УДК 009.4

ЗАГАЛЬНИЙ РЕГЛАМЕНТ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ЄС: ЩО ПОТРІБНО ВРАХОВУВАТИ ДЛЯ ПОЛІГРАФІЇ

А. Т. Кобевко, О. В. Тимченко

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

Аналізуються ризики втрати персональних даних користувачів у процесах пересилання та друку документів у зв'язку із запровадженням у країнах ЄС Загального регламенту про захист даних (General Data Protection Regulation, GDPR). З огляду на цей Регламент, всі наявні процеси інформаційних технологій користувачів інформаційних послуг потрібно перевірити з погляду достатності захисту персональних даних. Показано, що виявлені ризики для безпеки персональних даних можна суттєво зменшити з використанням серверів друку та зашифрованої передачі даних.

Ключові слова: *персональні дані, Загальний регламент про захист даних (GDPR), ризики процесу друку.*

Постановка проблеми. Оскільки Україна від 2014 року має укладену Угоду про асоціацію з Європейським Союзом, то українські поліграфічні підприємства повинні бути готові до таких змін, щоб мати змогу співпрацювати з європейськими підприємствами або надавати послуги іноземним замовникам. З травня 2018 року запроваджено новий Загальний регламент захисту персональних даних (GDPR) користувачів інформаційних послуг, зокрема їх персональних даних. З огляду на цей регламент наявні процеси передачі даних, їх опрацювання в межах інформаційних технологій мають бути перевірені й усунені всі недоліки безпеки [1].

Нове законодавство дає нові визначення про збір та обробку даних і порушує низку питань. Яку інформацію вважають персональними даними? Які процеси інформаційних технологій впливають на безпеку персональних даних? Як розпочати перебудову інформаційних систем відповідно до нових вимог?

Тому наявні процеси інформаційних технологій, зокрема процеси друку, мають бути перевірені щодо ступеня безпеки, будь-які недоліки безпеки потрібно виявити, виправити та оптимізувати.

Мета статті — проаналізувати процес друку, проілюструвати проходження документа через різні етапи з моменту запуску до кінцевого продукту, виявити наявні ризики та слабкі місця безпеки процесу.

Виклад основного матеріалу дослідження. Відповідно до GDPR фізичні особи мають право на захист своїх персональних даних (ст. 1, GDPR) [2]. Проте виникає питання, як розпізнати, чи певні дані або інформація вважаються персональними даними. Дані потрапляють у категорію персональних, коли особа може

бути прямо або опосередковано ідентифікована, наприклад, за ім'ям, номером телефону, даними рахунку, поштовою або IP-адресою.

Опрацювання даних є законним, лише за умови виконання принаймні однієї з наведених нижче умов (ст. 6 GDPR — Законність опрацювання) [1]:

- суб'єкт даних надав згоду на опрацювання своїх персональних даних для однієї чи кількох спеціальних цілей;
- опрацювання є необхідним для виконання контракту, стороною якого є суб'єкт даних, або для вжиття заходів на запит суб'єкта даних до укладення договору;
- опрацювання є необхідним для дотримання встановленого законом зобов'язання, яке поширюється на контролера;
- опрацювання є необхідним для того, щоб захистити життєво важливі інтереси суб'єкта даних або іншої фізичної особи;
- опрацювання є необхідним для виконання завдання в суспільних інтересах або здійснення офіційних повноважень, покладених на контролера;
- опрацювання персональних даних є необхідним для контролю, окрім випадків, коли над такими інтересами переважають інтереси фундаментальних прав і свобод суб'єкта даних, що потребують охорони персональних даних, особливо якщо суб'єктом даних є дитина.

Право на захист персональних даних охороняється ст. 5 GDPR (Принципи обробки персональних даних) [1]. Згідно із законом компанії, відповідальні за захист документів зобов'язані своєчасно повідомляти про витоки даних. Крім того, за порушення директив про захист даних накладають дуже високі штрафи.

До 25 травня 2018 року компанії мали переглянути свої IT-процеси, а також документувати або навіть спростити їх. Наявні описи IT-процесів, такі як оглядові обробки, можуть потребувати коригування або навіть оновлення. Одним з елементів захисту персональних даних є оптимізація повного процесу друку, оскільки дуже часто у процесі друку існують значні ризики для безпеки (рис. 1). До них належать [2]:

- незашифрована передача персональних даних по мережі;
- незашифроване зберігання персональних даних під час процесу друку на серверах або жорстких дисках принтера;

Рис. 1. Ризики для безпеки персональних даних у процесі друку

– виведення конфіденційних документів до неправильних принтерів;
– документи, які містять персональні дані, що з принтера потрапляють стороннім особам.

Мережевий друк

Загальною тенденцією є заміна принтерів на робочих місцях на мережеві з причин оптимізації адміністративних та фінансових витрат. А це призводить до передачі конфіденційних даних через незахищену корпоративну мережу.

Процес друку починається у прикладній програмі. Він запускається або безпосередньо на відповідній робочій станції (рис. 2), або на хості сеансу віддаленого робочого столу, сервері XenApp [3], або віртуальному робочому столі (рис. 3).

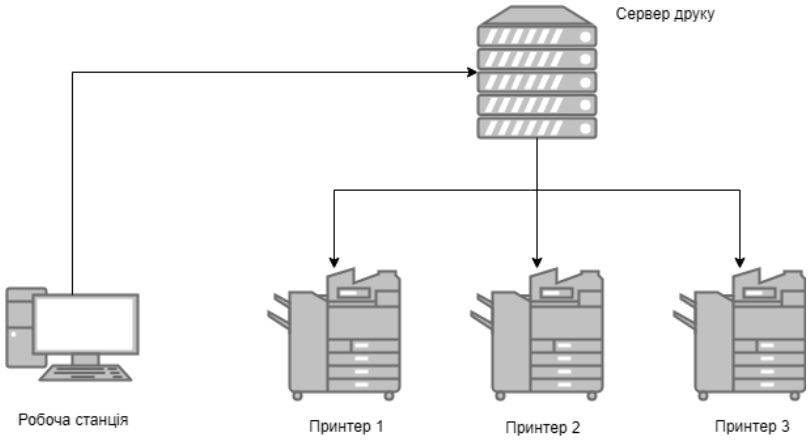

Рис. 2. Схема процесу друку від прикладної програми через сервер друку до мережевого принтера

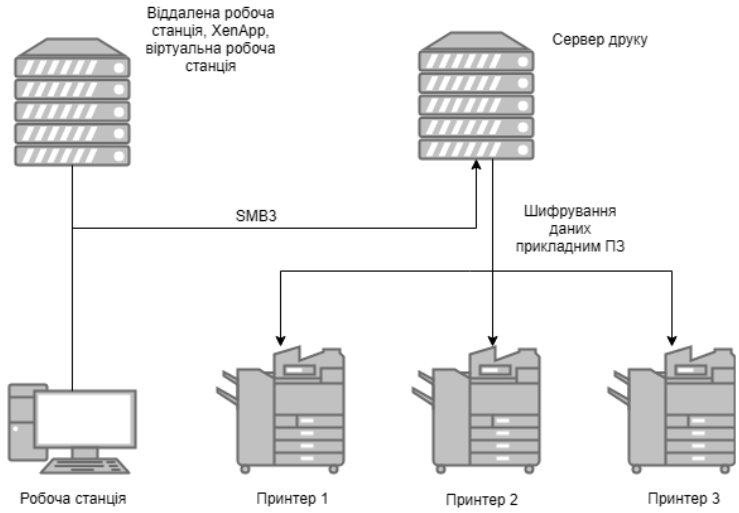

Рис. 3. Схема процесу шифрування даних друку на всі етапах від програми через сервер друку до мережевого принтера

XenApp — програмне забезпечення для віртуалізації і доставки додатків з віддаленого сервера на локальні пристрої користувачів через тонкий клієнт. Інакше кажучи, ця програма дає змогу запускати програми, створені для роботи у середовищі Windows, на комп'ютерах і мобільних пристроях, що працюють під управлінням інших операційних систем. Водночас самі додатки перебувають на виділеному сервері або в хмарі.

Для централізації процесів друку можна використовувати сервер друку. Це не лише спрощує адміністрування, а й дає можливість реалізувати технології безпеки, оскільки дає змогу захищати дані шифруванням із застосуванням прикладного програмного забезпечення (ПЗ) [4].

Слабкі точки друку в мережі

Адміністратори захищають програми та дані через захист доступу, а також шифрують підключення до серверів і робочих станцій. З іншого боку, дані для друку часто відправляються незахищеним шляхом до серверів друку, а звідти — до мережевих принтерів. Це призводить до виникнення таких слабких місць:

- мережеві карти всіх пристроїв, на які поширюється потік друку: робоча станція, робочий стіл, мережевий комутатор, маршрутизатор, сервер і мережевий принтер;
- принтери мають спільний доступ до сервера друку;
- жорсткі диски мережевих принтерів.

Шифрування в процесі друку

Існує кілька моментів, коли процес друку потрібно оптимізувати, щоб досягти всебічного та безпечного шифрування поліграфії, що відповідає стандарту GDPR.

Від програми до сервера друку

Від сервера Server Message Block (SMB) дані для друку можуть бути зашифровані програмою для спільного використання принтерів на сервері друку з можливостями Windows розділеного доступу до файлів (рис. 2). Це забезпечує взаємодію та доступ до спільних принтерів на сервері друку лише за допомогою зашифрованих з'єднань.

Від сервера друку до мережевих принтерів

Для підключень від сервера друку до мережевих принтерів можна використовувати лише сторонні рішення. Рішення окремих виробників принтерів призводять до збільшення адміністративного навантаження, оскільки вони мають бути встановлені та керовані для кожного користувача принтера на сервері друку. Тобто потрібне універсальне, незалежне від виробника рішення, яке також сумісне з великою кількістю різноманітних структур і бібліотек.

Мережевий принтер

На самому мережевому принтері необхідно переконатися, що неавторизовані особи не можуть увійти в інтерфейс принтера. Для цього потрібно використовувати сертифікати, які вимагають ім'я користувача та пароль. Якщо використовується внутрішній жорсткий диск принтера, він має бути зашифрований (на апаратній стороні). Викраденню готових роздруківок з вихідного лотка можна запобігти шляхом автентифікації користувача безпосередньо на принтері: смарт-карта, смартфон, а також автентифікацією PIN-кодом.

Висновки. Як описано в статті, процес друку проходить через різні етапи з моменту запуску до отримання кінцевого продукту. Стало зрозуміло, що підключення від сервера друку до мережевого принтера може бути захищене лише сторонніми рішеннями. Це призводить до високого адміністративного навантаження, оскільки рішення окремих виробників принтерів мають бути встановлені та керовані окремо на сервері друку. Мережевий принтер також становить ризик для безпеки. Коли друк виконується мережевим принтером, то не гарантується, що персональні дані користувачів не потраплять до сторонньої особи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Регламент європейського парламенту і ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). URL: https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf.
2. Printing Processes in the Context of the General Data Protection Regulation (GDPR). URL: https://www.thinprint.com/en/solutions/data-security-printing/.
3. Technical details about SMB/CIFS. URL: http://ubiqx.org/cifs/.
4. Citrix puts virtualization spin on flagship application delivery software. URL: https://www.networkworld.com/article/2275208/citrix-puts-virtualization-spin-on-flagship-application-delivery-software.html.

REFERENCES

1. Rehlament yevropeiskoho parlamentu i rady (IeS) 2016/679 vid 27 kvitnia 2016 roku pro zakhyst fizychnykh osib u zv'iazku z opratsiuvanniam personalnykh danykh i pro vilnyi rukh takykh danykh, ta pro skasuvannia Dyrektyvy 95/46/IeS (Zahalnyi rehlament pro zakhyst danykh). Retrieved from https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf (in Ukrainian).
2. Printing Processes in the Context of the General Data Protection Regulation (GDPR). Retrieved from https://www.thinprint.com/en/solutions/data-security-printing/ (in English).
3. Technical details about SMB/CIFS. Retrieved from http://ubiqx.org/cifs/ (in English).
4. Citrix puts virtualization spin on flagship application delivery software. Retrieved from https://www.networkworld.com/article/2275208/citrix-puts-virtualization-spin-on-flagship-application-delivery-software.html (in English).

doi: 10.32403/1998-6912-2019-2-59-50-55

GENERAL DATA PROTECTION REGULATION IN EU: WHAT TO CONSIDER FOR PRINTING INDUSTRY

A. T. Kobevko, O. V. Tymchenko

Ukrainian Academy of Printing,
19, Pid Holoskom St., Lviv, 79020, Ukraine
o_tymch@ukr.net

This paper analyzes the risks of personal data being lost in the process of sending and printing documents related to the implementation in the EU countries of the General Data Protection Regulation (GDPR). In view of this Regulation, all existing information technology processes of users of information services should be checked and any security deficiencies should be identified, corrected and optimized.

It has been shown that there are significant risks to the security of personal data during the printing process, including: unencrypted transmission of personal data over the network; unencrypted storage of personal data during the printing process on printers' servers or hard disks; outputting confidential documents to the wrong printers; Documents containing personal data are released to third parties from the printer.

It follows that critical equipment is network printers, which transfer sensitive data to which is carried out through the corporate network. A network printer also poses a security risk. When printing by a network printer, it is not guaranteed that the personal data will not be accessed by a third party. It is advisable to use a print server to centralize print processes. Not only does this simplify administration, but it also enables security technologies to be implemented. However, the applications themselves are on a dedicated server or in the cloud. The connection from a print server to a network printer can only be protected by third-party solutions. This results in high administrative burden, as the decisions of individual printer manufacturers must be installed and managed separately on the print server. Administrators protect applications and data through access security, and encrypt connections to servers and workstations. On the other hand, print data that is often sent unsafe to print servers and from there to network printers must be encrypted. On a network printer itself, make sure that unauthorized persons cannot enter the printer interface. Certificates that require a username and password should be used for this.

Keywords: *personal data, General Data Protection Regulation (GDPR), printing process risks.*

Стаття надійшла до редакції 18.07.2019.
Received 18.07.2019.