Audyt oprogramowania: potrzeba czy obowiązek?

Audyt przeprowadzany jest na wszystkich stacjach roboczych i serwerach w placówce. Pozwala na dostarczenie szczegółowych informacji o zainstalowanych na nich aplikacjach oraz plikach przechowywanych na dyskach, które mogłyby być sprzeczne z wytycznymi jednostki oraz obowiązującym prawem.

Krzysztof Gajda
Instytut Zdrowia Publicznego,
Wydział Nauk o Zdrowiu,
UJ CM

Licencje komputerowe to dokumenty, które porządkują sposób korzystania z programów komputerowych. Dzięki nim wiadomo, kto może używać danej aplikacji i w jakim celu. Określają one, co można z programem zrobić, regulują też prawa własności. Innymi słowy, licencja jest rodzajem umowy zawieranej pomiędzy stronami, określającej sposób używania jakiegoś produktu. Licencje oprogramowania opisują:

- sposób używania aplikacji,
- formy jej wykorzystania (pola eksploatacji),
- ograniczenia praw użytkownika.

Licencje definiują na przykład maksymalną liczbę komputerów, na których można zainstalować program, liczbę korzystających z niego użytkowników, połączeń sieciowych generowanych przez aplikację czy dozwolony czas użytkowania. Z reguły wyłączają także odpowiedzialność autora za skutki błędów w jego dziełach. Prawa autorskie na program komputerowy, które są konsekwencją licencjonowania w Polsce, wygasają 70 lat po śmierci autora lub 70 lat po jego pierwszym opublikowaniu, jeżeli autor nie rozpowszechniał go osobiście lub gdy nie jest znany. W praktyce nie ma więc jeszcze programów, które nie są już chronione.

Rodzaje licencji

W praktyce można spotkać bardzo wiele rodzajów licencji na programy komputerowe. Wśród nich należy wymienić licencje wyłączne – stosowane głównie w projektach tworzonych na miarę i konkretne zapotrzebowanie danego odbiorcy – oraz licencje niewyłączne, czyli te, które nie wymagają zgody pisemnej i pozwalają korzystać z aplikacji wielu osobom. Inny podział licencji obejmuje:

- licencje komercyjne,
- licencje niekomercyjne – z tej kategorii wywodzi się grupa określana często skrótem FOSS (*Free Libre*) bądź *Open Source Software*. Obejmuje ona zarówno wolne, jak i otwarte oprogramowanie.

Szczególnym rodzajem licencji jest wolne oprogramowanie, które każdy może uruchamiać w dowolnym celu. Może być ono również bez ograniczeń rozkładane na czynniki pierwsze i dostosowywane do indywidualnych potrzeb. Nie ma także żadnych ograniczeń w kopiowaniu, rozpowszechnianiu kopii oraz udoskonalaniu własnych wersji aplikacji.

Z kolei otwarte oprogramowanie koncentruje się na podejściu praktycznym, z nieograniczonym dostępem do źródeł, ale bez wykluczenia częściowego, komercyjnego wykorzystania aplikacji. W szczególnych przypadkach można wyróżnić następujące rodzaje licencji:

- *Abandonware* – to określenie na programy porzucone. Nie jest to typowa licencja. Obejmuje aplikacje, które nie są już rozwijane, nie ma ich w sprzedaży, bez wsparcia ze strony producenta i pomocy technicznej. To często produkty firm już nieistniejących.
- *Adware* – licencja darmowego oprogramowania, które zawiera elementy reklamowe. Nie należy jej mylić z cechą aplikacji o tej samej nazwie. W zamian za możliwość korzystania z produktu użytkownik wyraża zgodę na wyświetlanie i oglądanie banerów reklamowych. Programy tego typu zwykle mają kod zamknięty. Dostępne są też często warianty komercyjne bez mechanizmów reklamowych.
- *AGPL* – wersja GPL używana do licencjonowania produktów, które uruchamiane są przez sieć po stronie serwera. Przykładem mogą być aplikacje na stronach serwisów internetowych. W takiej konfiguracji nie zachodzi fizyczna dystrybucja programu, więc nie ma mowy o udostępnianiu jego kodu źródłowego, co jest wymogiem GPL.
- *Beerware* – licencja pozwalająca na dowolne korzystanie z programu pod warunkiem, że w razie spotkania z jego autorem, użytkownik zobowiązany jest

zafundować mu piwo. Wariant tej licencji obliguje użytkownika jedynie do wypicia piwa za zdrowie autora. Jest to licencja raczej żartobliwa i znana bardziej wśród grup znajomych lub przyjaciół.

- *Emailware* – wariant licencji bezpłatnych programów, których warunkiem używania jest przesłanie autorowi wiadomości e-mail.
- *Donationware* – programy na tej licencji mogą być dowolnie używane, kopiowane, dystrybuowane i modyfikowane. Warunkiem legalności takich działań jest przesłanie autorowi dobrowolnej opłaty. Jej wysokość nie jest z góry określona i zależy jedynie od licencjobiorcy. Może być ona wręcz symboliczna.

W literaturze można znaleźć znacznie więcej rodzajów licencji, często opisywanych lub nazywanych przez firmy piszące oprogramowanie. Warto zwrócić uwagę na dużą liczbę rodzajów licencji programów firmy Microsoft.

Użytkowanie programów komputerowych i działanie licencji jest następstwem prawa autorskiego. *Ustawa o prawie autorskim i prawach pokrewnych* to akt prawny zabezpieczający prawa twórców i wydawców w Polsce. Reguluje on między innymi stosunki między podmiotami udostępniającymi oprogramowanie w ramach jakiejś licencji i licencjobiorcami. Chroni autorskie prawa osobiste (niezbywalne i niewygasające prawo do wiązania autora z jego dziełem) oraz autorskie prawa majątkowe (zbywalne prawo związane z wynagrodzeniem za korzystanie z utworu). Zabezpiecza wizerunek, adresatów korespondencji i tajemnicę informacji. W stosunku do oprogramowania i licencji precyzuje pola eksploatacji, takie jak zakres, miejsce i czas korzystania z utworu. Nie narzuca jednak sztywnych reguł, które mogą być dowolnie kształtowane przez strony umowy. Najczęściej kontrakt dotyczący wytworzenia programu komputerowego na zamówienie przedsiębiorcy zostaje sporządzony jako umowa o dzieło, czyli umowa rezultatu. Z tego względu w kwestiach nieuregulowanych przez strony zastosowanie znajdą przepisy *Kodeksu cywilnego* dotyczące umowy o dzieło (art. 627-646 *Kodeksu cywilnego*), z zastrzeżeniem przepisów szczególnych dotyczących dzieła prawno-autorskiego, wynikających z przepisów *Ustawy o prawie autorskim i prawach pokrewnych* (art. 41-68). Umowy dotyczące oprogramowania komputerowego zakładają najczęściej:

1. wytworzenie nowego oprogramowania na specjalne życzenie zamawiającego,
2. dostosowanie istniejącego oprogramowania do potrzeb zamawiającego poprzez „kastomizację" lub stworzenie dodatkowych funkcjonalności,
3. nabycie przez zamawiającego funkcjonującego na rynku rozwiązania informatycznego.

Interoperacyjność w kontekście audytu jednostek publicznych

Interoperacyjność należy rozumieć jako zdolność systemów informatycznych do wymiany danych, niezależnie od platformy operacyjnej. W *Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r.* określone są Krajowe Ramy Interoperacyjności. Mowa jest między innymi o tym, że organ władzy publicznej, prowadzący rejestr publiczny zawierający obiekty inne niż wymienione w ust. 1, wnioskuje do ministra właściwego do spraw informatyzacji o opublikowanie w repozytorium interoperacyjności, prowadzonym w ramach ePUAP, schematu XML struktur danych cech informacyjnych tych obiektów. Ponieważ podmioty lecznicze świadczą usługi z pieniędzy publicznych, te, które mają podpisaną umowę z NFZ, też wykonują takie działania (raportowanie odbywa się w formacie XML). We wspomnianym rozporządzeniu mowa jest również o tym, że systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk. Zatem systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne (np. szpitale publiczne) wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych. Z tego między innymi powodu audyty systemów informatycznych podmiotów świadczących zadania publiczne wykonuje się w oparciu o COBIT 4.1, ISO 27001 oraz inne standardy i normy. Należy zwrócić szczególną uwagę na audyt zgodności z przepisami prawa, normami i regulacjami wewnętrznymi oraz audyty zgodności z ramami interoperacyjnymi.

Cele i etapy audytu oprogramowania

Audyt oprogramowania to ocena przedsiębiorstwa pod względem zarządzania licencjami oraz legalności posiadanego oprogramowania. Audyt przeprowadzany jest na wszystkich stacjach roboczych i serwerach w placówce i pozwala na dostarczenie szczegółowych informacji o zainstalowanych na nich aplikacjach oraz plikach przechowywanych na dyskach, które mogłyby być sprzeczne z wytycznymi jednostki oraz obowiązującym prawem. Brak zarządzania zakupionymi licencjami i różnorodność umów licencyjnych mogą powodować problemy, takie jak na przykład.:

- brak ciągłości w pracy, np. w momencie naprawy komputera. Nagle może okazać się, że nie można danej aplikacji zainstalować, bo nie ma do niej klucza licencyjnego lub płyty instalacyjnej,
- obniżenie bezpieczeństwa danych firmy, brak kontroli nad legalnością oprogramowania, czyli użytkowania oprogramowania zgodnie z jego licencją,
- utrudnienia w zakresie pracy zespołowej, w tym wymiany informacji.

Wiedza o tym, jakie oprogramowanie zostało zainstalowane i gdzie ono się znajduje, pozwala sku-

teczniej je chronić. To oznacza wyższy poziom bezpieczeństwa całej jednostki oraz pewność, że będzie ona funkcjonować prawidłowo. Według zaleceń BSA (*Business Software Alliance*), ale także zgodnie z racjonalnymi przesłankami, audyt oprogramowania powinien być dokonywany co najmniej raz w roku.

Podstawowe cele audytu to:

- inwentaryzacja oprogramowania,
- zestawienie zainstalowanego oprogramowania z nabytymi licencjami,
- polisy i procedury,
- rozwinięcie planu ewidencyjnego z uwzględnieniem odpowiedniej dokumentacji.

Proces audytu oprogramowania może przebiegać według wielu etapów, dostosowywanych do specyfiki funkcjonalnej placówki. Przykładowe etapy mogą wyglądać następująco:

1. Zebranie informacji o zainstalowanym oprogramowaniu.
2. Zebranie informacji o zakupionych licencjach.
3. Zebranie informacji o potrzebach w zakresie oprogramowania.
4. Zebranie informacji o rzeczywistym wykorzystaniu zainstalowanego oprogramowania do audytu oprogramowania.
5. Zestawienie zebranych informacji i stworzenie raportów.
6. Wdrożenie programu naprawczego polegającego na zakupach brakującego lub odinstalowaniu zbędnego oprogramowania.
7. Wdrożenie procedur zarządzania oprogramowaniem:
   - podpisanie odpowiednich dokumentów z pracownikami,
   - stały monitoring oprogramowania przy pomocy programu do audytu oprogramowania.

Reasumując, audyt oprogramowania powinien dać odpowiedź na pytania, czy oprogramowanie zainstalowane w placówce jest potrzebne, legalne i czy jego wersje są aktualne.

Metody przeprowadzania audytu oprogramowania

Przeprowadzenie audytu w zasadzie może odbywać się dwoma metodami. Pierwsza – droga, ale prostsza – to zlecenie wykonania audytu specjalistycznym firmom. Druga metoda to wykonanie audytu przy wykorzystaniu własnych zasobów. W tym drugim przypadku potrzebny jest czas i zaangażowanie pracowników, jednak jest to wariant zdecydowanie tańszy. Jeśli audyt wykonuje się kolejny raz, jest to metoda dobra. W przypadku audytu zerowego (wykonywanego po raz pierwszy) lepszą metodą jest zlecenie go zewnętrznej firmie wyspecjalizowanej w takich zadaniach. Gwarantuje to solidność i rzetelność przeprowadzenia tego procesu, z drugiej strony zaś związane jest z większymi kosztami.

W podmiotach leczniczych wykonywanie audytu oprogramowania może pomóc w podjęciu decyzji o zakupie kolejnych modułów szpitalnego systemu informatycznego (HIS) oraz o integracji modułów. Wymiana danych w modułach HIS możliwa jest, jeśli są one wyposażone w określony standard wymiany danych, np. HL7. Audyt oprogramowania może być pomocny w inwentaryzowaniu modułów również pod tym kątem.

Korzyści z audytu

Warto zwrócić uwagę na korzyści, jakie może dać regularne i solidne wykonywanie opisanych w artykule czynności. Podstawowe korzyści z audytu to między innymi:

- korzyści finansowe wynikające ze świadomego wykorzystania posiadanego oprogramowania i korzystania z optymalnych opcji zakupowych,
- optymalizacja planów inwestycyjnych związanych z oprogramowaniem (kupowanie wyłącznie tego, co jest naprawdę potrzebne),
- aktualizowanie tylko tych licencji, które naprawdę są używane – daje to wymierne korzyści finansowe dla całej firmy,
- redukcja kosztów pomocy technicznej wynikająca ze standaryzacji oraz usunięcia zbędnych i przestarzałych składników infrastruktury,
- maksymalne i optymalne wykorzystanie posiadanego oprogramowania,
- uniknięcie problemów prawnych oraz konsekwencji finansowych dzięki eliminacji naruszeń praw autorskich na terenie firmy (eliminacja piractwa komputerowego),
- audyt oprogramowania jest okazją do przeprowadzenia inwentaryzacji sprzętu komputerowego.

Działy IT powinny zapewnić rzetelność ewidencji autoryzowanego oprogramowania (oprogramowanie powinno być oznakowane, spisane i zaopatrzone w odpowiednie licencje). Można utworzyć bibliotekę licencjonowanego oprogramowania i zapewnić, że biblioteka oprogramowania jest odpowiednio kontrolowana – zarządzanie biblioteką oprogramowania powinno być stosowane w celu tworzenia ścieżek rewizyjnych zmian oprogramowania oraz w celu ewidencji numerów wersji, dat utworzenia i kopii poprzednich wersji. Dobrze jest okresowo ustalać nieautoryzowane oprogramowanie i przypisać odpowiedzialność za kontrolowanie go określonym osobom. Należy również zapisywać użycie nieautoryzowanego oprogramowania i raportować stan kierownictwu w celu podjęcia odpowiednich działań. Działy IT określają, kiedy kierownictwo podejmuje odpowiednie działania w przypadku naruszeń obowiązujących zasad. ❑

Piśmiennictwo

1. http://mojafirma.infor.pl/
2. http://www.microsoft.com/
3. *Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r.*
4. http://samorzad.infor.pl/
5. http://www.statlook.pl/