зареєстровано Міністерством соціальної політики України від 16 січня 2014 року за № 2 з рекомендаціями реєструючого органу від 16.01.2014 р. № 426/0/14-14/18 [Електронний ресурс]. – Режим доступу: http://profapk.org.ua/cms/legislature/agreement/industry/selo.html
1. Зміни та доповнення до Галузевої угоди між Міністерством аграрної політики та продовольства України, Всеукраїнським об'єднанням організацій роботодавців «Федерація роботодавців агропромислового комплексу та продовольства України» і Професійною спілкою працівників агропромислового комплексу України в сільському господарстві на 2014-2016 рр. зареєстровано Міністерством соціальної політики України від 07 лютого 2017 року № 9 з рекомендаціями реєструючого органу від 07.02.2017 № 2451/0/2-17/27 [Електронний ресурс]. – Режим доступу: http://minagro.gov.ua/node/23254.
2. Козаченко Г. Зарубіжний досвід мотивації праці / Г. Козаченко [Електронний ресурс]. – Режим доступу: http://milkua.info/uk/post/zarubiznij-dosvid-motivacii-praci.
3. Крушельницька О. В. Управління персоналом : [Навч. посіб.] / О.В. Крушельницька, Д.П. Мельничук. – К.: «Кондор», 2005. – 308 с. [Електронний ресурс]. – Режим доступу: http://library.if.ua/book/45/3149.html.
4. Менеджмент : [Навч. посіб.] / За ред. С.І. Михайлова. – Вінниця: НОВА КНИГА, 2006. – 416 с.
5. Завадський Й. С. Менеджмент : [Підручник]. Т.1. / Й. С. Завадський. – К.: УФІМБ, 2002. – 543 с.
6. Бабчинська О. І. Зарубіжний досвід мотивації персоналу та його впровадження на вітчизняних підприємствах / О.І. Бабчинська, С.В. Настечина [Електронний ресурс]. – Режим доступу: http://nauka.kushnir.mk.ua/?p=38898.
7. Пересипкіна Н. Чому негативні стимули не працюють / Н. Пересипкіна. [Електронний ресурс]. – Режим доступу: https://prohr.rabota.ua/motivatsiya-personalu-chomu-negativni-stimuli-ne-pratsyuyut/

Рецензент д.е.н., професор Писаренко В.В.

УДК 658:330.47
Дячков Д.В., к.е.н., доцент
Паскаль А.В., Кіт В.В., здобувачі вищої освіти СВО «Магістр»
Полтавська державна аграрна академія

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

У статті обґрунтовано необхідність формування системи інформаційної безпеки на сучасних підприємствах. Охарактеризовано основні переваги формування ефективної технології забезпечення інформаційної безпеки. Визначено загальну структуру системи інформаційної безпеки підприємства, яка повинна включати: засоби, підсистеми, програмну та технічну частини, автоматизовану систему обробки інформації, методи оцінки інформаційної захищеності підприємства. Запропоновано технологію забезпечення інформаційної безпеки підприємства, яка базується на взаємодії трьох складових: інформаційне забезпечення процесу управління на підприємстві; захист інформаційного середовища підприємства; діагностика рівня інформаційної безпеки. Узагальнено класифікацію та визначено систему взаємозв'язків методів та засобів оцінки інформаційної захищеності підприємства.

Ключові слова: захист інформації, технологія, внутрішні та зовнішні загрози, інформаційне забезпечення процесу управління, інформаційна безпека, система, Методи оцінки інформаційної захищеності підприємства

Diachkov D., Paskal A., Kit V.

TECHNOLOGY OF PROVIDING ENTERPRISE'S INFORMATION SECURITY

The article substantiates the necessity of forming an information security system in modern enterprises. The main advantages of forming effective technology for ensuring information security were described. The general structure of the information security system of the enterprise was defined, which should include: means, subsystems, program and technical parts, automated information processing system, methods for assessing the information security of the enterprise. The technology of information security of the enterprise was proposed, which based on the interaction of three components: information support of the enterprise management process; protection of the enterprise's information environment; diagnostics of the level of information security. The classification and the system of interrelationships between methods and means of assessing the information security of an enterprise were generalized.

Key words: information protection, technology, internal and external threats, information support of the management process, information security, system, methods of assessing the information security of the enterprise.

Дячков Д., Паскаль А., Кит В.

ТЕХНОЛОГИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

В статье обоснована необходимость формирования системы информационной безопасности в современных предприятиях. Охарактеризованы основные преимущества формирования эффективной технологии обеспечения информационной безопасности. Определена общая структура системы информационной безопасности предприятия, которая должна включать: средства, подсистемы, программную и техническую части, автоматизированную систему обработки информации, методы оценки информационной защищенности предприятия. Предложена технология обеспечения информационной безопасности предприятия, которая основывается на взаимодействии трех составляющих: информационное обеспечение процесса управления предприятием; защита информационной среды предприятия; диагностика уровня информационной безопасности. Обобщена классификация и определена система взаимосвязей методов и средств оценки информационной защищенности предприятия

Ключевые слова: защита информации, технология, внутренние и внешние угрозы, информационное обеспечение процесса управления, информационная безопасность, система, методы оценки информационной защищенности предприятия.

Постановка проблеми у загальному вигляді і її з важливими науковими та практичними завданнями. В сучасних трансформаційних умовах, успіх розвитку підприємства в значній мірі визначається застосуванням інформаційних технологій та інформаційних послуг. Проте для належного функціонування інформаційні системи підприємства повинні забезпечувати виконання основних трьох умов – характеристик інформації: доступність, цілісність, конфіденційність. Це так звана класична тріада інформаційної безпеки. Для збереження кожної з характеристик інформації необхідний свій підхід, своє рішення. Тому сучасна інформаційна система повинна мати належний захист, який би відповідав основним базовим вимогам: автоматизація процесів обробки інформації, включаючи всі аспекти, пов'язані із забезпеченням безпеки інформації; протистояння загрозам безпеці інформації; відповідність вимогам та критеріям, визначеним організаційно-розпорядчими та іншими документами політики інформаційної безпеки, включаючи вимоги нормативно-правових актів, тощо. Відтак, комплексні дослідження з питань забезпечення захисту інформації, управління нею за використанням сучасних інформаційних технологій є актуальним завданням сучасного підприємництва.

Аналіз останніх досліджень, у яких започатковано вирішення проблеми. Питання технології забезпечення інформаційної безпеки підприємства розглядалися багатьма вітчизняними і закордонними авторами, серед яких Газізов А. [4], Гарасім Ю. [5], Забара І. [6], Кіпарісов Г.[7], Петренко С. [8], Ткаченко В. [9], Шаньгін В. [10] та інші.

Разом з тим, незважаючи на значні досягнення в теоретичних дослідженнях і методичних розробках щодо розробки та використання системи інформаційної безпеки на підприємстві, не отримали свого вирішення ряд питань як концептуального, так і методичного характеру. Необхідність та значимість додаткових досліджень проблеми різного роду захисту інформації, документації та персональних даних співробітників, з одного боку, і практичної затребуваності методологічно вивіреної та обґрунтованої технології забезпечення інформаційної безпеки, з іншого, визначили мету дослідження.

Цілі статті. Метою статті є розробка положень щодо визначення ефективної технології забезпечення інформаційної безпеки підприємства.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. На сучасному етапі традиційні ресурси втрачають своє першорядне значення. Інформація постає головним ресурсом і товаром науково-технічного та соціально-економічного розвитку світового співтовариства. Інформація не тільки впливає на прискорення розвитку науки, техніки та різних галузей народного господарства, а й відіграє значну роль в процесах забезпечення охорони, збереження

власності, спілкування тощо. Водночас, застосування технологій обробки інформаційних ресурсів потребує підвищеної уваги до питань інформаційної безпеки. Руйнування інформаційного ресурсу, його тимчасова недоступність або несанкціоноване використання можуть завдати значних матеріальних збитків. Без належного ступеня захисту інформації впровадження інформаційних технологій може виявитися економічно невигідним в результаті значних втрат конфіденційних даних, що зберігаються і обробляються в комп'ютерних мережах. Тому проблема забезпечення інформаційної безпеки діяльності підприємства є актуальною.

Відповідно до умов функціонування у динамічному ринковому середовищі, інформаційна безпека підприємства, представляє собою характеристику стану джерел інформації що гарантує певний рівень інформаційно-аналітичного забезпечення, який базується на захисті інформаційного середовища і обумовлює отримання ефективного та результативного інформаційного продукту.

Узагальнення різних поглядів на проблематику формування технології забезпечення інформаційної безпеки, дозволило визначити основні аспекти для її ефективного впровадження та застосування, які полягають у [1-4, 7, 10]:

розмежуванні доступу до робочих місць, як адміністративними заходами (розмежування доступу в приміщення), так і з використанням різних систем захисту від несанкціонованого доступу;

виділенні на підприємстві посадової особи (адміністратора з безпеки), відповідальної за функціонування систем захисту інформаційних ресурсів;

розробці та контролі практичного здійснення заходів щодо забезпечення безпечного функціонування систем захисту;

періодичному контролі цілісності систем захисту і дотримання режиму охорони приміщень, в яких розташовані системи захисту;

періодичному контролі журналів операцій, автоматично створюваних програмними модулями, що входять в системи захисту;

зберіганні резервних копій ключових носіїв всіх операторів, що працюють в системах захисту;

запобіганні отримання зловмисниками ключових носіїв і їх тиражування власниками;

можливості довести неправомірні дії користувачів і обслуговуючого персоналу інформаційної системи;

захисті мережевої інфраструктури на основі виділеної локальної мережі або на основі віртуальної приватної мережі;

захисті серверів, автоматизованих робочих місць та телекомунікаційного обладнання інформаційних систем від несанкціонованого доступу до їх ресурсів, шкідливого програмного забезпечення і мережевих атак, здійснюваних із зовнішніх мереж;

застосуванні засобів і систем захисту, які мають дозвільні сертифікати.

Очевидно, що впровадження ефективної технології забезпечення інформаційної безпеки на підприємстві призводить до поліпшення контролю за використанням різних видів ресурсів, підвищення загального рівня безпеки та структурування інформаційних ресурсів.

В загальному вигляді структура системи інформаційної безпеки підприємства повинна включати засоби, підсистеми, програмну та технічну частини, автоматизовану систему обробки інформації, методи оцінки інформаційної захищеності підприємства (рис. 1).

Інформаційна безпека підприємства на практиці включає сукупність напрямів, методів, засобів і заходів, що знижують вразливість інформації і перешкоджають

несанкціонованому доступу до інформації, її розголошенню або витоку. Елементами цієї системи є: правовий, організаційний, інженерно-технічний захист інформації, а основною її характеристикою – комплексність. Структура системи, склад і зміст елементів, їх взаємозв'язок залежать від об'єму і цінності інформації, що захищається, характеру можливих загроз безпеки інформації, необхідної надійності захисту і вартості системи. Технологію забезпечення інформаційної безпеки підприємства можна представити як взаємодію складових: інформаційне забезпечення процесу управління на підприємстві; захист інформаційного середовища підприємства; діагностика рівня інформаційної безпеки [6].

При побудові моделі системи інформаційної безпеки повинні враховувати взаємозв'язок між складовими. Наприклад, вихід з ладу будь-якого обладнання може призвести до втрати даних або виходу з ладу іншого критично важливого елемента системи. Подібні взаємозв'язки визначають основу технології побудови моделі організації з точки зору інформаційної безпеки.

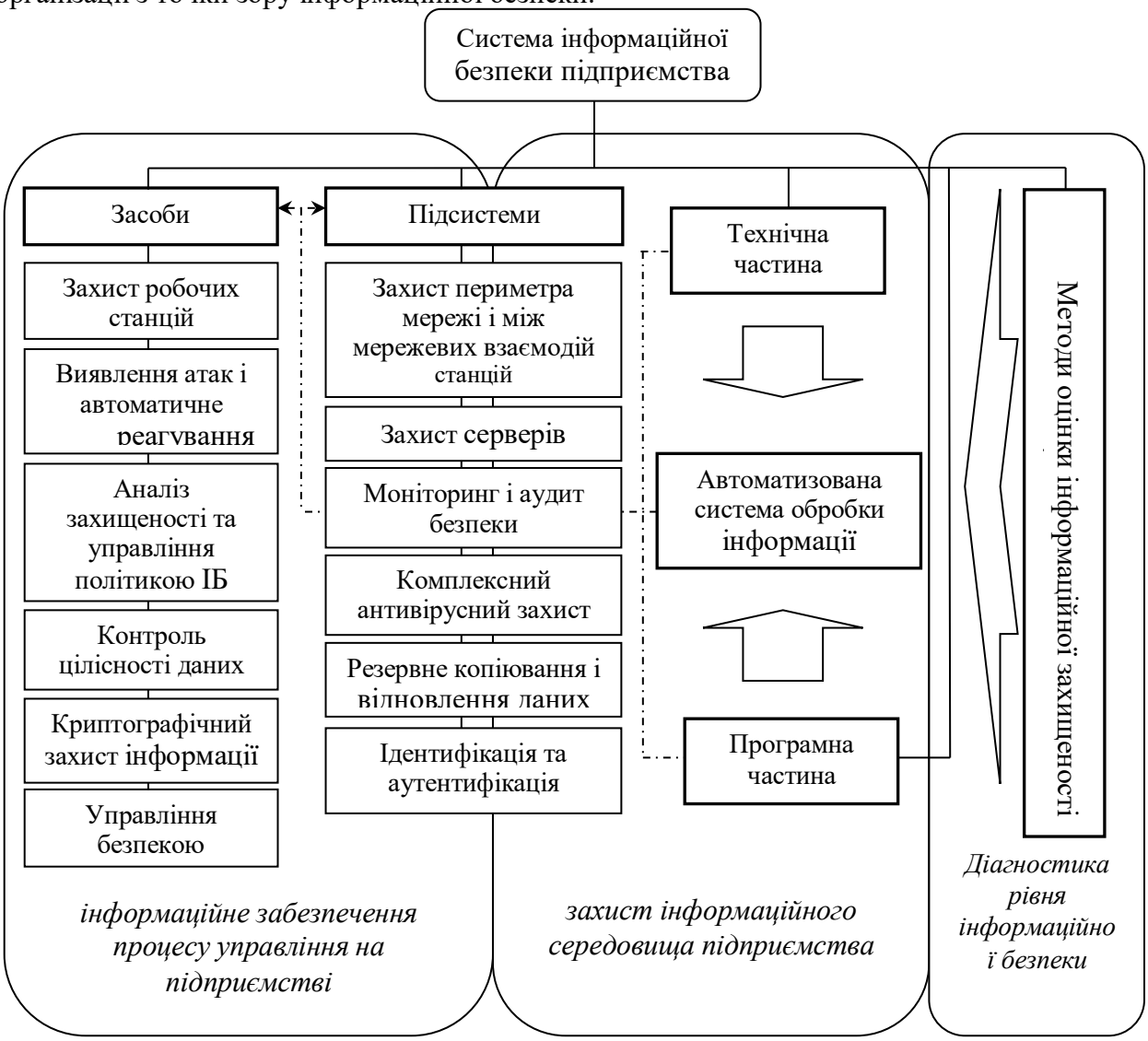

Рис.1. Структура системи захисту інформаційної системи підприємства [розроблено авторами на основі 7-9]

З цією метою, запропоновані рекомендації, які слід застосовувати при формуванні технології захисту інформаційної системи підприємства:

механізми захисту інформаційної системи повинні бути прості для технічного обслуговування і «прозорі» для користувачів;

кожен користувач повинен мати мінімальний набір «привілеїв», необхідних для інформаційної взаємодії;

можливість відключення «механізмів» захисту інформаційної системи в «особливих» випадках, коли механізми «заважають» інформаційній взаємодії користувачів;

незалежність «механізмів» захисту від самої системи; розробники повинні враховувати, найгірші наміри користувачів та передбачати здійснення серйозних помилки помилок при використанні інформаційних технологій.

Для проведення якісного аудиту інформаційної безпеки підприємства повинна бути надана вичерпна інформація про інформаційну інфраструктуру підприємства і методах її захисту. Класифікація та складна система взаємозв'язків методів, засобів, одиниць оцінки, гарантій оцінки, забезпечення єдності оцінки та довіри наведені у табл. 1.

Таблиця 1

Методи, засоби оцінки інформаційної захищеності підприємства [9]

№ з/п	Вид захисту інформації	Методи та засоби оцінки	Одиниці оцінки	Гарантії оцінки	Забезпечення єдності оцінки та довіри
1	Криптографічний	Розрахункові. Стійкість системи шифрування	Час розкриття методом прямого перебору	Теоретичне доведення, експеримент	Досягнута продуктивність обчислювальної техніки
2	Від витоку технічними каналами	Інструментальні. Метрологічні вимірювальні прилади	Відношення сигнал/шум. С/Ш=Іс-Іш	Клас вимірювальних приладів, похибка вимірювання	Державна метрологічна система
3	Від НСД до комп'ютерних систем	Експертні оцінки, аудит дослідження	Одиниці умовних шкал	Кваліфікація експертів	Система державної експертизи
4	Від фізичного НСД до носіїв інформації	Експертні оцінки, моделювання, атестація, аудит	Ймовірність подолання рубежів охорони	Кваліфікація експертів	Система атестації КЗЗ – комплексів засобів захисту
5	Організаційні заходи (від людського фактора)	Експертні оцінки, атестація, аудит	Одиниці умовних шкал	Кваліфікація експертів	Система атестації КЗЗ
6	Від вірусів	Експертиза. Статистичні дослідження. Оцінка ризиків	Ймовірності, математичне очікування, дисперсія	Довірчий інтервал (критерій Пірсона тощо)	Сертифікація. Система збору й аналізу статистичних даних
7	За допомогою брандмауерів				
8	Система виявлення атак				

Постійна робота в сфері підтримки інформаційної безпеки на належному рівні є необхідною умовою ефективності підприємницької діяльності [5]. Водночас безпека інформаційної системи має розглядатися як важлива складова загальної безпеки підприємства. Вищезазначене обумовлює необхідність розробки концепції інформаційної безпеки, в якій слід передбачити не тільки заходи, пов'язані з інформаційними технологіями (криптозахист, програмні засоби адміністрування прав користувачів, їх ідентифікації та аутентифікації, брандмауери для захисту входів-виходів мережі тощо), але і відповідні заходи адміністративного та технічного характеру.

Висновки. Захист інформаційних ресурсів підприємства є одним з ключових завдань в умовах підвищення рівня внутрішніх і зовнішніх загроз інформаційної безпеки, що можуть безпосередньо вплинути на його фінансову діяльність і стійкість на ринку. Щоб зберегти бізнес, розвиватися і бути конкурентоспроможним,

підприємствам необхідно створити ефективну систему управління інформаційною безпекою. Пропонована технологія забезпечення інформаційної безпеки зорієнтована на вирішення питань надійної аутентифікації користувачів і серверів, захист конфіденційної інформації при її передачі по каналах зв'язку, контроль справжності та цілісності електронних документів, забезпечення юридичнозначимого електронного документообігу, захищеного обміну електронними документами як всередині підприємства так і з зовнішніми користувачами. Тому перспективні напрями досліджень полягають у визначенні технічних та програмних складових для забезпечення необхідного рівня інформаційної безпеки на підприємстві.

Список використаних джерел:

1. ISO/IEC 27035. Information technology. Security techniques. Information security incedent management. – 2011. – 78 p.
2. Y.1291: An architectural framework for support of Quality of Service in packet networks. – [Електронний ресурс]. – Режим доступу: http://www.itu.int/rec/ T-REC-Y.1291/en.
3. Y.1541: Network performance objectives for IP-based services. – [Електронний ресурс]. – Режим доступу: http://www.itu.int/rec/T-REC-Y.1541/en.
4. Газизов А. Р. Концепция организационного построения защищенной информационной системы торгового предприятия / А. Р. Газизов // Вестник АГТУ. Сер. Управление, вычислительная техника и информатика. – 2018. – №2. – С. 110-115.
5. Гарасим Ю. Р. Аналіз систем захисту, які мають властивість живучості / Ю. Р. Гарасим // Військово-технічний збірник. – 2010. № 1 (4). – С. 87-95.
6. Забара І. М. Міжнародна інформаційна безпека в міжнародному праві: до питання визначення / І. М. Забара // Український часопис міжнародного права. – 2012. – № 4. – С. 63-69.
7. Кипарисов Г. Н. Обеспечение информационной безопасности в МБОУ СОШ №121 городского округа Самара / Г. Н. Кипарисов, О. Р. Загидуллина, О. Г. Корганова // Материалы X Всероссийской научно-технической конференции [Актуальные проблемы информационной безопасности. Теория и практика использования программно-аппаратных средств] (21-22 марта 2017 г., Самара) / Отв. редакторы А.И. Никонов, В.П. Свиридов. – Самара, Самар. гос. техн. ун-т, 2017. – С.23-25.
8. Петренко С. А. Возможная методика построения системы информационной безопасности предприятия. – [Электронный ресурс]. – Режим доступа: http://itzashita.ru/theory/vozmozhnaya-metodika-postroeniya-sistemy-informacionnoj-bezopasnosti-predpriyatiya.html 2018
9. Ткаченко В. Современные подходы к оценке рисков информационных технологий / В. Ткаченко, В. Сысоев // [Електронний ресурс]. – Режим доступу: http://www.cbz.com.ua/resources/files/12224515494d0f29e1ca cc9.pdf
10. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: [учеб. пособ.] – М.: ИД «ФОРУМ»: ИНФРА-М, 2011. – 416 с.

Рецензент д.е.н., професор Маркіна І.А.

УДК 330.131.7
Дячков Д.В., к.е.н., доцент,
Крепко К.В., Кисіль І.Г., здобувачі вищої освіти СВО «Магістр»
Полтавська державна аграрна академія

ОНТОЛОГІЧНІ ЗАСАДИ ВИЗНАЧЕННЯ СУТНОСТІ КОНКУРЕНТОСПРОМОЖНОСТІ ПІДПРИЄМСТВА ЯК ЗАСОБУ ПРОТИДІЇ ПІДПРИЄМНИЦЬКИМ РИЗИКАМ

В статі охарактеризовано значення конкурентоспроможності для забезпечення протидії підприємницьким ризикам. Доведено багатоаспектність застосування в теорії та практиці категорії «конкурентоспроможності», неоднозначність її трактування. Як вітчизняна так і світова наукова спільнота має різні, іноді протилежні, підходи до визначення конкурентоспроможності підприємства. Узагальнення напрацювань в зазначеній предметній сфері дослідження дозволило визначити три основні підходи до визначення конкурентоспроможності підприємства: компаративний, ресурсний та системний.