МЕНЕДЖМЕНТ

УДК 338:004.7.056
JEL L 86

Концептуальні засади забезпечення ефективного захисту інформації в контексті економічної безпеки підприємства

Печенюк А.В.

Подільський державний аграрно-технічний університет

E-mail: anvaspe@meta.ua

OPEN ACCESS

Печенюк А.В. Концептуальні засади забезпечення ефективного захисту інформації в контексті економічної безпеки підприємства. Економіка та управління АПК. 2020. № 1. С. 84–92.

Pechenjuk A.V. Konceptual'ni zasady zabezpechennja efektyvnogo zahystu informacii' v konteksti ekonomichnoi' bezpeky pidpryjemstva. Ekonomika ta upravlinnja APK. 2020. No 1. PP. 84–92.

Рукопис отримано: 27.03.2020р.
Прийнято: 09.04.2020р.
Затверджено до друку: 21.05.2020р.

doi: 10.33245/2310-9262-2020-155-1-84-92

Обґрунтовано необхідність формування ефективної системи інформаційної безпеки підприємства. Наголошується на тому, що за формування інформаційної політики фірма має дотримуватися вимог чинного законодавства, враховувати рівень технічного забезпечення, особливості регламентації доступу співробітників до конфіденційної інформації тощо. Зазначено, що витрати на організацію заходів по захисту інформації мають бути відповідними її цінності.

Виділено основні загрози, до яких може призвести порушення конфіденційності інформації, яка складає комерційну таємницю. Наведено перелік основних нормативно-правових актів, спрямованих на притягнення до цивільної, адміністративної та кримінальної відповідальності за незаконне збирання, розголошення та використання відомостей, що становлять комерційну таємницю. Узагальнено головні етапи побудови політики інформаційної безпеки, охарактеризовано найбільш розповсюджені види інформаційних загроз, пов'язаних з використанням сучасних комп'ютерних технологій.

Наголошено на необхідності розробки вітчизняної оригінальної бухгалтерської (управлінської) програми, яку у перспективі могла б використовувати переважна більшість українських підприємств.

Виділено три групи інструментів, які застосовують в теорії та практиці інформаційної безпеки підприємства (активні, пасивні та комбіновані), наголошено на необхідності планування та безперервного контролю в реальному часі всіх важливих процесів і станів, що впливають на безпеку даних.

Зазначено, що навіть якщо система інформаційної безпеки побудована з урахуванням усіх сучасних методів і засобів захисту, це не гарантує стовідоткового захисту інформаційних ресурсів підприємства, проте грамотно побудована політика інформаційної безпеки дозволяє мінімізувати відповідні ризики.

Ключові слова: захист інформації, інформаційна політика, інформаційна безпека, конфіденційна інформація, інформаційні загрози, інформаційно-комунікаційні технології, програмне забезпечення.

Постановка проблеми. На сьогодні інформація як ресурс користується значним попитом. Інформаційна інфраструктура та сучасні інформаційні технології кардинально змінюють повсякденну діяльність мільйонів підприємств. Динамічне зростання кількості злочинів у економічній та інформаційній сферах, стрімке поширення систем електронного документообігу, поява глобальних баз даних (зокрема – персональної та комерційної інформації) потребують побудови надійної системи інформаційного захисту суб'єктів господарювання.

Україна все частіше стикається з масштабними проявами інформаційної злочинності, що загрожують сталому та безпечному функціону-

ванню інформаційно-телекомунікаційних систем. Про високий рівень загроз у кібернетичному просторі України свідчать, наприклад, результати дослідження відомого німецького оператора зв'язку Deutsche Telecom, згідно з якими наша країна опинилася на четвертій сходинці світового рейтингу серед країн – об'єктів і джерел кібернетичних атак [1, с. 26].

До основних завдань системи інформаційної безпеки сучасного підприємства можна віднести: захист законних інтересів фірми від протиправних посягань на конфіденційну інформацію, запобігання розголошенню, втратам, витоку, спотворенню та знищенню службової інформації. Система інформаційної безпеки має сприяти підвищенню якості послуг, що надаються підприємством, і гарантувати безпеку майнових прав та інтересів клієнтів [2, с. 131].

Тому особливо актуальною є систематизація концептуальних основ формування інформаційної політики підприємств, спроможної забезпечити генерування, поширення, ефективне використання та захист інформаційних потоків і ресурсів. Організація ефективної інформаційної безпеки є одним з найголовніших завдань, яке має бути вирішене за побудови інформаційної системи сучасного підприємства.

Аналіз останніх досліджень та публікацій. У 1992 році Верховною Радою України прийнято Закон «Про інформацію» [3], у 2014 – Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [4]. Із липня 2003 р. в Україні введена кримінальна відповідальність за незаконне втручання в роботу комп'ютерів і комп'ютерних мереж, а також за поширення комп'ютерних вірусів, що призвело до спотворення, зникнення, блокування інформації чи її носіїв. З метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, суб'єктів господарювання в Україні затверджена та введена в дію Указом Президента України від 15 березня 2016 року № 96/2016 «Стратегія кібербезпеки України» [5].

Зміна умов зовнішнього середовища, вплив внутрішніх і зовнішніх чинників посилюють необхідність удосконалення методів управління інформаційною безпекою підприємства, формування ефективної системи інформаційної безпеки, оцінки рівня інформаційної безпеки підприємства.

Особливості побудови ефективної інформаційної системи підприємства досліджено Батюком А.Є., Двулітом З.П., Обельовською К.М., концептуальні основи формування інформаційної політики узагальнено Гудзем О.Є., Маковійом В.В., проблеми побудови ефективної моделі інформаційної безпеки проаналізовано у працях Нікітина Г.Д., Мезенцевої К.О., Мельника М.О., технологічні особливості формування інструментарію інформаційної безпеки підприємства представлено в публікаціях Захарченка М.В., Кільдішева В.Й., Кононовича В.Г., методичне забезпечення процесу захисту інформації досліджено Верескуном М.В., проблеми захисту конфіденційної інформації проаналізовано Головаенем С.М., Сенченком Є., Сісецькою А., особливості забезпечення інформаційної безпеки корпоративної економіки в умовах глобалізаційних процесів розкрито Валіулліною З.В., Убийвовком І.І.

Незважаючи на наявність важливих рекомендацій та настанов провідних науковців щодо забезпечення інформаційної безпеки підприємства, проблема формування цілісної системи забезпечення ефективного захисту конфіденційної інформації суб'єктів господарювання залишається недостатньо дослідженою.

Метою дослідження стало узагальнення концептуальних засад забезпечення ефективного захисту інформації та розробка пропозицій щодо підвищення ефективності інформаційної безпеки сучасного підприємства.

Матеріал і методи дослідження. Теоретичною базою дослідження стали праці фахівців у галузі інформаційної безпеки підприємства, фундаментальні положення загальної економічної теорії. Для досягнення поставленої мети було використано як емпіричні (спостереження, порівняння, моделювання) так і теоретичні методи дослідження (аналіз і синтез, аналогія, формалізація та абстрагування).

Результати дослідження та обговорення. Стрімке впровадження інформаційних технологій у всі сфери життєдіяльності суспільства в умовах глобалізаційних процесів актуалізує проблему визначення обґрунтованих та ефективних шляхів забезпечення інформаційної безпеки. Налагоджена інформаційна політика підприємства визначає ефективність дій менеджменту, а отже обсяг, достовірність, цілісність, якість обробки інформації актуалізують застосування інформаційних технологій в управлінні грошово-кредитними, фінансовими, соціально-економічними процесами суб'єкта господарювання [6, с. 36].

Інформаційна діяльність будь-якого вітчизняного суб'єкта господарювання здійснюється згідно з вимогами законодавства України та статутам підприємства як внутрішня програма, що окреслює основні принципи комунікації і формування інформаційного

простору фірми та забезпечує необхідну конфіденційність, безпеку й підвищення іміджу підприємства. Під час формування інформаційної політики необхідно враховувати всі аспекти діяльності підприємства, починаючи з інформаційно-комунікаційних можливостей, регламентації доступу співробітників до конфіденційної інформації та закінчуючи системою безпеки й взаємодії з усіма контрагентами [7, с. 67].

Канали реалізації інформаційної політики мають забезпечувати рівноправний, своєчасний і не пов'язаний із надмірними витратами доступ користувачів до необхідної інформації [8, с. 15].

Під захистом інформації розуміють, зазвичай, сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Охорона відомостей, що становлять комерційну таємницю, є надчутливим аспектом діяльності будь-якого суб'єкта господарювання. Особливо це стосується захисту комерційної таємниці від несанкціонованого доступу конкурентів до неї. Комерційна таємниця у руках конкурентів – це своєрідний ключ, за допомогою якого можна отримати ряд переваг у конкуренції на відповідному ринку, які неможливо було б отримати завдяки власним досягненням, або ж навіть витіснити законного власника таких відомостей з ринку. Чинне законодавство України спрямоване на запобігання виникненню таких ситуацій, передбачаючи цивільну, адміністративну і кримінальну відповідальність за незаконне збирання, розголошення та використання відомостей, що становлять комерційну таємницю [9].

Аналіз звітів корпорації Gartner свідчить про те, що витрати на інформаційну безпеку у світі щорічно зростають приблизно на 8,2 %, і у 2020 році їх обсяг сягне 170 млрд дол. США [1, с. 27].

Головна умова інформаційної безпеки підприємства – здатність протистояти існуючим і потенційним небезпекам та загрозам, які завдають (можуть завдати) фінансову шкоду підприємству або спрямовані на небажану зміну структури капіталу, примусову ліквідацію фірми тощо.

Сьогодні значна частина інформації може бути отримана з відкритих джерел без порушення етичних норм. Система побудови інформаційної безпеки кожного підприємства цілком індивідуальна. Її ефективність значною мірою залежать від наявної в державі законодавчої бази, від обсягу ресурсів, виділених адміністрацією підприємства, від усвідомлення співробітниками важливості забезпечення безпеки бізнесу [10, с. 128].

Сучасне підприємство має вміти належним чином будувати політику інформаційної безпеки, тобто розробляти і ефективно впроваджувати комплекс превентивних заходів по захисту конфіденційних даних та інформаційних процесів. Така політика передбачає відповідні вимоги на адресу персоналу, менеджерів і технічних служб.

Сферу політики інформаційної безпеки сучасного підприємства можна поділити на дві складові. Перша – загальні принципи роботи з інформаційними ресурсами (базами даних) для кожної із категорій користувачів. Друга – чітко визначені правила такої роботи. Під час побудови політики інформаційної безпеки потрібно розуміти, що вона завжди буде компромісом між рівнем захищеності інформаційних ресурсів системи, який ми бажаємо отримати, тим, наскільки зручно користувачам буде працювати із системою і, звичайно тими витратами коштів, що необхідні для її експлуатації [11, с. 126].

Головними етапами побудови політики інформаційної безпеки є:

1) реєстрація всіх ресурсів, які мають бути захищені;

2) аналіз та створення переліку можливих загроз для кожного ресурсу;

3) оцінка ймовірності появи кожної загрози;

4) вжиття заходів, які дозволяють економічно ефективно захистити інформаційну систему [12, с. 167].

Усю інформацію можна поділити на дві великі групи: відкриту й підлягаючу захисту (закриту або інформацію з обмеженим доступом (ІОД)). Про відкриту інформацію вести мову з погляду її захисту немає сенсу, оскільки вона є загальнодоступною.

Дослідження показують, що аналіз доступних матеріалів дає до 95 % цінної інформації про конкурента і його технологічні нововведення, інші 5 % містять секрет фірми та можуть бути отримані зловмисником за допомогою нелегальних дій. Доступ до документованої, службової інформації ґрунтується на нелегальних діях і на несанкціонованому доступі до інформації. Нелегальні дії можуть передбачати злодійство, навмисний обман, хабарництво, використання слабкості або хворобливого стану співробітника, шантаж співробітників, використання екстремальних ситуацій тощо [13, с. 183].

Найбільш розповсюджені види інформаційних загроз, пов'язаних з використанням сучасних комп'ютерних технологій:

– шкодочинне програмне забезпечення;

– інтернет-шахрайство;

– несанкціонований доступ до інформаційних ресурсів та інформаційно-телекомунікаційних систем;

– логічні бомби (набори команд, що записуються в програму і спрацьовують за певних умов;

– «троянські коні» (програми, що виконують певні дії без відома власника зараженої системи, наприклад, – відсилають за певною адресою конфіденційну інформацію);

– різні види атак, що дозволяють проникнути в мережу або перехопити управління нею;

– крадіжка коштів;

– засоби пригальмовування обміну даними в мережі;

– природні катаклізми [14].

Яскравим прикладом загроз і викликів для інформаційної безпеки вітчизняних суб'єктів господарювання є програмні продукти «1С», які впроваджує, реалізує та супроводжує російська франчайзингова компанія «1С». Адже в Україні понад 130 тисяч підприємств використовують систему програм «1С: Підприємство», особливістю якої є той факт, що код платформи є закритим і без участі розробника (ПАТ «1С») рішення всіх технічних питань виявляється непростим. Це дає можливість здійснювати пильний контроль з боку іноземного розробника програмних продуктів за всіма аспектами облікової діяльності українських суб'єктів підприємництва.

Аналогічні інформаційні ризики пов'язані і з використанням програмного комплексу «Парус», який використовується в Україні значною кількістю бюджетних установ, тобто розробник може мати прямий інформаційний доступ до державних бюджетних показників [1, с. 28].

Слід зазначити, що українські ІТ-фахівці спроможні розробити вітчизняну оригінальну бухгалтерську (управлінську) програму. Для цього потрібне створення належних умов, а саме: встановлення державного замовлення на розробку відповідної бухгалтерської (управлінської) програми і заборона на використання іноземного програмного забезпечення контролюючими фіскальними органами.

Фірми-конкуренти можуть уживати такі незаконні способи одержання конфіденційної інформації:

– регулярне візуальне спостереження приміщень фірми, роботи персоналу;

– прослуховування приміщень фірми, розмов співробітників у неслужбовій обстановці;

– імітовані переговори щодо ділового співробітництва й одержання цінної інформації у процесі переговорів;

– перехоплення інформації, яка циркулює в технічних каналах поширення інформації;

– аналіз відходів виробництва, огляд сміття тощо [13, с. 184].

Організація ефективного захисту інформаційної системи сучасного підприємства залежить від:

– рівня секретності та властивостей інформації, яка підлягає захисту;

– конкретної технології обробки інформації;

– технічних і програмних засобів, що використовуються підприємством;

– місця розташування підприємства;

– специфіки діяльності тощо [15, с. 237].

Необхідно також відзначити, що рівень загроз і, відповідно рівень інформаційної безпеки промислового підприємства, постійно змінюються під дією різних чинників. Найбільш впливовими з них є наступні:

– розширення співпраці підприємства з партнерами;

– автоматизація бізнес-процесів на підприємстві;

– розширення кооперації виконавців за побудови і розвитку інформаційної інфраструктури підприємства;

– зростання обсягів інформації підприємства, яка передається по відкритих каналах зв'язку;

– зростання кількості комп'ютерних злочинів [16, с. 57].

У теорії та практиці інформаційної безпеки підприємства виділяють такі три групи інструментів: активні засоби захисту (розвідка, дезінформація тощо); пасивні засоби (встановлення екранів проти несанкціонованого витоку інформації тощо); комплекс засобів підтримки – органічне поєднання попередньо вказаних груп щодо моделювання потенційних (невідомих раніше практиці) загроз [10, с. 130].

Під час розробки системи інформаційної безпеки слід донести до всіх співробітників основні, базові правила поводження з інформацією з урахуванням того, що більшість робочих питань на сьогодні вирішується за допомогою комп'ютерів та мобільних гаджетів [17].

Повноцінна інформаційна безпека підприємства передбачає безперервний контроль в реальному часі всіх важливих процесів і станів, що впливають на безпеку даних. Захист має здійснюватися цілодобово та охоплювати увесь життєвий цикл інформації – від моменту її надходження або створення до моменту знищення або втрати актуальності [16, с. 59].

Політика безпеки, окрім правил розмежовування доступу, встановлює правила керування. Функції керування покладаються на

довірених осіб, які несуть відповідальність за безпеку опрацьовуваної інформації. Цих осіб називають, здебільшого, адміністраторами комп'ютерних систем [18, с. 124].

Можна виділити такі основні групи засобів протидії загрозам інформаційній безпеці:

– правові або законодавчі (законодавчо-права база, нормативні документи Державної служби спеціального зв'язку та захисту інформації);

– морально-етичні (дотримання норм поведінки, що складаються в інформаційному суспільстві країни);

– організаційні або адміністративні (регламентують процес функціонування системи обробки даних, використання її ресурсів, діяльність персоналу, а також порядок взаємодії користувачів із системою);

– фізичні (ґрунтуються на використанні механічних, електро- або електронно-механічних пристроїв, призначених для створення фізичних перешкод на можливих шляхах проникнення потенційних порушників, їх доступу до компонентів системи та інформації, що захищається, а також засоби візуального спостереження, зв'язку і охоронної сигналізації);

– технічні (використання різних електронних пристроїв і спеціального програмного забезпечення) [15, с. 291].

Зазвичай, кожне сучасне підприємство регламентує правила роботи з інформацією. Політика безпеки інформації є складовою частиною загальної політики безпеки фірми. Необхідною у сучасних умовах є розробка переліку вимог, загроз та оцінювання ризиків і описання створеного комплексу заходів протидії інформаційним загрозам [18, с. 137].

Для побудови ефективної системи захисту інформації, підприємство має дати відповіді на питання:

– які інформаційні ресурси підлягають захисту;

– яке програмне забезпечення можна використовувати на службових комп'ютерах;

– дисциплінарні стягнення і загальні вказівки про проведення службових розслідувань;

– на кого поширюються правила;

– хто розробляє загальні вказівки;

– хто має право змінювати вказівки;

– точний опис повноважень та привілеїв посадових осіб;

– хто може надавати повноваження та привілеї;

– порядок надання і позбавлення привілеїв у галузі інформаційної безпеки;

– повнота і порядок звітності про порушення безпеки та злочинної діяльності;

– особливі обов'язки керівництва і службовців щодо забезпечення інформаційної безпеки;

– дати введення в дію та перегляду;

– хто і яким чином ввів в дію ці правила [19].

Відповідно до Інструкції з безпеки систем RFC 2196 «Site Security Handbook» (RFC – Request for Comment) виділять чотири основні етапи побудови політики інформаційної безпеки:

1) реєстрація всіх ресурсів, які підлягають захисту;

2) аналіз і створення переліку потенційних загроз для кожного ресурсу;

3) оцінка ймовірності появи кожної загрози;

4) прийняття рішень, які дозволяють ефективно захистити інформаційну систему [20, с. 351].

Для підвищення рівня інформаційної безпеки підприємства доцільно запровадити процес планування заходів щодо забезпечення технічного захисту конфіденційної інформації. Такий план має розроблятися на підставі технології обробки конфіденційної інформації, аналізу ризиків, сформульованої політики її безпеки. План визначає основні завдання захисту, загальні правила обробки конфіденційної інформації в інформаційній системі, мету побудови та функціонування комплексної системи захисту конфіденційної інформації. План забезпечення технічного захисту конфіденційної інформації на всіх етапах її життєвого циклу може переглядатися та за необхідності змінюватися [14].

Для підвищення ефективності технічного захисту інформації на підприємстві слід реалізувати відповідний комплекс заходів:

1) здійснити аналіз об'єктів, умов функціонування фірми, оцінити ймовірність прояву загроз та очікувану шкоду від їх реалізації, підготувати дані для побудови окремої моделі загроз;

2) розробити план технічного захисту конфіденційної інформації;

3) реалізувати організаційні, первинні технічні та основні технічні заходи захисту конфіденційної інформації, установити необхідні зони безпеки інформації, провести атестацію технічних засобів забезпечення інформаційної діяльності, робочих місць (приміщень) на відповідність вимогам безпеки інформації;

4) провести аналіз функціонування системи захисту конфіденційної інформації, перевірку виконання заходів технічного захисту конфіденційної інформації, контроль ефективності захисту, підготувати та видати дані для

керування системою захисту конфіденційною інформацією.

Для мінімізації ризиків, пов'язаних з інформаційною безпекою, менеджмент сучасного підприємства має:

– користуватися ефективним повноцінним антивірусним програмним забезпеченням та регулярно оновлювати бази даних сигнатур вірусів;

– застосовувати програмний міжмережний екран (брандмауер) та штатні засоби захисту від шкідливого програмного забезпечення;

– забезпечити резервне копіювання даних шляхом їх збереження на знімних носіях інформації (CD/DVD, HDD тощо), відділених серверах;

– дотримуватись вимог сучасної методики створення паролів, забезпечувати їх регулярну зміну;

– не зберігати аутентифікаційні дані в легкодоступних місцях;

– уважно відстежувати прояви Інтернет-шахрайства;

– за користування Інтернет-ресурсами (соціальні мережі, системи обміну повідомленнями, новини, онлайн-ігри) не переходити по невідомих посиланнях та не завантажувати файли, що мають потенційно небезпечне розширення (наприклад, .exe, .bin, .ini, .dll, .com, .sys, .bat тощо);

– за під'єднання змінних носіїв інформації забезпечувати їх автоматичну перевірку на наявність шкодочинного програмного забезпечення;

– регулярно підвищувати рівень обізнаності з питань безпечного використання інформаційних технологій та протидії інформаційним загрозам, для реалізації яких використовується «людський чинник» (соціальна інженерія, Інтернет-шахрайство) [14].

Слід розуміти, що навіть якщо система інформаційної безпеки побудована з урахуванням усіх сучасних методів і засобів захисту, а підприємство має ретельно підібраний та кваліфікований персонал, це не гарантує стовідсоткового захисту інформаційних ресурсів підприємства: жодна система захисту не може довгий час протистояти цілеспрямованим діям озброєного сучасними технологіями кваліфікованого порушника.

Проте грамотно побудована політика інформаційної безпеки дозволяє мінімізувати відповідні ризики. В теперішніх умовах таку політику треба постійно підтримувати: контролювати, модернізувати, оновлювати.

Висновки. Однозначної відповіді на питання, як забезпечити повноцінний захист інформаційної системи, не існує. Це пов'язано з наявністю низки чинників впливу на прийняття того чи іншого рішення: специфіка діяльності, політика безпеки, фінансові можливості, технічна підготовка персоналу тощо.

Водночас безпека інформаційної системи має розглядатися як важлива складова загальної безпеки підприємства. Причому необхідна розробка концепції інформаційної безпеки, в якій слід передбачити не тільки заходи, пов'язані з інформаційними технологіями (криптозахист, програмні засоби адміністрування прав користувачів, їх ідентифікації та автентифікації, брандмауери для захисту входів-виходів мережі тощо), але й відповідні заходи адміністративного та технічного змісту.

У статті представлено пропозиції з запровадження на підприємстві ефективного процесу планування заходів щодо забезпечення технічного захисту конфіденційної інформації, доведено необхідність регулярного моніторингу інформаційних загроз, наголошується на доцільності застосування комплексного підходу до організації інформаційної безпеки.

Перспективним напрямом подальших досліджень є розробка комплексу заходів з формування належної інформаційної культури управлінського персоналу, що дозволить підвищити ефективність інформаційної діяльності сучасного підприємства.

СПИСОК ЛІТЕРАТУРИ

1. Микитенко Т.В., Петровська І.О., Рогов П.Д. Проблеми інформаційної безпеки суб'єктів господарювання в Україні та можливі шляхи їх вирішення в сучасних умовах. Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2014. №1. С. 24–31. URL: http://journals.uran.ua/index.php/2304-2699/article/view/126694

2. Печенюк А.В. Проблеми організації ефективного захисту інформації. Бухгалтерський облік, контроль та аналіз в умовах інституціональних змін та сталого економічного розвитку: матеріали II міжнар. наук.-практ. інтернет-конф. 25 листопада 2015 р. Тернопіль: Крок, 2015. С. 129–133.

3. Про інформацію: Закон України від 21.12.2019. URL: https://zakon.rada.gov.ua/laws/ show/2657-12.

4. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

5. Про рішення Ради національної безпеки і оборони України. Про Стратегію кібербезпеки України: Укази Президента України від 27 січня 2016 року. URL: https://zakon5.rada.gov.ua/laws/show/96/2016.

6. Валіулліна З.В. Інформаційна безпека корпоративної економіки в умовах глобалізаційних процесів. Вісник Дніпропетровського університету. Серія: Менеджмент інновацій. 2016. Вип. 6. С. 34–43. URL: https://www.ssoar.info/ssoar/bitstream/handle/document/62126/ssoar-ejmi-2016-6-valiullina-.pdf?sequence=1.

7. Гудзь О.Є., Маковій В.В. Концептуальні основи формування інформаційної політики підприємств. Науковий вісник Ужгородського національного університету. 2019. Вип. 23. С. 65–69. URL: http://dspace.msu.edu.ua:8080/jspui/bitstream/123456789/3222/1/%D0%9DEHEDOSH_COMPONENTS_LOGISTICS.PDF.pdf.

8. Pecheniuk A. Problems of building of effective information security of the enterprise. Problems and achievements of modern science: coll. of scientific papers «ΛΟΓΟΣ» with materials of the International scientific-practical conf., Cork, May 6, 2019. Cork: NGO «European Scientific Platform», 2019. Vol. 6. P. 14–16.

9. Сісецька А., Сенченко Є. Антимонопольний комітет України на захисті комерційної таємниці. URL: https://vkp.ua/publication/antimonopolnyy_komitet_ukrainy_na_zaschite_ kommercheskoy_tayny.

10. Убийвовк І.І. Інформаційна безпека діяльності підприємств. Причорноморські економічні студії. 2016. № 9(2). С. 126–131. URL: http://bses.in.ua/journals/2016/9-2-2016/29.pdf.

11. Мельник М.О., Нікітин Г.Д., Мезенцева К.О. Аналіз побудови моделі політики інформаційної безпеки підприємства. Системи обробки інформації. 2017. Вип. 2(148). С. 126–128. URL: http://www.hups.mil.gov.ua/periodic-app/article/17407.

12. Печенюк А.В. Особливості організації інформаційної безпеки сучасного підприємства. Інститут бухгалтерського обліку, контроль та аналіз в умовах глобалізації: міжнар. зб. наук. праць. Вип. 2. Тернопіль: Крок. 2014. С. 165–168. URL: http://ibo.tneu.edu.ua/index.php/ibo/article/view/124/123.

13. Кавун С.В., Пилипенко А.А., Ріпка Д.О. Економічна та інформаційна безпека підприємств у системі консолідованої інформації: навч. посіб. Харків: ХНЕУ, 2013. 364 с. URL: http://www.repository.hneu.edu.ua/bitstream.

14. Базовий курс з інформаційної безпеки. URL: http://cert.gov.ua/pdf/Брошура-CERT-UA-Інформаційна-безпека.pdf.

15. Остапов С.Е., Євсеєв С.П., Король О.Г. Технології захисту інформації: навч. посіб. Харків: ХНЕУ, 2013. 476 с. URL: https://www.twirpx.com/file/2340575/

16. Верескун М.В. Методичне забезпечення системи інформаційної безпеки промислових підприємств. Економіка і організація управління. 2014. № 1 (17). С. 54–60.

17. Базові правила інформаційної безпеки на підприємстві. URL: https://uk-winner.com/basic-rules-of-information-security-at-the-enterprise.

18. Захарченко М.В., Кононович В.Г., Кільдішев В.Й. Інформаційна безпека інформаційно-комунікаційних систем. Комплекси засобів захисту інформації від НСД. Одеса: ОНАЗ ім. О.С. Попова, 2011. 168 с.

19. Кузьменко Б.В. Захист інформації. Організаційно-правові засоби забезпечення інформаційної безпеки. URL: http://itman.at.ua/news/kuzmenko_b_v_chajkovska_o_a_ zakhist_informaciji_navchalnij_posibnik_ch_1_organizacijno_pravovi_zasobi_zabezpechennja_informacijnoji/2011-03-25-5.

20. Батюк А.Є., Двуліт З.П., Обельовська К.М. Інформаційні системи в менеджменті. Львів: Національний університет «Львівська політехніка», «Інтелект–Захід», 2004. С. 343–380.

21. Головань С.М. Захист конфіденційної інформації в організації. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/26513/05-Golovan.pdf?sequence=1.

REFERENCES

1. Mykytenko, T.V., Petrovska, I.O., Rohov, P.D. (2014). Problemy informatsiinoi bezpeky subiektiv hospodariuvannia v Ukraini ta mozhlyvi shliakhy yikh vyrishennia v suchasnykh umovakh [Problems of informative safety of subjects of menage in Ukraine and possible ways of their decision are in modern terms]. Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen Natsionalnoho universytetu oborony Ukrainy imeni Ivana Cherniakhovskoho [Collection of scientific works of Center of military-strategic researches of the National university of defensive of Ukraine of the name of Ivan Cherniakhovskii], no 1, pp. 24–31. Available at: http://journals.uran.ua/index.php/2304-2699/article/view/126694

2. Pecheniuk, A.V. (2015). Problemy orhanizatsii efektyvnoho zakhystu informatsii [Problems of organization of effective protection of information]. Bukhhalterskyi oblik, kontrol ta analiz v umovakh instytutsionalnykh zmin ta staloho ekonomichnoho rozvytku [Accounting, control and analysis in the face of institutional change and sustainable economic development]: materialy II mizhnar. nauk.-prakt. internet-konf. 25 lystopada 2015 r. Ternopil: Krok, pp. 129–133.

3. Pro informatsiiu: Zakon Ukrainy [On Information]. Law of Ukraine. Available at: https://zakon.rada.gov.ua/laws/show/2657-12.

4. Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemak: Zakon Ukrainy [On Information Protection in Information and Telecommunication Systems]. Law of Ukraine. Available at: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

5. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku. Pro Stratehiiu kiberbezpeky Ukrainy Ukaz Prezydenta Ukrainy. [On the Decision of the National Security and Defense Council of Ukraine of January 27, 2016. On the Cybersecurity Strategy of Ukraine]. Presidential Decree. Available at: https://zakon5.rada.gov.ua/laws/show/96/2016.

6. Valiullina, Z.V. (2016). Informatsiina bezpeka korporatyvnoi ekonomiky v umovakh hlobalizatsiinykh protsesiv [Information security of corporate economy in the conditions of globalization processes]. Visnyk Dnipropetrovskoho universytetu [Bulletin of Dnipropetrovsk University], no. 6. pp. 34–43. Available at: https://www.ssoar.info/ssoar/bitstream/handle/document/62126/ssoar-ejmi-2016-6-valiullina-.pdf?sequence=1.

7. Hudz, O.Ie., Makovii, V.V. (2019). Kontseptualni osnovy formuvannia informatsiinoi polityky pidpryiemstv [Conceptual bases of formation of information policy of the enterprises]. Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu [Scientific Bulletin of Uzhgorod National University], no. 23, pp. 65–69. Available at: http://dspace.msu.edu.ua:8080/ jspui/bitstream/123456789/3222/1/%D0%9DEHEDOSH_COMPONENTS_LOGISTICS.PDF.pdf

8. Pecheniuk, A. (2019). Problems of building of effective information security of the enterprise. Problems and achievements of modern science: coll. of scientific papers «ΛΟΗΟΣ» with materials of the International scientific-practical conf., Cork, May 6, 2019. Cork: NGO «European Scientific Platform», no. 6, pp. 14–16.

9. Sisetska, A., Senchenko, Ye. Antymonopolnyi komitet Ukrainy na zakhysti komertsiinoi taiemnytsi [Antimonopoly Committee of Ukraine for the Protection of Trade Secrets]. Available at: https://vkp.ua/publication/antimonopolnyy_komitet_ukrainy_na_zaschite_kommercheskoy_tayny.

10. Ubyivovk, I.I. (2016). Informatsiina bezpeka diialnosti pidpryiemstv [Information security of activity of enterprises]. Prychornomorski ekonomichni studii [Black Sea Economic Studies], no 9(2), pp. 126–131. Available at: http://bses.in.ua/journals/2016/9-2-2016/29.pdf

11. Melnyk, M.O., Nikityn, H.D., Mezentseva, K.O. (2017). Analiz pobudovy modeli polityky informatsiinoi bezpeky pidpryiemstva [Analysis of building a model of enterprise information security policy]. Systemy obrobky informatsii [Information processing systems], no. 2(148), pp. 126–128. Available at: http://www.hups.mil.gov.ua/periodic-app/article/17407

12. Pecheniuk, A.V. (2014). Osoblyvosti orhanizatsii informatsiinoi bezpeky suchasnoho pidpryiemstva [Features of organization of information security of the modern enterprise]. Instytut bukhhalterskoho obliku, kontrol ta analiz v umovakh hlobalizatsii [Institute of accounting, control and analysis in the conditions of globalization]: mizhnar. zb. nauk. Prats. Ternopil: Krok, no 2, pp. 165–168. Available at: http://ibo.tneu.edu.ua/index.php/ibo/article/view/124/123.

13. Kavun, S.V., Pylypenko, A.A., Ripka, D.O. (2013). Ekonomichna ta informatsiina bezpeka pidpryiemstv u systemi konsolidovanoi informatsii [Economic and information security of enterprises in the system of consolidated information]. Kharkiv: KhNEU. 364 p. Available at: http://www.repository.hneu.edu.ua/bitstream.

14. Bazovyi kurs z informatsiinoi bezpeky [Basic Information Security Course]. Available at: http://cert.gov.ua/pdf/Broshura-CERT-UA-Informatsiina-bezpeka.pdf.

15. Ostapov, S.E., Yevseiev, S.P., Korol, O.H. (2013). Tekhnolohii zakhystu informatsii: navchalnyi posibnyk [Information security technologies: a textbook]. Kharkiv: KhNEU. 476 p. Available at: https://www.twirpx.com/file/2340575/.

16. Vereskun, M.V. (2014). Metodychne zabezpechennia systemy informatsiinoi bezpeky promyslovykh pidpryiemstv [Methodical provision of information security system of industrial enterprises]. Ekonomika i orhanizatsiia upravlinnia [Economics and management organization], no 1(17), pp. 54–60.

17. Bazovi pravyla informatsiinoi bezpeky na pidpryiemstvi [Basic rules of information security at the enterprise]. Available at: https://uk-winner.com/basic-rules-of-information-security-at-the-enterprise.

18. Zakharchenko, M.V., Kononovych, V.H., Kildishev, V.I. (2011). Informatsiina bezpeka informatsiino-komunikatsiinykh system [Information security of information and communication systems]. Kompleksy zasobiv zakhystu informatsii vid NSD [Information security complexes]. Odesa: ONAZ im. O.S. Popova. 168 p.

19. Kuzmenko, B.V. Zakhyst informatsii. Orhanizatsiino-pravovi zasoby zabezpechennia informatsiinoi bezpeky [Protection of information. Organizational and legal means of ensuring information security]. Available at: http://itman.at.ua/news/kuzmenko_b_v_chajkovska_o_a_zakhist_informaciji_navchalnij_posibnik_ch_1_organizacijno_pravovi_zasobi_zabezpechennja_informacijnoji/2011-03-25-5.

20. Batiuk, A.Ie., Dvulit, Z.P., Obelovska, K.M. (2004). Informatsiini systemy v menedzhmenti [Information systems in management]. Lviv: Natsionalnyi universytet «Lvivska politekhnika», «Intelekt-Zakhid», pp. 343–380.

21. Holovan, S.M. Zakhyst konfidentsiinoi informatsii v orhanizatsii [Protecting sensitive information in an organization]. Available at: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/26513/05-Golovan.pdf?sequence=1.

Концептуальные основы обеспечения эффективной защиты информации в контексте экономической безопасности предприятия

Печенюк А.В.

Обоснована необходимость формирования эффективной системы информационной безопасности предприятия. Подчеркивается, что при формировании информационной политики фирма должна соблюдать требования действующего законодательства, учитывать уровень технического обеспечения, особенности регламентации доступа сотрудников к конфиденциальной информации. Указано, что расходы на организацию мероприятий по защите информации должны соответствовать ее ценности.

Указаны основные угрозы, к которым может привести нарушение конфиденциальности информации, составляющей коммерческую тайну. Приведен перечень основных нормативно-правовых актов, направленных на привлечение к гражданской, административной и уголовной ответственности за незаконный сбор, разглашение и использование сведений, составляющих коммерческую тайну. Обобщено главные этапы построения политики информационной безопасности, охарактеризованы наиболее распространенные виды информационных угроз, связанных с использованием современных компьютерных технологий.

Указано на необходимость разработки отечественной оригинальной бухгалтерской (управленческой) программы, которая в перспективе могла бы использоваться подавляющим большинством украинских предприятий.

Выделены три группы инструментов, применяемых в теории и практике информационной безопасности предприятия (активные, пассивные и комбинированные), отмечена необходимость планирования и непрерывного контроля в реальном времени всех важных процессов и состояний, влияющих на безопасность данных.

Отмечено, что даже если система информационной безопасности построена с учетом всех современных методов и средств защиты, это не гарантирует стопроцентной защиты информационных ресурсов предприятия, однако грамотно построена политика информационной безопасности позволяет минимизировать соответствующие риски.

Ключевые слова: защита информации, информационная политика, информационная безопасность, конфиденциальная информация, информационные угрозы, информационно-коммуникационные технологии, программное обеспечение.

Conceptual framework for ensuring effective information protection in the context of the economic security of an enterprise

Pecheniuk A.

The necessity of formation of an effective information security system of the enterprise is substantiated. It is

emphasized that when designing an information policy, the firm must comply with the requirements of the current legislation; take into account the level of technical support, especially the regulation of employees' access to confidential information, etc. It is stated that the costs of organizing information security measures should correspond to its value.

The main threats to which a violation of the confidentiality of information constituting a commercial secret can lead are indicated. The list of basic regulatory acts aimed at bringing to civil, administrative and criminal liability for the illegal collection, disclosure and use of information constituting a commercial secret is given. The main stages of arranging an information security policy are summarized; the most common types of information threats associated with the use of modern computer technologies are characterized.

The necessity of developing a domestic original accounting (management) program that could be used in the long term by the vast majority of Ukrainian enterprises is pointed out.

There are three groups of tools that are applied in the theory and practice of information security of the enterprise (active, passive and combined), emphasizing the need for planning and continuous monitoring in real time of all important processes and conditions that affect data security.

It is noted that even if the information security system is built taking into account all modern methods and means of protection, it does not guarantee one hundred percent protection of the information resources of the enterprise, but a well-designed information security policy allows to minimize the corresponding risks.

Keywords: information security, information policy, information security, confidential information, information threats, information and communication technologies, software.

Печенюк А.В. ID: https://orcid.org/0000-0002-8348-5044