Інформаційна безпека організацій видавничо-поліграфічної сфери

Юлія Романишин
кафедра документознавства та інформаційної діяльності
Івано-Франківський національний технічний університет нафти і газу,
Івано-Франківськ, Україна
yulromanyshyn@gmail.com

Abstract. The article deals with theoretical and practical aspects of information security at the organization level. The main information threats for the modern institutions are identified. There are highlighted the most reliable and innovative methods of information protection. It is considered practical implementation of certain methods and means of information protection on the example of publishing and printing company.

Ключові слова: інформаційна безпека, інформація, захист інформації, інформаційні загрози.

Вступ

Стрімкий ріст інформації у сучасному суспільстві та розвиток інформаційно-комунікаційних технологій її створення й підтримки збільшує доступ до різноманітних інформаційних потоків та ресурсів, які функціонують як на рівні окремої організації, так і в глобальній мережі Інтернет. Оскільки релевантна інформація становить основу інформаційного виробництва її цінність є високою і, відповідно, набирають високої актуальності проблеми інформаційної безпеки та захисту інформації.

Результати дослідження

Інформаційна безпека – це стан захищеності інформаційної системи організації, при якому унеможливлюється нанесення шкоди через: неповноту, невчасність, невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; порушення цілісності, конфіденційності, доступності, несанкціоноване використання та розповсюдження інформації [1].

На основі проаналізованих джерел [2-4] можна виокремити наступні інформаційні загрози в сучасних організаціях, а саме: відсутність регламентованого доступу до інформації та даних; вільне втручання в програмне забезпечення; відсутність регламентації користувачів інформації; відсутність дублювання важливих документів на документальних носіях даних; часті удосконалення одного і того ж програмного забезпечення різними особами; відсутність схем інформаційного забезпечення рівнів управління тощо [4].

На сьогодні, перелік сучасних методів та способів забезпечення захисту інформації й інформаційної безпеки як організації, так і даних й інформації є досить великий. Ми виокремили найбільш актуальні серед них, а саме: засоби антивірусного захисту; засоби шифрування інформації; інструменти перевірки цілісності вмісту дисків; віртуальні приватні мережі; міжмережеві екрани (фаейрволи або брандмауери); засоби аутентифікації користувачів (відповідають за доступ до ресурсів конкретних користувачів); аналізатори мережевих атак; резервне копіювання (Google Disk, хмарні сервіси); фільтри спаму; фільтрація вмісту е-пошти (засіб захисту від втрати конфіденційної інформації) тощо [3-4].

Звісно, що ці методи можуть застосовуватися окремо, але для їх максимального ефекту, варто використовувати їх раціональне поєднання у комплексі.

Розглянемо рівень забезпечення інформаційної безпеки у діяльності видавничо-поліграфічної фірми ТзОВ “Респект”.

ТзОВ “Респектр” (https://respectr.com/) – це приватна друкарня, яка спеціалізується на широкоформатному екосольвентному друці та продажі рекламних конструкцій. Основним координаційним центром друкарні є відділ обробки замовлень. Обмін інформаційними потоками відбувається між підрозділами на всіх рівнях організації. На виробничому рівні відбувається обмін інформацією про макети замовлень. На вищих рівнях – обмін звітною та розпорядчою інформацією. Зовнішні інформаційні потоки поступають в організацію у формі замовлень клієнтів. Вихідні потоки – це готові продукти, які видаються замовникам.

Важливою частиною захисту інформації в ТзОВ “Респектр” є технічний захист. Електронний цифровий підпис для друкарні є складовою системи захисту інформації. У кожного працівника організації є власний ЕЦП. Друкарня обмінюється е-документами із партнерами та клієнтами за допомогою Інтернет-сервісу Paperless. ТзОВ “Респектр” зберігає важливу інформацію в електронному вигляді (бухгалтерські БД, БД клієнтів, технічна документація, е-листування) та застосовує спеціальну систему резервного копіювання Handy Backup, для унеможливлення втрати інформації. Програма встановлена на кожному комп’ютері, а резервні копії зберігаються на загальному мережевому диску. Крім того, на офісних комп’ютерах друкарні встановлений антивірус Avast Business Prime, оскільки антивірусний захист є важливим аспектом захисту інформації. Перераховані заходи дозволяють скоротити ризики втрати важливої інформації.

Незважаючи на достатній рівень захищеності інформації на ТзОВ “Респектр”, все ж таки є деякі недоліки.

Однією з проблем є видача замовлень користувачам. Готова продукція надсилається замовникам кур’єрами або іншими службами доставки. Проте, серед клієнтів існує практика самовивозу друкарської продукції із цеху. Така децентралізована система видачі замовлень заважає вести статистику, викликає плутанину серед замовників, а також спричиняє більші витрати на кур’єрську доставку. Для вирішення проблеми пропонуємо встановити інтерактивну дошку на пропускному пункті друкарського цеху із списком клієнтів та їх замовлень і, можливістю безпосередньо самим клієнтам ставити позначку про отримання замовлення. У кінці дня адміністратор за допомогою кур’єрської доставки відправляє замовлення, які не забрали особисто.

Оскільки друкарня використовує централізоване збереження резервних копій на базі система Handy Backup, то ризик втрати всієї інформації у випадку несправності мережевого диску досить високий. Тому, доцільно додатково створювати резервні копії на кожному комп’ютері.

Висновки

Отже, вдосконаливши деякі аспекти захисту інформації ТзОВ «Респект» зможе забезпечити себе від несанкціонованого доступу, втрати чи спотворення інформації. Сьогодні, на інформаційному ринку стає дедалі актуальнішою технологія інфраструктури відкритих ключів, тому на перспективу вважаємо доречним для ТзОВ “Респектр” використання цієї технології, як засобу для забезпечення надійного захисту при передачі даних й інформації через мережу Інтернет, що є актуальним для аналізованої організації.

Література

[1] С. В. Северина, “Інформаційна безпека та методи захисту інформації”, Вісник Запорізького національного університету, №1(29), с. 155-161, 2016.

[2] А. В. Марунич, “Захист інформації як основна складова економічної безпеки підприємства”, Управління розвитком, № 14, с. 130-132, 2014.

[3] І. В. Либідь, “Методи забезпечення інформаційної безпеки”, Сучасні інформаційні технології. URL: http://www.rusnauka.com/35_OINBG_2010/Informatica/76346.doc.htm.

[4] [4] О. В. Черевко, “Теоретичні засади поняття інформаційної безпеки та класифікація загроз у системі інформаційного захисту”, Ефективна економіка, №5, 2014.