Економічні науки

УДК 004.056.5

Русіна Юлія Олександрівна
кандидат економічних наук,
доцент кафедри фінансів та фінансово-економічної безпеки
Київський національний університет технологій та дизайну
Русина Юлия Александровна
кандидат экономических наук,
доцент кафедры финансов и финансово-экономической безопасности
Киевский национальный университет технологий и дизайна
Rusina Yuliia
Candidate of economic sciences, associate professor of the
Department of Finance and Financial and Economic Security
Kyiv National University of Technologies and Design

Острякова Валентина Юріївна
менеджер з розвитку бізнесу
ТОВ «BeeMiner»
Острякова Валентина Юрьевна
менеджер по развитию бизнеса
ООО «BeeMiner»
Ostriakova Valentyna
Business Development Manager
BeeMiner Ltd.

УДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ПІДПРИЄМСТВІ
СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ НА ПРЕДПРИЯТИИ

IMPROVEMENT OF THE INFORMATION SECURITY MANAGEMENT SYSTEM IN ENTERPRISE

Анотація: *Стаття присвячена аналізу сутності системи управління інформаційною безпекою, її проблем та загроз, і як наслідок, визначенню пріоритетних шляхів удосконалення системи управління інформаційною безпекою на підприємстві.*

Ключові слова: *інформаційна безпека, система управління інформаційною безпекою, загрози системі управління інформаційною безпекою, шляхи удосконалення інформаційної безпеки.*

Аннотация: *Статья посвящена анализу сущности системы управления информационной безопасностью, ее проблем и угроз, и как следствие, определение приоритетных путей совершенствования системы управления информационной безопасностью на предприятии.*

Ключевые слова: *информационная безопасность, система управления информационной безопасностью, угрозы системы управления информационной безопасностью, пути совершенствования информационной безопасности.*

Summary: *The article is devoted to the analysis of the essence of the information security management system, its problems and threats, and as a consequence, the identification of priority ways to improve the information security management system at the enterprise.*

Key words: *information security, information security management system, threats of information security management system, ways of improving information security.*

Постановка проблеми. В сучасних економічних умовах інформація є найбільш цінним ресурсом відповідно до всіх напрямів діяльності підприємства, а визначення ефективних шляхів удосконалення системи

управління інформаційною безпекою підприємств стає все більш значущим і складнішим завданням для керівництва. Система управління інформаційною безпекою є однією зі складових частин управління економічною безпекою, яка формує систему захищеності всього підприємства.

Аналіз останніх досліджень і публікацій. Дослідженню проблематиці удосконалення системи управління інформаційною безпекою присвячені праці таких науковців, як: І. Анікін, С. Кавун, І. Конєєв, Л. Донець, Ю. Романова та інші [10; 12; 13; 14; 15]. Однак, не дивлячись на велику кількість наукових публікацій, єдиного алгоритму щодо удосконалення системи управління не було представлено.

Формулювання цілей статті. Метою написання статті є аналіз сутності системи управління інформаційною безпекою, обґрунтування пріоритету створення та удосконалення системи управління інформаційною безпекою на підприємстві.

Виклад основного матеріалу. Науковці ідентифікують поняття інформаційної безпеки по-різному, основні визначення наведені в табл. 1.

Таблиця 1

Визначення дефініції «інформаційна безпека»

[складено автором на основі джерел 10; 12; 13; 14; 15]

Науковець	Визначення
Кавун С.В.	Інформаційна безпека – це стан захищеності інформаційного середовища, що являє собою діяльність щодо запобігання витоку інформації, що захищається, несанкціонованих і ненавмисних впливів на інформацію, що захищається.
Конєєв І.Р.	Інформаційна безпека – це такий стан захищеності життєво важливих інтересів особи, суспільства і держави, при якому зводиться до мінімуму заподіяння шкоди через неповноту, несвоєчасність і недостовірність інформації.
Донець Л.І.	Інформаційна безпека – це стан захищеності потреб інформації особистістю, суспільством і державою
Анікін І.В.	Інформаційна безпека – це складова інформаційної політики держави
Романова Ю.Д.	Інформаційна безпека – це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації

Ми пропонуємо трактувати інформаційну безпеку як стан інформації, інформаційних систем і ресурсів, за якого інформаційні дані захищаються від витоку, знищення, підробки, крадіжки тощо. Для забезпечення стану захищеності необхідним є комплекс правових, технічних і організаційних заходів, що спрямовані на запобігання неправомірних дій з інформацією.

Систему управління інформаційною безпекою розуміють як частину загальної системи управління, базою якої є аналіз ризиків, а призначенням – створення, реалізація, контроль та вдосконалення заходів у сфері інформаційної безпеки [11].

Задля реалізації ефективної політики забезпечення інформаційної безпеки необхідне досягнення таких основних цілей:

1) захищеність інформації (конфіденційність та унеможливлення доступу сторонніх осіб);
2) цілісність (захист від спотворення інформації у будь-якому її вигляді);
3) доступність (забезпечення доступу до інформації зацікавлених осіб).

Основними проблемами, які постають перед підприємством у сфері інформаційної безпеки, можна зазначити наступні:

- підтримка інформаційної безпеки;
- зовнішні та внутрішні канали витоку інформації;
- грошові втрати від інформаційних інцидентів;
- атаки на конфіденційну інформацію;
- недосконаліть програмного забезпечення підприємств;
- персональні мобільні пристрої, що мають доступ до акаунтів з конфіденційною та персональною інформацією.

Проблематика інформаційної безпеки підприємств викликана дією загроз, які за природою виникнення поділяються на внутрішні та зовнішні (Рис. 1).

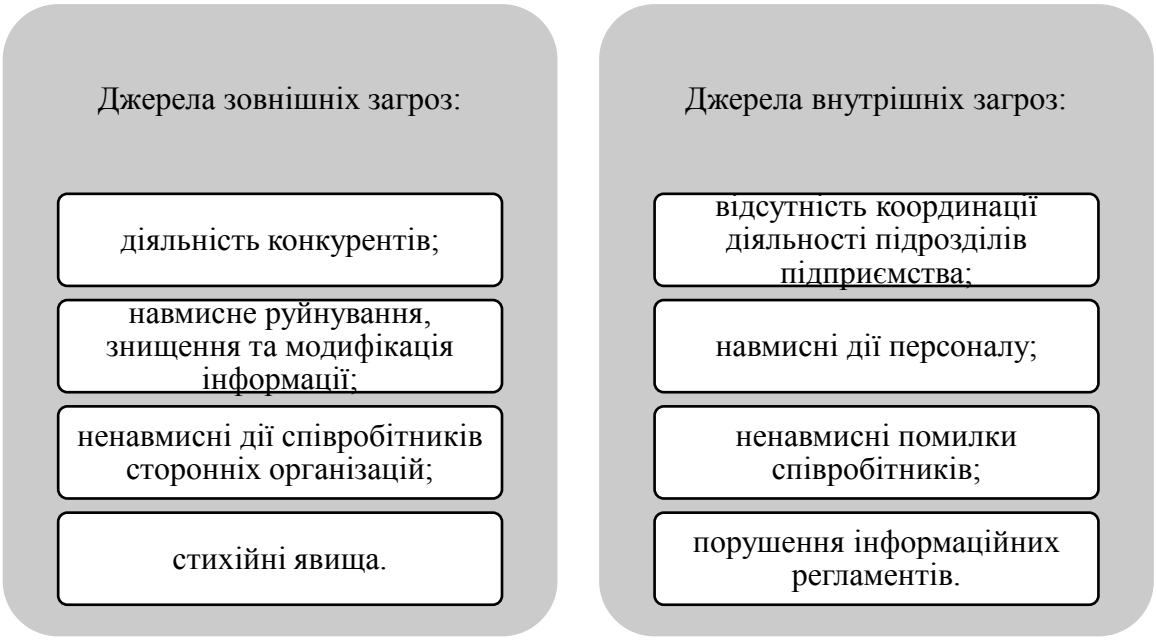

Рис. 1. Джерела внутрішніх та зовнішніх загроз інформаційній безпеці підприємства
[складено автором на основі джерел 14; 15]

Враховуючи зазначене вище, представимо систему інформаційної безпеки як процес управління ризиками та небезпеками і зобразимо у вигляді моделі управління ризиками (Рис. 2).

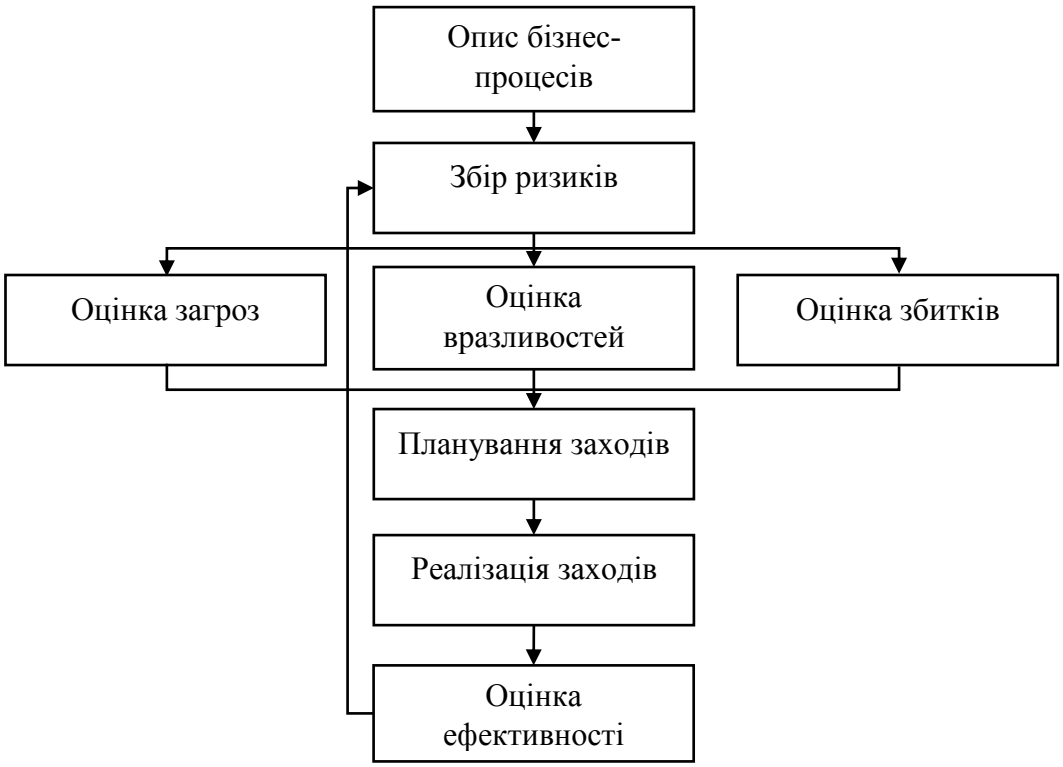

Рис. 2. Модель управління ризиками для системи інформаційної безпеки
[складено автором на основі джерел 9; 10; 11]

Важливим фактором у процесі боротьби з проблемами та ризиками є визначення організаційної структури системи управління інформаційною безпекою підприємства. Вона включає систему правових, технічних та організаційних засобів, що забезпечують нормалізацію діяльності у сфері безпеки [9].

Організаційна структура системи управління базується на основі розмежування функціональних повноважень між підрозділами підприємства. В залежності від розміру та статусу підприємства основними суб'єктами організаційної структури управління інформаційною безпекою можуть бути [13, с. 747]:

- генеральний директор;
- начальник департаменту безпеки;
- директори територіальних підрозділів;
- відділ інформаційної безпеки;
- аутсорсингові компанії;
- співробітники тощо.

Незважаючи на різноманіття суб'єктів, основним є відділ інформаційної безпеки – підрозділ, що приймає безпосередню участь в організації і відповідає за забезпечення інформаційної безпеки в рамках своїх повноважень. Співробітники цього відділу згідно функціональних обов'язків виконують наступні роботи у сфері інформаційної безпеки:

- розробка проектів і реалізація стратегій забезпечення інформаційної безпеки;
- визначення вимог до бізнес-проектів, засобів їх реалізації та автоматизації;
- розробка внутрішньої нормативної бази;
- координація діяльності підрозділів з урахуванням певних пріоритетних напрямів розвитку інформаційної безпеки;

- формулювання і обґрунтування пропозицій до проекту бюджету або фінансового плану підприємства;
- робота по виявленню та оцінці загроз, аналіз ризиків і підтримка їх в актуальному стані;
- розрахунок результатів оцінки ризиків для керівництва, а також пропозиції шляхів і засобів обробки ризиків з урахуванням їх ефективності;
- розробка пропозицій по удосконаленню механізмів забезпечення інформаційної безпеки та контроль реалізації вимог до інформаційної безпеки;
- розслідування за фактами інцидентів;
- контроль виконання вимог щодо процесу управління доступом до інформаційних систем і ресурсів користувачів, штатного персоналу, впровадження і підтримки систем [11; 14, с. 29-30].

Формуючи і удосконалюючи організаційну структуру системи управління інформаційною безпекою, важливим є дотримання певних правил і принципів:

- законність – функціонування у відповідності до законодавства, стандартів, положень, керівних документів, а також локальних нормативних документів (основними у сфері інформаційної безпеки є Закони України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про телекомунікації», «Про захист персональних даних», а також Постанови Кабінету Міністрів України «Про охорону держсекретів і інформації с обмеженим доступом, що є власністю держави», «Про забезпечення режиму секретності при обробці інформації з обмеженим доступом в автоматизованих системах», «Про деякі питання захисту інформації, охорона якої забезпечується державою», «Про затвердження Порядку підключення до глобальних мереж передачі даних») [1-8];

- централізація – функціонування за єдиними функціональними, організаційними та методичними принципами;
- безперервність – безперервний процес, що складається з етапів планування, впровадження, оцінки ефективності, покращення контролю, приведення можливих ризиків до прийнятного рівня.

Алгоритм удосконалення системи управління інформаційною безпекою на підприємстві, базуючись на дослідженнях науковців і на стандартах практики, характеризується низкою ознак:

1) Управління в масштабі всього підприємства – охоплення всіх його горизонтальних, вертикальних, а також кросфункціональних оргструктур.
2) Відповідальність керівництва – усвідомлення та підзвітність у сфері інформаційної безпеки перед контрагентами. Керівники беруть участь у процесах управління інформаційною безпекою, здійснюють фінансову підтримку, контроль, а також несуть відповідальність за ризики і небезпеки.
3) Інформаційна безпека розглядається як обов'язкова бізнес-вимога, що впливає на реалізацію цілей, тактичних завдань, планів, політик і вимог регуляторів. Співробітники підприємства розуміють, що інформаційна безпека – це не витрата і довільна стаття бюджету, а вартість ведення бізнесу та певна інвестиція.
4) Забезпечення з урахуванням ризиків. Достатній рівень захищеності оцінюється на розрахунку допустимих ризиків (ризиків порушення вимог регуляторів, збоїв у роботі, репутаційні і фінансові втрати).
5) Поділ відповідальності та визначення ролей. Чітке виокремлення посад з чітко розмежованими обов'язками та звітністю.
6) Адекватність політики, що підтримується персоналом і забезпечується всіма необхідними організаційними і технічними заходами.
7) Достатня кількість ресурсів, яка необхідна для підтримки системи управління інформаційною безпекою.

8) Поінформованість і обізнаність співробітників. Кожен співробітник має чіткі обов'язки, мотивований і дотримується норм корпоративної культури, а також періодично приймає участь у тренінгах і семінарах в області інформаційної безпеки.
9) Безпечний життєвий цикл програмного забезпечення. Вимоги до інформаційної безпеки виконуються з моменту придбання програмного забезпечення і до його списання.
10) Регулярність аудиту, і, за необхідності, перегляд корпоративної системи інформаційної безпеки чи окремих її компонентів [13].

Висновки. Сутність викладеного вище дає підстави стверджувати, що однією з ключових частин формування системи захищеності підприємства є інформаційна безпека. Для збереження цілісності підприємства, розвитку, а також конкурентоспроможності на ринку, необхідне створення ефективної системи управління інформаційною безпекою. Без належного захисту інформаційного середовища підприємства унеможливлюється забезпечення економічної безпеки.

Література

1. Закон України «Про інформацію» / ВВР України. – 1992. – №48. – Ст. 650.
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31 травня 2005 р. / ВВР України. – 2006. – №26. – Ст. 347.
3. Закон України «Про телекомунікації» від 18 листопада 2003 р. / ВВР України. – 2004. – № 12. – Ст. 155.
4. Закон України «Про захист персональних даних» від 1 червня 2010 р. / ВВР України. – 2010. – № 12. – Ст. 109
5. Постанова Кабінету Міністрів України «Про охорону держсекретів і інформації с обмеженим доступом, що є власністю держави» від

17.08.2006 р. № 549 / Офіційний вісник України. – 2006. – № 549. – Ст. 548.

6. Постанова Кабінету Міністрів України «Про забезпечення режиму секретності при обробці інформації з обмеженим доступом в автоматизованих системах» від 4.08.2010 р. № 699 / Офіційний вісник України. – 2010. – № 699. – Ст. 873.
7. Постанова Кабінету Міністрів України «Про деякі питання захисту інформації, охорона якої забезпечується державою» від 19.10.2016 р. № 736 / Офіційний вісник України. – 2016. – № 736. – Ст. 384.
8. Постанова Кабінету Міністрів України «Про затвердження Порядку підключення до глобальних мереж передачі даних» від 12.04.2002 р. № 522 / Офіційний вісник України. – 2002. – № 16. – Ст. 864.
9. ISO/IEC 27001:2005, MOD. – [Електронний ресурс]. – Режим доступу: http://s-byte.com/useful/27001.pdf
10. Аникин И.В. Теория информационной безопасности и методология защиты информации [Текст] / И.В. Аникин, В.И. Глова, Л.И. Нейман, А.Н. Нигматуллина . — Казань: Изд-во Казан. гос. техн. ун-та, 2008. — 358с.
11. Журавель М.М. Проблеми захисту інформації [Електронний ресурс] / М.М. Журавель, С.В. Паршуков. – Режим доступу: http://informatika.udpu.org.ua/?page_id=1173
12. Кавун С.В. Інформаційна безпека. Навчальний посібник. Ч.1 / С.В. Кавун, В.В. Носов, О.В. Мажай. – Харків: Вид. ХНЕУ, 2008. – 352 с.
13. Конеев И.Р. Информационная безопасность предприятия / И.Р. Конеев, А.В. Беляев. – СПб.: БХВ-Петербург, 2003. – 747 с.
14. Тарасова О.В. Корпоративна культура як інструмент ефективного менеджменту підприємства. / О.В. Тарасова, С.С. Марінова // Економіка харчової промисловості. – 2013. – № 3(19). – С. 28–32.
15. Романова Ю.Д. Інформаційні технології в менеджменті (управлінні): підручник і практикум для академічного бакалаврату /

під заг. ред. Д.Ю. Романової. – М: Видавництво Юрайт, 2015. – 478 с.

References

1. Zakon Ukrainy «Pro informatsiiu» // VVR Ukrainy. – 1992. – #48. – St. 650.
2. Zakon Ukrainy «Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh» vid 31 travnia 2005 r. // VVR Ukrainy. – 2006. – #26. – St. 347.
3. Zakon Ukrainy «Pro telekomunikatsii» vid 18 lystopada 2003 r. // VVR Ukrainy. – 2004. – # 12. – St. 155.
4. Zakon Ukrainy «Pro zakhyst personalnykh danykh» vid 1 chervnia 2010 r. // VVR Ukrainy. – 2010. – # 12. – St. 109
5. Postanova Kabinetu Ministriv Ukrainy «Pro okhoronu derzhsekretiv i informatsii s obmezhenym dostupom, shcho ye vlasnistiu derzhavy» vid 17.08.2006 r. # 549 // Ofitsiinyi visnyk Ukrainy. – 2006. – # 549. – St. 548.
6. Postanova Kabinetu Ministriv Ukrainy «Pro zabezpechennia rezhymu sekretnosti pry obrobtsi informatsii z obmezhenym dostupom v avtomatyzovanykh systemakh» vid 4.08.2010 r. # 699 // Ofitsiinyi visnyk Ukrainy. – 2010. – # 699. – St. 873.
7. Postanova Kabinetu Ministriv Ukrainy «Pro deiaki pytannia zakhystu informatsii, okhorona yakoi zabezpechuietsia derzhavoiu» vid 19.10.2016 r. # 736 // Ofitsiinyi visnyk Ukrainy. – 2016. – # 736. – St. 384.
8. Postanova Kabinetu Ministriv Ukrainy «Pro zatverdzhennia Poriadku pidkliuchennia do hlobalnykh merezh peredachi danykh» vid 12.04.2002 r. # 522 // Ofitsiinyi visnyk Ukrainy. – 2002. – # 16. – St. 864.
9. ISO/IEC 27001:2005, MOD. – [Elektronnyi resurs]. – Rezhym dostupu: http://s-byte.com/useful/27001.pdf

10. Anykyn Y.V. Teoryia ynformatsyonnoi bezopasnosty y metodolohyia zashchytы ynformatsyy [Tekst] /Y.V. Anykyn, V.Y. Hlova, L.Y. Neiman, A.N. Nyhmatullyna . — Kazan : Yzd-vo Kazan. hos. tekhn. un-ta, 2008. — 358s.
11. Zhuravel M. M. Problemy zakhystu informatsii [Elektronnyi resurs] / M. M. Zhuravel, S. V. Parshukov. – Rezhym dostupu: http://informatika.udpu.org.ua/?page_id=1173
12. Kavun S. V. Informatsiina bezpeka. Navchalnyi posibnyk. Ch.1 / S. V. Kavun, V. V. Nosov, O. V. Mazhai. – Kharkiv : Vyd. KhNEU, 2008. – 352 s.
13. Koneev Y. R. Ynformatsyonnaia bezopasnost predpryiatyia / Y. R. Koneev, A. V. Beliaev. – SPb. : BKhV-Peterburh, 2003. – 747 s.
14. Tarasova O. V. Korporatyvna kultura yak instrument efektyvnoho menedzhmentu pidpryiemstva. / O. V. Tarasova, S. S. Marinova // Ekonomika kharchovoi promyslovosti. – 2013. – # 3(19). – S. 28–32.
15. Romanova Yu. D. Informatsiini tekhnolohii v menedzhmenti (upravlinni): pidruchnyk i praktykum dlia akademichnoho bakalavratu / pid zah. red. D. Yu. Romanovoi. – M: Vydavnytstvo Yurait, 2015. – 478 s.