УДК 658.012

Я. М. Кіпчарська
Українська академія друкарства

МЕТОДИЧНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПОЛІГРАФІЧНОГО ПІДПРИЄМСТВА

Розглянуто сутність інформаційної безпеки й процес її забезпечення, сформовано схему кругообігу інформації та обґрунтовано засади побудови механізму захисту інформації на поліграфічному підприємстві.

Інформаційна безпека, кругообіг інформації, система захисту інформації, механізм захисту інформації

На сучасному етапі розвитку суспільства інформаційні технології активно впроваджуються в усі сфери національної економіки, інформація стає визначальним фактором ефективної діяльності підприємства. Кожний господарюючий суб'єкт, незалежно від форми власності та організаційно-правової форми, знаходиться в певному інформаційному середовищі, насиченому різноманітними ризиками, здатними миттєво знищити фінансові і матеріальні ресурси. Звідси, особливого значення набувають визначення типу необхідної для підприємства інформації, кваліфіковане її опрацювання й уміле використання при прийнятті рішень та для організації поточного контролю фінансово-господарської діяльності. Тенденція до підвищення цінності інформації як бізнес-ресурсу і як товару разом зі зростанням рівня інформаційних загроз приводить до суттєвого розширення вимог до існуючих систем інформаційної безпеки на більшості підприємств, зокрема і поліграфічних, діяльність яких безпосередньо залежить від обсягу, швидкості та якості обробки інформації. Тому вирішення проблеми розроблення ефективно функціонуючої системи інформаційної безпеки на сучасному поліграфічному підприємстві, що безпосередньо пов'язано з проблемою ефективності корпоративної системи захисту інформації, є вкрай важливим завданням.

Вагомий внесок у дослідження проблеми економічної безпеки підприємства зробили вітчизняні та зарубіжні науковці, зокрема, О. Ареф'єва, О. Барановський, В. Білоус, З. Герасимчук, Я. Жаліло, О. Кузьмін, А. Кірієнко, Т. Ковальчук, Б. Кравченко, О. Ляшенко, С. Покропивний, В. Пономаренко, Є. Раздіна, С. Реверчук, М. Флейчук, В. Франчук, І. Циглик, А. Штангрет та ін. Попри вагомість наукових досліджень вітчизняних і зарубіжних науковців щодо цієї багатопланової й складної проблеми багато аспектів ще не з'ясовано. Це стосується, зокрема, і дослідження однієї з функціональних складових економічної безпеки – інформаційної безпеки підприємства.

Питання економічної сутності інформації та визначення її цінності, а також особливості управління інформаційними ресурсами та інформаційною інфраструктурою досліджено в наукових працях учених Б. Аніна, Н. Бекето-

ва, В. Бушуєва, В. Захарова, О. Кохановської, С. Наливайченко, С. Паринової, В. Ортинського, С. Станицького, А. Чекатова, В. Щетиніна, І. Яковенко та ін. Незважаючи на високий рівень наукових робіт зазначених науковців, все-таки недостатньо вивченими залишаються проблеми системи інформаційної безпеки, що не дає можливості для підвищення рівня стабільності та функціонування підприємств.

Метою нашої статті є формування методичних засад забезпечення інформаційної безпеки на поліграфічному підприємстві.

Під інформаційною безпекою мають на увазі захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних дій природного чи випадкового характеру, які можуть завдати збитку власникам інформаційного ресурсу або користувачам інформації і підтримуючої інфраструктури [5]. Разом з тим під інформаційною безпекою підприємства розуміється комплекс заходів і засобів захисту, що забезпечують збереження й конфіденційність інформації в поєднанні з визначеною доступністю до неї користувачів. Відповідно, інформаційна безпека має три основні складові [2]:

конфіденційність — властивість, яка гарантує, що інформація недоступна і не може бути розкрита несанкціонованими особами, об'єктами чи процесами. Можливість ознайомитися з інформацією мають лише ті особи, які володіють відповідними повноваженнями;

цілісність — властивість, яка гарантує, що система повноцінно виконує свої функції без навмисних або випадкових несанкціонованих втручань. Можливість внести зміни в інформацію повинні мати лише ті особи, які на це вповноважені;

доступність — можливість отримання авторизованого доступу до інформації з боку вповноважених осіб у відповідний санкціонований для роботи період часу.

Виходячи з того, що інформаційна безпека відображає захищеність інформаційного середовища та ефективність інформаційного забезпечення процесу управління на підприємстві, процес забезпечення інформаційної безпеки доцільно представити як взаємодію трьох підсистем:

захисту інформаційного середовища;

інформаційного забезпечення процесу управління;

діагностики рівня інформаційної безпеки [1].

Захист інформаційного середовища підприємства передбачає захищеність від зловмисних дій як конкурентів, так і власних співробітників, а також від незловмисних внутрішніх негативних впливів. Дану тезу обґрунтуємо наступними міркуваннями: найбільшим джерелом витоку інформації є персонал, тобто люди, які працюють з інформацією, створюють й обробляють її, але можуть продати чи просто передати останню із-за необережності. Саме тому важливим завданням для поліграфічних підприємств, насамперед тих, які здійснюють підготовку і промисловий випуск бланків документів суворого обліку та цінних паперів, є здійснення продуманої кадрової політики з

мінімізацією інформаційних втрат. Доцільним є розроблення положення про комерційну таємницю й конфіденційну інформацію, оскільки воно не вимагає якихось великих зусиль і витрат для створення, але є основою для правового захисту як комерційних таємниць поліграфічного підприємства, так і всієї його діяльності.

Для захисту економічних інтересів та інформації на поліграфічних підприємствах слід використовувати різні автоматизовані системи контролю й обмеження доступу, зокрема, зчитувачів і контролерів, електронних ключів і магнітних карт, які, незважаючи на свою простоту, забезпечують необхідний рівень захисту.

У зв'язку з тим, що значна частина важливої інформації у видавничо-поліграфічній галузі знаходиться в комп'ютерних мережах, потрібен захист від несанкціонованого використання. Відповідальність за забезпечення захисту інформації в системі покладається на її власника, який розробляє комплексну систему – взаємопов'язану сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації [6].

Додаткове оснащення поліграфічного підприємства системами відеоспостереження дозволяє забезпечити постійний контроль за ситуацією на території підприємства в режимі реального часу, у тому числі для віддалених користувачів (наприклад, керівників, з використанням інтернет-технологій). А така важлива функція, як цілодобовий запис і архівування відеоматеріалів, допоможе зібрати і зберегти незаперечні докази правопорушень, розкрадань на території підприємства.

Головними завданнями підсистеми інформаційного забезпечення процесу управління на поліграфічному підприємстві є: збір необхідної інформації; обробка і систематизація інформації; оцінка й аналіз інформації; прогнозування всіх аспектів діяльності підприємства; надання необхідної інформації особам, що приймають рішення. Завдяки наявності аналогічних даних про конкурентів або бізнес-партнерів легко проводити порівняльний аналіз забезпечення інформаційної та економічної безпеки власного бізнесу з іншими поліграфічними підприємствами; оцінювати свої відносні переваги та недоліки; порівнювати і компонувати свої можливості та можливості партнерів. Тому для забезпечення інформаційної безпеки підприємства в складі системи безпеки організовують підрозділи конкурентної (ділової) розвідки, контррозвідки та інформаційно-аналітичної служби. Кожна з цих служб виконує певні функції, які в сукупності характеризують процес створення та захисту інформаційної безпеки поліграфічного підприємства. До таких належать:

збирання інформації всіх видів щодо діяльності того чи того суб'єкта господарювання;

аналіз одержуваної інформації з обов'язковим дотриманням загальноприйнятих принципів методів організації робіт;

прогнозування тенденцій розвитку науково-технологічних, економічних і політичних процесів на підприємстві, у країні та світі для конкретної

сфери бізнесу, а також показників, яких необхідно досягти суб'єкту господарювання;

оцінка рівня економічної безпеки за кожною складовою окремо та в комплексі, розроблення рекомендацій щодо підвищення цього рівня на конкретному підприємстві;

інші види діяльності з розроблення інформаційної складової економічної безпеки (зв'язок з громадськістю, формування сприятливого іміджу фірми, захист конфіденційної інформації) [4].

Діагностику рівня інформаційної безпеки на поліграфічному підприємстві пропонується проводити за трьома ключовими напрямками – за оцінкою:

програмно-технічної захищеності інформації;

інформаційної надійності персоналу;

інформації, що надається особам, які приймають рішення, інформаційною службою підприємства.

Актуальність виділення запропонованих напрямків випливає з ключових завдань щодо забезпечення інформаційної безпеки підприємства, які покладені не лише на працівників відділу економічної безпеки, а й на кожного працівника в процесі виконання своїх безпосередніх обов'язків, зокрема:

забезпечення – програмно-технічного захисту від несанкціонованого доступу до закритої інформації, захисту від промислового шпигунства, безпеки підтримки зв'язків з контрагентами, а також організація збору, оцінки, обробки, систематизації та аналізу інформації, необхідної для забезпечення ефективного процесу управління підприємством [3].

Розглянувши особливості забезпечення інформаційної безпеки поліграфічних підприємств, нами доведено, що саме наявність розвиненої системи інформаційної безпеки є однією з найважливіших умов забезпечення їх конкурентоспроможності і навіть життєздатності. Тому, враховуючи це, запропоновано графічну схему кругообігу інформації на поліграфічному підприємстві (див. рисунок).

Захист інформаційного середовища підприємства передбачає:

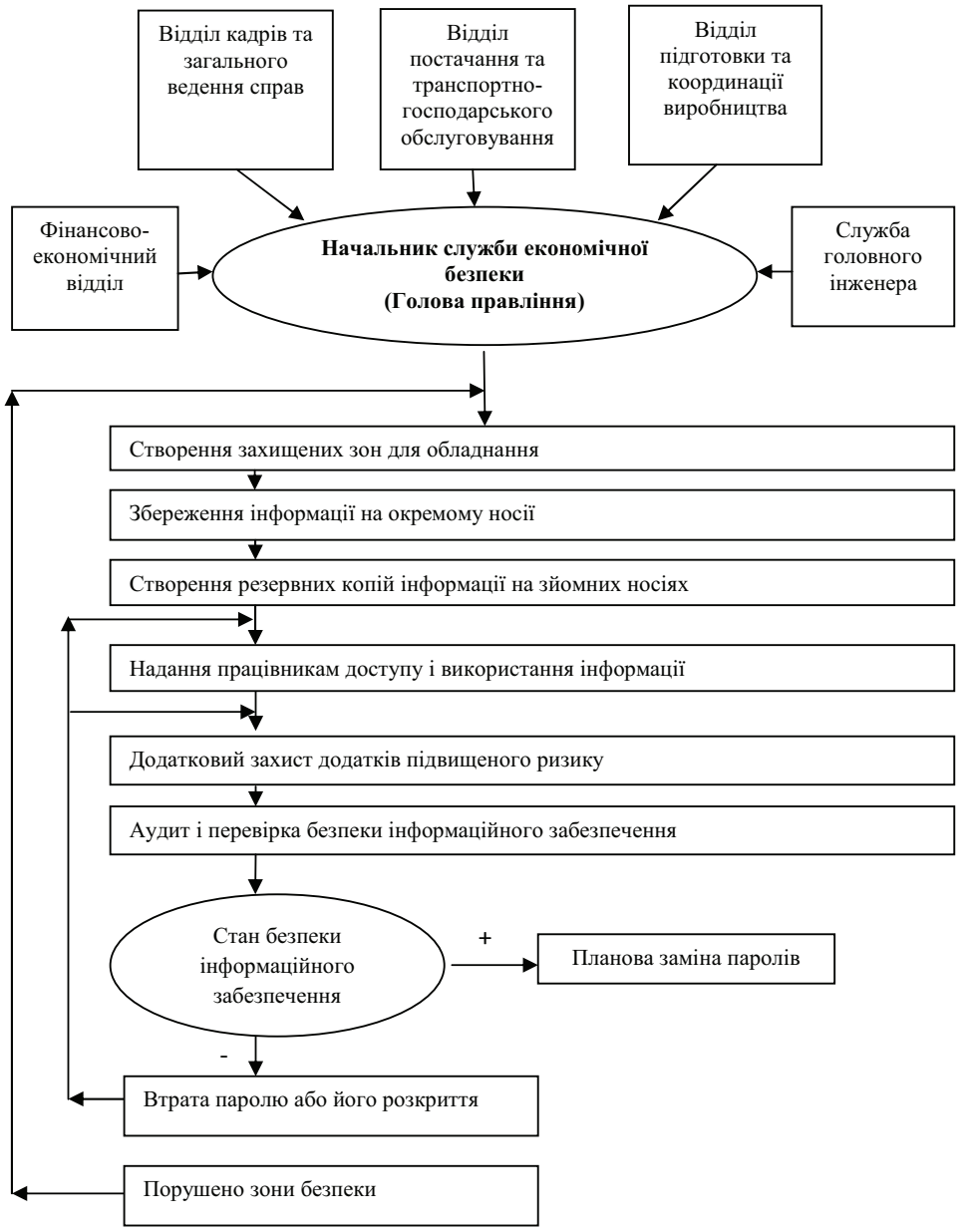
створення захисних зон для обладнання. Для цього забороняється використовувати неперевірені носії інформації, здійснюється захист обладнання від шкідливих програм, які можуть містити віруси, за допомогою антивірусних програм.

надходження інформації з підрозділів підприємства в електронному вигляді по внутрішній мережі на основний сервер, де створюються її резервні копії на зйомних носіях. Це дасть змогу у випадку знищення чи викрадення основного носія швидко відновити всю втрачену інформацію, користуватися інформацією з будь-якого комп'ютера внутрішньої мережі.

надання працівникам кодів і паролів доступу для використання інформації. Це гарантує, що інформацією може скористатися лише визначений користувач або коло користувачів. На програми, які мають підвищену вагу для підприємства, встановлюються додаткові ключі доступу.

аудит і перевірку безпеки інформаційного забезпечення. Це дозволяє перевірити безпеку системи, виявити небезпечні місця і ліквідувати їх.

планову заміну паролів доступу до інформації. Рекомендується щоквартально змінювати паролі, усі зміни повинні реєструватися в спеціальному журналі.



Графічна схема кругообігу інформації
на поліграфічному підприємстві

Слід зазначити, що створити абсолютну систему захисту принципово неможливо. При достатній кількості часу і засобів можна подолати будь-який захист. Тому має сенс вести мову тільки про деякий прийнятний рівень безпеки. Високоефективна система захисту має чималу вартість, використовує під час роботи істотну частину потужності й ресурсів комп'ютерної системи і може створювати відчутні додаткові незручності користувачам.

Часто доводиться створювати систему захисту в умовах великої невизначеності. Тому вжиті заходи і встановлені засоби захисту, особливо спочатку їх експлуатації, можуть забезпечувати як надмірний, так і недостатній рівень захисту. Природно, що для забезпечення можливості варіювання рівнів захищеності засоби захисту мають володіти визначеною гнучкістю. Особливо важливою ця властивість є в тих випадках, якщо установку засобів захисту необхідно здійснювати в працюючих системах, не порушуючи процесу її нормального функціонування.

Крім того, зовнішні умови і вимоги з часом змінюються. У таких ситуаціях виникає потреба в позбавленні користувачів інформації від вживання кардинальних заходів щодо повної заміни засобів захисту новими. Слід зазначити, що механізми захисту повинні бути інтуїтивно зрозумілими і простими у використанні, їхнє завдання полягає в наступному:

визначенні безпеки інформації;

виявленні потенційного порушника і можливих каналів просування інформації, яка потребує захисту;

виборі відповідних заходів, методів, механізмів і засобів захисту;

побудові замкненої, ефективної, комплексної системи захисту.

Дослідивши суть інформаційної безпеки та розглянувши процес її забезпечення на поліграфічному підприємстві, ми переконалися, що досягнення необхідного для розвитку рівня інформаційної безпека можливе лише при спільній взаємодії персоналу, програмно-апаратних засобів і засобів захисту інформації. Беручи за основу цю обставину, нами розроблено схему кругообігу інформації та сформовано засади реалізації механізму захисту інформації, що зумовить підвищення ефективності засобів захисту і зниження ризиків втрати і спотворення інформації.

1. Журавель М. Ю. Формування системи показників оцінки рівня інформаційної безпеки підприємства / М. Ю Журавель, Т. В. Полозова // Вісн. екон. транспорту і промисловості. – 2011. – № 33. – С. 171–177. 2. Ортинський Л. В. Економічна безпека підприємств, організацій та установ / В. Л. Ортинський, І. С. Керницький та ін. – К.: Правова єдність, 2009. – 544 с. 3. Полозова Т.В. Організаційне забезпечення складових економічної безпеки підприємства / Т.В. Полозова, М.Ю. Журавель // Економіка: проблеми теорії та практики: зб. наук. пр.: в 7 т. – Вип. 257; Т. ІІІ. – Д.: ДНУ, 2009. – С. 613–619. 4. Сороківська О. А. Інформаційна безпека підприємства: нові загрози та перспективи / О. А. Сороківська, В. Л. Гевко // Вісн. Хмельн. нац. ун-ту. – 2010. – № 2. – С. 32–35. 5. Степанова О. М. Інформаційна безпека в умовах розвитку інформаційної системи підприємства / О. М. Степанова, Л. М. Дегтярьова // Інформаційна безпека . – 2009. – №1. – С. 59–63. 6. Швайка Л. А. Економіка видавничо-поліграфічної галузі: підруч. / Л. А. Швайка, А. М. Штангрет. – Львів : Укр. акад. друкарства, 2008. – 480 с.

МЕТОДИЧЕСКИЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОЛИГРАФИЧЕСКОГО ПРЕДПРИЯТИЯ

Рассматриваются сущность информационной безопасности и процесс ее обеспечения. Сформирована схема круговорота информации и обоснованы принципы построения механизма защиты информации на полиграфическом предприятии.

METHODOLOGICAL BASIS FOR PROVIDING INFORMATION SAFETY OF PRINTING COMPANY

The article discusses the nature of information safety, the process of its software, the scheme of the circulation of information and reasonable basis for building protection mechanism for printing company.

Стаття надійшла 07.11.2013

УДК 65.012.8

Х.О. Турхан

Українська академія друкарства

МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ МАШИНОБУДІВНИХ ПІДПРИЄМСТВ

Обґрунтовано методичні засади формування ключових елементів механізму забезпечення фінансової безпеки машинобудівних підприємств та розглянуто їх суть.

Механізм, фінансова безпека підприємства, фінансові інтереси, важелі, принципи

За сучасних умов господарювання, коли ситуація в країні характеризується фінансово-економічною нестабільністю та більшість промислових підприємств є збитковими, актуальності набуває питання фінансової безпеки підприємств.

Попри те, що машинобудування є однією з провідних галузей промислової індустрії України, питома вага машинобудівних підприємств у виготовленні продукції промисловості упродовж останніх років мала нестабільний характер. Окрім того, у 2011–2013 рр. спостерігалося незначне зростання частки машинобудування, але цього недостатньо порівняно з розвинутими країнами світу, де цей відсоток становить 30–50%. Не можна оминути увагою і той факт, що, за даними Державної служби статистики України, за останні роки кількість збиткових машинобудівних підприємств перевищувала 30%. Усе це актуалізує важливість і пріоритетність розроблення та реалізації механізму забезпечення фінансової безпеки машинобудівних підприємств.