jako jedno z kryteriów wyboru dostawcy oprogramowania w ramach CRM. Od dostawców wymaga się, aby dostępne na rynku oprogramowanie umożliwiało kontrolę bezpieczeństwa informacji, ochronę danych przed utratą, niepowołanym dostępem do aplikacji systemowej, a także

poprawę danych. obsługiwanych w systemie. Co więcej, niezbędnym wymogiem jest wyposażenie oprogramowania w możliwość formułowania kopii archiwalnych oraz w funkcję automatycznego odtwarzania danych w przypadku zaistnienia ewentualnej awarii. Prawidłowo przygotowane oprogramowanie powinno też ułatwiać użytkownikowi otrzymywanie powiadomień na temat wyszukanych błędów w CRM, co ma szczególnie istotne znaczenie w przypadku zapewniania bezpieczeństwa informacji.

Kluczowym sposobem przeciwdziałania wobec rozmaitych incydentów związanych z bezpieczeństwem informacji w logistycznym systemie informatycznym CRM jest wyposażenie tego systemu w liczne mechanizmy zabezpieczające. Oprócz wspomnianych wcześniej kanałów oraz protokołów, w piśmiennictwie wyróżniono następujące mechanizmy zabezpieczające:

- szyfrowane połączenie SSL zapewniające poufność w procesie przesyłania informacji;
- procedury uwierzytelniania poszczególnych użytkowników z wykorzystaniem loginu i hasła;
- wielopoziomowe systemy uprawnień użytkowników poprzez definiowanie różnych poziomów uprawnień w oparciu, z jednej strony, o funkcje zawarte w CRM, z drugiej natomiast, w związku z kompetencjami poszczególnych pracowników organizacji;
- dzienniki zdarzeń (inaczej logi) umożliwiające przywrócenie danych i śledzenie zmian w bazach danych, zwłaszcza pod kątem incydentów;
- codzienne automatycznie generowane kopie bezpieczeństwa pozwalające na przywrócenie stanu bazy danych na wypadek awarii sprzętu i oprogramowania albo fizycznej straty samych danych.

Kluczowym uwarunkowaniem uwzględnianym przez przedsiębiorców przy wdrażaniu systemów klasy CRM oraz stosowaniu polityki bezpieczeństwa informacji w tym systemie należy postrzegać wymogi prawne narzucone przez ustawodawcę odnośnie ochrony informacji. Dotyczy to zwłaszcza bezpieczeństwa przetwarzania danych osobowych, w szczególności po wejściu w życie unijnego rozporządzenia RODO. Ustawodawca narzucił firmom stosującym CRM szereg istotnych zasad zarządzania bezpieczeństwem informacji. Ze względu na złożoność wskazanej problematyki, warto jedynie wzmiankowo wskazać na kilka z nich. Należą do nich na przykład wymóg zbierania tzw. minimalnej liczby kategorii danych (zgodnie z zasadą *privacy by default*), wyposażenie administratora w prawo nadawania dostępu każdemu użytkownikowi CRM z osobna, przyjęcie aplikacji kontrolującej w sposób precyzyjny, kto, kiedy oraz jakie dane przeglądał w CRM, czy przygotowania procedury

usunięcia danych osobowych lub zaprzestania ich przetwarzania w sytuacji uzyskania zgłoszenia od klienta. Rozporządzenie RODO wymaga ponadto, aby transmisja danych odbywała się w oparciu o szyfrowane połączenie HTTPS, jeżeli administrator CRM korzysta z aplikacji dostępnych on-line. Zmiany prawne przyniosły także rozwiązanie, zgodnie z którym administrator co jakiś czas musi zmieniać hasło logowania do systemu CRM, a system powinien być wyposażony w funkcję określenia siły proponowanego hasła oraz uniemożliwiać powtórne wykorzystanie wcześniejszego hasła z racji gromadzenia informacji na temat haseł w pamięci systemowej. Rozporządzenie RODO zniosło przy tym obowiązek zgłaszania do publicznego organu nadzorczego (wcześniej GIODO, obecnie PUODO) zbiorów danych posiadanych w organizacji. Administrator danych osobowych musi zamiast tego prowadzić tzw. rejestr czynności przetwarzania, mający charakter wewnętrznego dokumentu firmowego i jest, zgodnie z przyjętymi wymogami, prowadzony zarówno elektronicznie, jak i w formie papierowej.

W ramach zapewniania bezpieczeństwa informacji w systemie klasy CRM niezbędne jest także odnotowywanie i zapisywanie incydentów związanych z takim bezpieczeństwem. Zgodnie z normą jakościową *ISO/IEC TR 18044:2004*, opisywanym incydentem jest w tym przypadku pojedyncze zdarzenie albo seria niespodziewanych bądź też niepożądanych zdarzeń losowych, których następstwem jest stworzenie znacznego prawdopodobieństwa zakłócenia działań biznesowych organizacji, a także zagrożenie bezpieczeństwu informacji". Do zarządzania bezpieczeństwem informacji w przedsiębiorstwie zastosowanie mają także inne normy jakościowe ISO, a przede wszystkim norma *ISO/IEC 27001 – Information Security Management System (ISMS)*. Zarządzanie incydentami, począwszy od ich identyfikacji i rejestracji, stanowi wymóg funkcjonalny po wdrożeniu logistycznego systemu informatycznego CRM. Inne etapy zarządzania incydentami związanymi z bezpieczeństwem informacji w organizacji dotyczą selekcjonowania ujawnionych zdarzeń, rozwinięcia incydentów i analizy ich przyczyn, opracowania procedur reagowania na incydenty z opracowaniem działań krótkookresowych i długookresowych oraz testowania (sondowania) aktualizowanych zabezpieczeń w odniesieniu do potencjalnych zagrożeń dla bezpieczeństwa informacji w przyszłości. Zamknięciem procesu zarządzania incydentami jest natomiast analiza skuteczności zrealizowanych działań zaradczych i następnie utrwalenie działających mechanizmów w systemie CRM. Omówione etapy mogą w praktyce zaistnieć przy licznych zagrożeniach dotyczących bezpieczeństwa informacji w CRM. Wśród takich zagrożeń wymienia się błędy i pomyłki ludzkie w ramach pracy na bazach danych, zamierzone działania szpiegowskie lub o charakterze sabotażu, kradzież danych, celowe ataki na

oprogramowanie, odchylenia w jakości usług systemowych i techniczne błędy oraz awarie sprzętu lub oprogramowania.

Kończąc rozważania w tym obszarze zainteresowania, należy wskazać również na istnienie pewnych barier w związku z przyjmowaniem systemu informatycznego klasy CRM przez przedsiębiorstwo. Oczywistą barierą mogą być wysokie koszty finansowe, które utrudniają implementację rozwiązań technologicznych zwłaszcza przez podmioty gospodarcze z sektora małych i średnich firm. Oprócz tego, stopień skomplikowania tego systemu i czas potrzebny na naukę pełnego opanowania jego funkcji przez osoby zarządzające, to również ważne ograniczenie. Innym czynnikiem jest ewentualna trudność w integracji poszczególnych funkcji zarządzania w ramach danego systemu, w tym integracja jego funkcji z innymi systemami informatycznymi (zwłaszcza ERP czy ERP II jako najczęściej wybieranymi jako centralne systemy informatyczne dla przedsiębiorstwa).

Warto nadmienić, że integracja, o której mowa, obejmuje także bezpieczeństwo zarządzania informacjami. Użytkownik musi zagwarantować takie bezpieczeństwo, niezależnie od wewnętrznych problemów związanych z koordynacją funkcji poszczególnych systemów informatycznych. W praktyce mogą zaistnieć też trudności w zakresie wyboru najlepszego dostawcy w rezultacie, iż konkurencja na rynku polskim w dalszym ciągu nie jest na tyle silna w porównaniu na przykład do rynków zachodnioeuropejskich. Elementem jakości oferty dostawców oprogramowania jest między innymi zdolność do zapewnienia ochrony informacji gromadzonych oraz przetwarzanych w systemie CRM. Wszelkie wątpliwości w tej dziedzinie to czynnik dyskwalifikujący potencjalnego dostawcę i zmuszający przedsiębiorcę do poszukiwania innej oferty w zakresie zakupu i wdrożenia informatycznego systemu CRM. Jak dodaje F. Mroczko, dla firmy stosującej system CRM liczy się przede wszystkim budowanie lojalności klienta. Brak zdolności zapewnienia wysokich standardów bezpieczeństwa danych osobowych tego ostatniego to istotne zagrożenie towarzyszące myśleniu o potencjalnym wdrożeniu systemu klasy CRM. Z kolei inne zagrożenia towarzyszące stosowaniu systemu informatycznego klasy CRM to ryzyko przechowywania informacji prywatnych na temat klientów bez wiedzy oraz bez zgody osób zainteresowanych, nieautoryzowane wprowadzanie zmian w systemie lub użycie danych niezgodnie z przeznaczeniem, czy choćby potencjalne ryzyko zniszczenia informacji.

3. PODSUMOWANIE I WNIOSKI

Podsumowując przedstawioną analizę, trudno nie zgodzić się ze stanowiskiem, zgodnie z którym bez wdrażania logistycznych systemów informatycznych wiele przedsiębiorstw nie mogłoby się dostatecznie szybko rozwijać w warunkach rosnącej presji konkurencyjnej na większości dzisiejszych rynków. Przyjmowanie systemów informatycznych klasy CRM to przykład odpowiedzi na powyższe wymogi, a zarazem przejaw dążenia menedżerów do przyjęcia narzędzi pozwalających na budowanie długoterminowych relacji między firmą a klientami. Co więcej, w świecie, w którym informacja to jeden z najcenniejszych zasobów (aktywów) organizacji, korzystanie z pomocy systemów informatycznych, w tym choćby CRM, to naturalna konsekwencja rozwoju biznesu.

W związku z argumentami przedstawionymi w artykule można przedstawić następujące wnioski ogólne:

1. System informatyczny klasy CRM to interesujące rozwiązanie przyczyniające się do maksymalizacji szans organizacji na osiągnięcie sukcesu rynkowego. Ocena prawidłowości funkcjonowania tego systemu zależy w istotnej mierze od skutecznych rozwiązań służących ochronie bezpieczeństwa informacji, które są przetwarzane w CRM.
2. Bezpieczeństwo informacji w logistycznym systemie informatycznym klasy CRM zależy zarówno od uwarunkowań zewnętrznych, jak i wewnętrznych. Jeśli chodzi o te pierwsze, najważniejsze znaczenie należy przypisać ustawodawstwu krajowemu oraz międzynarodowemu w przedmiocie ochrony informacji, ze szczególnym uwzględnieniem ochrony danych osobowych (jak choćby przykład RODO).
3. Z kolei w sytuacji uwarunkowań wewnątrzorganizacyjnych, skuteczna ochrona informacji w systemie CRM zależy w praktyce od spełnienia kilku kluczowych zasad. Pierwsza obejmuje świadomość odpowiedzialności pracowników za bezpieczeństwo informacji. Druga dotyczy efektywnego zarządzania informacją z użyciem CRM oraz uczynienia z ochrony informacji jednego z priorytetów funkcjonowania systemu. Kolejna zasada wiąże się natomiast ze stosowaniem rozwiązań technologicznych zgodnych z polityką bezpieczeństwa przyjętą w organizacji.
4. Ochrona informacji w systemie informatycznym CRM obejmuje stosowanie takich przykładowych rozwiązań praktycznych, jak szyfrowanego połączenia SSL, sposobów uwierzytelniania użytkowników systemu, wielopoziomowych systemów uprawnień

(logów), dzienników zdarzeń, czy choćby sporządzania automatycznych kopii bezpieczeństwa, które pozwalają na fizyczną ochronę danych zgromadzonych w systemie.

W rezultacie rozważań, dociekań i na podstawie wyników z analiz można potwierdzić w całości przyjętą we wstępie tezę, iż system informatyczny klasy CRM stanowi doskonalące rozwiązanie wspierające rozwój organizacji, którego efektywne działanie zależy w istotnej mierze od przestrzegania zasad bezpiecznego zarządzania informacjami. Wdrożenie wskazanego rozwiązania stanowi sposób na usprawnienie funkcjonowania firmy w trudnym otoczeniu konkurencyjnym w XXI wieku. Wiarygodność organizacji należy przy tym w dużej mierze od tego, jak wysoki jest stopień ochrony informacji w logistycznym systemie informatycznym klasy CRM. Działania takie jak kradzież, niekontrolowany wyciek danych, groźba ich odsprzedania innym podmiotom, czy też przejściowe trudności w sprostaniu nowym normom prawnym w zakresie ochrony danych osobowych, to czynniki osłabiające wiarygodność organizacji w warunkach zautomatyzowanego, teleinformatycznego zarządzania relacjami z klientami. Ponadto, należy prognozować, że problematyka bezpieczeństwa danych osobowych i innych informacji przetwarzanych w systemach informatycznych w prywatnych podmiotach gospodarczych stale zyskuje na znaczeniu i należy spodziewać się utrzymania tego trendu w nieodległej przyszłości. Może to mieć szczególne znaczenie przy wdrażaniu systemów klasy CRM jako narzędzi do pozyskania wiedzy na temat konsumentów.

LITERATURA

Babicka-Klecor, Z. RODO a zgłaszanie zbiorów danych do GIODO, https://legalgeek.pl/rodo-a-zglaszanie-zbiorow-danych-do-giodo/ (14.03.2019).

Bartuś, K. Billewicz, G. Olszak, C. (2015). Wykorzystanie systemów klasy CRM w działalności biznesowej przedsiębiorstw - wybrane wyniki badań. Studia Ekonomiczne Uniwersytetu Ekonomicznego w Katowicach, nr 232.

Billewicz, G. Olszak, C. (2014). Wdrażanie systemów klasy CRM - etapy i wybrane problemy. Studia Ekonomiczne Uniwersytetu Ekonomicznego w Katowicach, nr 187.

Błasiak, P. (2016). Bezpieczeństwo informacji w systemie informatycznym klasy CRM. W: W. Jagodziński, B. Kmieciak (red.), Człowiek w społeczeństwie. Wybrane aspekty badawcze. Bezpieczeństwo, zdrowie, edukacja (s. 38). Katowice: Wydawnictwo Naukowe Sophia.

Błasiak, P. Karbownik, K. (2016). CRM - system wspomagania wybranych obszarów logistycznych. W: R. Knosala (red.), Innowacje w zarządzaniu i inżynierii produkcji (t. 2, s. 763). Opole: Polskie Towarzystwo Zarządzania Produkcją.

Buchwald, T. Guzewski, T. (2014). System zarządzania relacjami z klientem w przedsiębiorstwie międzynarodowym. Progress in Economic Sciences, nr 1.

Cabała, P. Sołtysik, M. Tyrańska, M. (2015). Analiza problemów w procesie projektowania. W: A. Stabryła (red.), Praktyka projektowania systemów organizacyjnych przedsiębiorstwa (s. 66). Kraków: Wydawnictwo Mfiles.pl.

Fajfer, P., (2011). Wdrożenie systemu informatycznego - korzyści płynące z użytkowania systemu ERP. Organizacja i Zarządzanie, nr 2.

Hofman, M. Skrzypek, E. (2010). Zarządzanie procesami w przedsiębiorstwie. Warszawa: WKP.

Janowski, J. (2008). Elektroniczny obrót prawny. Warszawa: WKP.

Jelonek, D. (2015). The Evolution of Customer Relationship Management System. W: X. Zhuang (red.), Recent Advances in Computer Science (s. 29). Island 2015 (materiały pokonferencyjne).

Kochański, T. (2016). Pozyskiwanie wiedzy z systemów klasy Customer Relationship Management. W: Z. Kurasiński, M. Pawlisiak (red.), Logistyka w XXI wieku - wybrane zagadnienia (s. 25). Łódź-Warszawa: Wydawnictwo Społecznej Akademii Nauk.

Kochański, T. (2006). Sztuczna inteligencja w odkrywaniu wiedzy w systemach klasy CRM, Warszawa: Szkoła Wyższa im. Bogdana Jańskiego.

Łuczak, J. Tyburski, M. (2009). Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001. Poznań: Uniwersytet Ekonomiczny w Poznaniu.

Młynarczyk A. Czy twój CRM jest gotowy na RODO?, http://ladybusiness.pl/czy-twoj-crm-jest-gotowy-na-rodo/ (14.03.2019).

Mroczko, F. (2016). Logistyka, Wałbrzych: Wyższa Szkoła Zarządzania i Przedsiębiorczości.

Norma jakościowa ISO/IEC TR 18044:2004 Information technology - Security Techniques - Information Security Incident Management, https://webstore.iec.ch/p-preview/info_isoiec18044%Bed1.0%7Den.pdf (14.03. 2019).

Pałęga, M. (2014). Bezpieczeństwo informacji w logistycznym systemie informatycznym klasy CRM. Logistyka, nr 3.

Porębska-Miąc, T. (2013). Projektowanie i wdrażania systemów CRM. Studia Ekonomiczne Uniwersytetu Ekonomicznego w Katowicach, nr 128.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (Dz.Urz. UE L 119/1 z 4.5.2016).

Sołtysik-Piorunkiewicz, A. (2008). Zarządzanie relacjami z klientem z wykorzystaniem techniki customer care - charakterystyka systemów CRM. Zeszyty Naukowe Wyższej Szkoły Humanitas. Zarządzanie, nr 2.

Suchorzewska, A. (2010). Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem. Warszawa: WKP.

Wróblewska, W. (2013). Zarządzanie relacjami z klientami jako źródło sukcesu organizacji. Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Administracja i Zarządzanie, nr 97.

Zakres funkcjonalny systemu CRM (2012). Warszawa: Polska Organizacja Turystyczna.