конкурентних переваг в умовах зниження рівня платоспроможності населення), стратегію диверсифікації (для зниження рівнів ризиків та збільшення виробництва та реалізації сільськогосподарської продукції) та ряд інших стратегій, які дозволятимуть українським сільськогосподарським підприємствам одночасно досягати багато цілей. Досягнення багатьох цілей підприємством дозволить не лише покращувати позицію на ринку, а й збільшувати обсяг прибутків, що в свою чергу дозволить підвищувати заробітну плату працівникам, підвищувати надходження до місцевого та державного бюджетів й розвивати соціальну інфраструктуру у сільській місцевості, що буде позитивно впливати на сільську громаду.

Список використаних джерел

1. Selected Paper prepared for presentation at the 140th EAAE Seminar, “Theories and Empirical Applications on Policy and Governance of Agri-food Value Chains,” Perugia, Italy, December 13-15, 2013. 18 с.

2. Gabriela Chmelíková. Economic Value Added versus Traditional Performance Metrics in the Czech Food-Processing Sector/ Gabriela Chmelíková. *International Food and Agribusiness Management Review*. 2008. Volume 11. Issue 4. 49-66.

Бурлаков Олександр
канд. екон. наук, доцент
Подільський державний аграрно-технічний університет
Кам’янець-Подільський, Україна

ТЕОРЕТИЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

Дослідження інформаційної безпеки підприємства, будучи проблематикою, як загальної теорії організації, так і інформаційного права, сьогодні набуває нових аспектів. Їх поява попередньо визначається, в першу чергу, якісними змінами самого соціуму [1].

Людина, у прагненні підвищити ступінь своєї захищеності від негативного впливу природних сил, так змінила умови свого існування, що вони стали джерелом небезпек.

В системі забезпечення безпеки все більшого значення набуває забезпечення інформаційної безпеки підприємства. Це пов'язано із зростаючим обсягом інформації, з необхідністю її зберігання, передачі та обробки. Переведення значної частини інформації в електронну форму, використання локальних та глобальних мереж створюють якісно нові небезпеки конфіденційної інформації [3].

Щодо поняття «інформаційна безпека підприємства» необхідно зазначити, що воно є надзвичайно актуальним на сучасному етапі розвитку інформаційних технологій, який супроводжується введенням інформаційних систем в усі сфери діяльності людини.

Проблеми, пов'язані з інформаційною безпекою на підприємствах, можуть бути вирішені тільки за допомогою системного і комплексного підходу. З методологічної точки зору, підхід до проблем інформаційної безпеки починається з виявлення суб'єктів інформаційних відносин та інтересів цих суб'єктів [4].

Весь спектр інтересів суб'єктів, пов'язаних з використанням інформації, можна розділити на такі категорії: забезпечення доступності, цілісності і конфіденційності ресурсів інформаційного середовища [1].

Доступність – якість інформації, що визначає її швидке і точне знаходження конкретними користувачами.

Цілісність – поняття, що визначає збереження якості інформації та її властивостей.

Конфіденційність передбачає забезпечення секретності даних і доступу до певної інформації окремим користувачам.

До основних видів загроз інформаційної безпеки організації відносять:

1. Несприятлива для підприємства економічна політика держави. Регулювання економіки державою за допомогою маніпуляцій (визначення валютного курсу, облікова ставка, митні тарифи і податки) є причиною багатьох протиріч на підприємствах в сфері виробництва, фінансів і комерції.
2. Дії інших господарюючих суб'єктів. В даному випадку ризики безпеки інформації пов’язані з використанням засобів нездорової конкуренції.
3. Кризові явища в світовій економіці. Кризи мають особливість перетікати з однієї країни в іншу, використовуючи канали зовнішніх економічних зв'язків. Вони також завдають шкоди забезпеченню безпеки інформації. Це слід врахувати при визначенні методів і засобів забезпечення інформаційної безпеки організації.

Процес комплексного захисту інформації повинен здійснюватися безперервно на всіх етапах. Реалізація безперервного процесу захисту інформації можлива тільки на основі систем концептуального підходу і промислового виробництва засобів захисту, а створення механізмів захисту і забезпечення їх надійного функціонування і високої ефективності може бути здійснено тільки фахівцями високої кваліфікації в галузі захисту інформації [5].

Отже, за результатами проведеного дослідження можна відзначити, що за допомогою комплексного використання різних програмно-апаратних засобів захисту інформації, представлених різними виробниками, можна досягти більш високих показників їх ефективності. До таких засобів відносять обладнання для криптографічного захисту мовної інформації, програми для криптографічного захисту текстової або іншої інформації, програми для забезпечення аутентифікації поштових повідомлень за допомогою електронного цифрового підпису, програми забезпечення антивірусного захисту, програми захисту від мережевих вторгнень, програми виявлення вторгнень, програми для приховування зворотної адреси відправника електронного листа.

Розробка регламентів інформаційної безпеки при використанні телекомунікацій, дотримання персоналом регламентів, внутрішніх нормативних актів, а також впровадження заходів по досягненню конфіденційності, цілісності та доступності інформації дозволять не тільки підвищити результативність системи інформаційної безпеки, але і будуть сприяти зміцненню зовнішніх позицій підприємства.

Список використаних джерел

1. Аніловська Г.Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій. URL : http://www.nbuv.gov.ua/portal/chem_biol/ nvnltu/18_9/270_Anilowska_18_9.pdf (дата звернення 11.01.2018).
2. Гатчин Ю. А., Сухостат В. В. Теория информационной безопасности и методология защиты информации. Санкт-Петербург : СПбГУ ИТМО, 2010. 98 с.
3. Гриджук Г.С. Систематизація методів інформаційної безпеки підпримства. URL : http://www.nbuv.gov.ua/portal/natural/ Vntu/2009_19_1/pdf/64.pdf (дата звернення 11.01.2018).
4. Доктрина інформаційної безпеки України: Затверджено Указом Президента України від 08.07.2009 № 514/2009. Офіційне інтернет-представн. Президента України. 30.01.2010. С. 1-8.
5. Сороківська О.А., Гевко В.Л. Інформаційна безпека підприємства: нові загрози та перспективи. URL : http://nbuv.gov.ua/portal/Soc_Gum/ Vchnu_ekon/2010_2_2/032-035.pdf (дата звернення 11.01.2018).

Вдовичинський Дмитро
аспірант
Науковий керівник: д-р екон. наук, професор Чикуркова А.Д.
Подільський державний аграрно-технічний університет
Кам'янець-Подільський, Україна

СУЧАСНА ПАРАДИГМА МЕНЕДЖМЕНТУ ТА ВІТЧИЗНЯНИЙ БІЗНЕС

Парадигма – це «теорія, теоретична модель, яку мають і використовують як зразок постановки, обґрунтування, вирішення проблем в межах певного предмета дослідження» [1]. В менеджменті, як суспільній науці, відображаються існуючі соціально-економічні умови виробництва, які постійно змінюються, і тому його парадигма не є сталою. Відомий спеціаліст в галузі менеджменту П.Ф. Друкер писав: «Для суспільної науки, якою є менеджмент, уявлення про дійсність набагато важливіше, ніж для природних наук» [2].

Парадигма менеджменту постійно еволюціонувала - від найпростішої на ранніх етапах розвитку економіки (до кінця XVII ст. це був контроль за виконанням), до застосування на різних етапах розвитку генерованих таких складових парадигми, як: раціоналізація виробництва; планування; мінімізація витрат виробництва; маркетингова орієнтація; технологія publik relations; стратегічний менеджмент; диверсифікація і багатопрофільність виробництва; фірмовий стиль і культура організації тощо, і до сучасної, яка сформувалась на основі відбору найбільш ефективних технологій менеджменту на всіх етапах його історичного розвитку, що виявились найбільш дієвими в нинішніх соціально-економічних умовах.