УДК 330.65:056

К. С. Жадько,
д. е. н., професор, завідувач кафедри підприємництва та економіки підприємства,
Університет митної справи та фінансів
ORCID ID: https://orcid.org/0000-0002-2650-1431

DOI: 10.32702/2306-6792.2024.14.21

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВ-ПОСТАЧАЛЬНИКІВ ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ ПОСЛУГ

K. Zhadko,
Doctor of Economic Sciences, Professor, Head of the Department of Entrepreneurship and Enterprise, Economics University of Customs and Finance

MANAGEMENT OF INFORMATION SECURITY FOR ENTERPRISES PROVIDING ELECTRONIC COMMUNICATION SERVICES

Автором розглянуто кіберзагрози, які представляють кіберзлочинці для державних та приватних організацій. Відмічено важливість регулярного оцінювання з боку компаній своїх систем безпеки, проведення навчання персоналу та вдосконалення стратегії кіберзахисту. Співпраця між державними установами та приватним сектором також є ключовим фактором у боротьбі з кіберзлочинністю. На думку автора, ефективне управління інформаційною безпекою вимагає інтеграції технічних засобів захисту з організаційними заходами, а також постійного вдосконалення на основі нових загроз і викликів. Лише такий підхід дозволить забезпечити надійний захист інформаційних ресурсів в умовах швидкоплинного технологічного розвитку і глобальних змін. Запропоновано розглянути основні компоненти комплексної системи інформаційної безпеки, які складаються з: законодавчої, економічної, програмно-технічної та адміністративно-управлінської складової. У межах єдиної системи забезпечення інформаційної безпеки корпорацій можна виділити державну та недержавну підсистеми.

The author has examined the cyber threats posed by cybercriminals to both public and private organizations. They noted the importance of regular security system assessments by companies, employee training, and the enhancement of cybersecurity strategies. Collaboration between government agencies and the private sector is also a key factor in combating cybercrime. The analysis of cyberattacks emphasized the necessity of international cooperation in the field of cybersecurity, including sharing information about threats, developing joint protection strategies, and conducting joint training exercises, which could significantly improve the level of readiness for such incidents.

For effective functioning of information security in the context of globalization, it is necessary to view it as a complex interaction between public and private protection systems. Government bodies can provide regulatory and legislative support, develop security standards, ensure compliance, and coordinate actions in case of global cyber threats. Private companies, on the other hand, should invest in modern protection technologies, develop and implement their own security policies, and actively cooperate with government structures.

According to the author, effective information security management requires the integration of technical protection measures with organizational actions, as well as continuous improvement based on new threats and challenges. Only such an approach will ensure reliable protection of information resources in the face of rapid technological development and global changes.

Передплатний індекс 21847

The author has proposed considering the main components of a comprehensive information security system, which consist of legislative, economic, software-technical, and administrative-management components. Within a unified system of corporate information security, both public and private subsystems can be distinguished.

An integrated approach to ensuring information security, including legislative and administrative-management components, will create an effective and reliable system for protecting corporate information resources. This will not only provide protection against cyber threats but also contribute to the sustainable development of the corporate economy in the face of globalization challenges.

Ключові слова: інформаційна безпека, кібератаки, комунікаційні послуги, підприємства електронних комунікаційних мереж та послуг.

Key words: information security, cyber attacks, communication services, enterprises of electronic communication networks and services.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Захист важливої інформації компанії вимагає ретельного підходу та збалансованості у виборі заходів інформаційної безпеки. Використання найсучасніших технологій не завжди є панацеєю, оскільки їх ефективність залежить від правильної інтеграції з існуючими системами та процедурами. Навіть велика кількість інструментів може ускладнити управління безпекою, якщо вони не інтегровані в єдину стратегію інформаційної безпеки компанії. Ефективне управління вимагає не лише технічних рішень, але й усвідомлення ризиків і застосування відповідних політик та навчання персоналу.

Часто механізми, що забезпечують постійний моніторинг та аналіз систем інформаційної безпеки, не функціонують належним чином. Це призводить до того, що коригування і вдосконалення системи відбувається нерегулярно або зовсім не відбувається. Відсутність формалізованих процесів управління і забезпечення інформаційної безпеки створює додаткові операційні витрати, оскільки всі виникаючі проблеми вирішуються на індивідуальній основі, без систематичного підходу. Такий підхід не лише підвищує витрати, але й знижує ефективність реагування на загрози.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Праці відомих вчених, зокрема: О. Данилян, Р. Калюжний, С. Ковтун та інших, присвячені етимологічним питанням концепції "інформаційної безпеки" в деяких предметних галузях досліджень. М. Марущак, А. Морозов, Б. Кормич згадують про якісно нові можливості застосування систем інформаційної безпеки разом з іншими методами захисту бізнес-процесів у своїх працях.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Полягає в дослідженні сутності управління інформаційною безпекою підприємств, які надають електронні комунікаційні послуги. Методологічну основу дослідження складають аналіз наукових публікацій, звітів та статистичних даних, що стосуються інструментів управління безпекою цих підприємств. У статті використовуються загальнонаукові методи, зокрема пізнання, узагальнення, системний аналіз та синтез. Під час дослідження здійснюється аналіз наукових праць як вітчизняних, так і зарубіжних учених.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Телекомунікаційні компанії, медіаорганізації, інтернет-провайдери (ISP), постачальники послуг інформаційних технологій (IT) та вебсайти в Нідерландах стали мішенню нової хвилі кібершпигунства, організованої зловмисником, відомим під псевдонімом Sea Turtle. Атака спричинила загрозу Cosmic Wolf, Marbled Dust, Teal Kurma та UNC1326, була вперше зафіксована аналітиками з Cisco Talos у квітні 2019 року. Компанія Sea Turtle викликає значне занепокоєння серед фахівців з інформаційної безпеки через її складність та широкомасштабність, зловмисниками використовуються різноманітні методи для досягнення цілей, зокрема фішинг, маніпуляції з DNS-записами та експлуатацією вразливостей в інфраструктурі мережі. Основною метою даних атак є отри-

Передплатний індекс 21847

мання несанкціонованого доступу до конфіденційної інформації, шпигунство та втручання у внутрішні процеси організацій.

Однією з основних цілей Sea Turtle є інтернет-провайдери та IT-компанії, які забезпечують послуги зв'язку та обробки даних. Атаки на інфокомунікаційні компанії можуть мати серйозні наслідки, оскільки вони надають критично важливі послуги великій кількості користувачів. Злам інфраструктури таких компаній може призвести до масових витоків даних, порушення роботи мереж та втрати довіри з боку клієнтів.

Медіаорганізації та вебсайти також стають частими мішенями Sea Turtle, що пов'язано із тим, що такі ресурси часто поширюють інформацію, яка може загрожує репутації державних структур. Злом державних сайтів дозволяє зловмисникам отримати доступ до внутрішньої інформації, а також змінювати або видаляти публікації, маніпулюючи громадською думкою. Важливо відзначити, що діяльність Sea Turtle має явні ознаки підтримки із боку державних організацій, підтвердженням виступає високий рівень підготовки атак, доступ до складних технічних ресурсів та ретельною організацією операцій, що можливо лише за внутрішнього сприяння атаці. Внутрішнє сприяння дозволяє зловмисникам діяти масштабовано, спричиняє до значних пошкоджень у інформаційних та комунікаційних системах підприємств, а інколи й до їх руйнації. Для протидії таким загрозам компанії та організації повинні вживати комплексних заходів з інформаційної безпеки. Це включає регулярні оновлення програмного забезпечення, навчання співробітників методам захисту від фішингу, впровадження багаторівневих систем автентифікації та постійний моніторинг мережевої активності для виявлення можливих атак. Таким чином, кампанія Sea Turtle демонструє зростаючу загрозу кібершпигунства, що вимагає від організацій підвищеної уваги до питань інформаційної безпеки та впровадження передових заходів захисту для збереження своїх даних і забезпечення стабільної роботи.

Міністерство цифрової трансформації України та Міністерство досліджень, інновацій і цифровізації Румунії підписали угоду про співпрацю, спрямовану на розвиток електронних комунікацій, цифровізації та кіберзахисту. Це партнерство відкриває нові можливості для обміну досвідом між фахівцями обох країн, а також реалізацію спільних проектів, спрямованих на вдосконалення телекомунікаційної інфраструктури, розвиток цифрових послуг і зміцнення кібербезпеки. Одним із ключових аспектів угоди є створення умов для інтеграції українських спеціалістів у міжнародну спільноту, де вони зможуть отримувати цінний досвід і знання від румунських колег. Цей обмін досвідом сприятиме підвищенню професійного рівня обох сторін і дозволить впроваджувати найсучасніші технологічні рішення в обох країнах. Спільні проєкти, що передбачаються угодою, мають на меті розвиток телекомунікаційної інфраструктури, яка є основою для ефективного функціонування цифрових послуг, що включає модернізацію існуючих мереж, впровадження нових технологій, таких як 5G, а також розвиток широкосмугового доступу до Інтернету в сільських та віддалених районах. Завдяки цьому громадяни обох країн зможуть отримувати доступ до якісних цифрових послуг, незалежно від місця проживання.

Цифровізація є ще одним важливим напрямком співпраці. Угода передбачає розвиток електронного урядування, що дозволить спростити доступ громадян до державних послуг, зменшити бюрократичні процедури і підвищити прозорість урядових процесів. Спільні проекти в цій сфері можуть включати розробку та впровадження електронних платформ для надання державних послуг, цифрових ідентифікаційних систем та інших інноваційних рішень [1].

Кіберзахист займає особливе місце в угоді, оскільки зростаюча залежність від цифрових технологій вимагає надійного захисту інформаційних систем від кібератак. Україна та Румунія планують обмінюватися знаннями та досвідом у сфері кібербезпеки, спільно розробляти та впроваджувати заходи для захисту критичної інфраструктури, а також проводити спільні навчання та тренінги для підвищення кваліфікації фахівців з кіберзахисту.

У січні 2023 року керівник Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ розкрив деякі деталі масштабної кібератаки проти оператора мобільного зв'язку "Київстар". За його словами, ця атака спричинила "катастрофічні" руйнування та мала на меті завдати значного психологічного удару та зібрати розвіддані. Згідно з інформацією, наданою Вітюком, атака знищила "майже все", включаючи тисячі віртуальних серверів і ПК, що, за його словами, робить її ймовірно першим прикладом деструктивної кібератаки, яка повністю знищила ядро телекомунікаційного оператора. Він також зазначив, що хакери були присутні в системі щонайменше з травня 2023 року, дана ата-

Передплатний індекс 21847

ка стала справжнім шоком для українського суспільства та міжнародної спільноти, оскільки продемонструвала новий рівень кіберзагроз, з якими можуть стикатися країни та їх критичні інфраструктури. Завдані "Київстару" руйнування, не лише порушили роботу одного з найбільших операторів мобільного зв'язку в Україні, але й вплинули на мільйони користувачів, які втратили доступ до зв'язку та інтернет-послуг, що в свою чергу, підкреслило необхідність посилення кібербезпеки та захисту критичних інфраструктур. Наслідки атаки були масштабними і багатоаспектними. Руйнування тисяч віртуальних серверів та ПК паралізували операційну діяльність "Київстар", що ускладнило відновлення нормальної роботи. Клієнти компанії відчули значні перебої у зв'язку, що призвело до зниження рівня довіри до надійності послуг оператора.

Окрім фізичних руйнувань, атака мала потужний психологічний ефект. Втрата контролю над телекомунікаційною інфраструктурою створила атмосферу невпевненості та тривоги серед населення. Люди, які звикли до безперебійного зв'язку, були змушені шукати альтернативні способи комунікації, що вплинуло на їхній щоденний побут та роботу [2; 3]. Однією з головних цілей атаки було збирання розвідданих. Проникнення хакерів у системи "Київстар" дозволило їм отримати доступ до величезної кількості конфіденційної інформації, включаючи дані про користувачів, комерційні та технічні дані, що створило додаткові ризики для національної безпеки та приватності громадян. Хакери перебували в системі щонайменше з травня 2023 року, що свідчить про високий рівень підготовки і складність атаки. Така тривала присутність дозволила зловмисникам ретельно підготуватися і здійснити атаку, яка принесла максимальні руйнування.

Ця атака підкреслила важливість розробки та впровадження більш ефективних стратегій кібербезпеки. Українським та міжнародним організаціям слід посилити співпрацю у сфері кіберзахисту, обмінюватися інформацією про загрози та спільно розробляти контрзаходи. Крім того, важливо регулярно проводити аудити та перевірки систем, щоб виявляти вразливості та забезпечувати швидке реагування на будь-які спроби проникнення.

Посилення навчання та підвищення кваліфікації фахівців з кібербезпеки також є ключовим елементом захисту. Співробітники компаній та державних установ повинні бути обізнані про новітні загрози та методи їх протидії [4].

Таким чином, атака на "Київстар" стала уроком для всіх країн та організацій, що займаються захистом критичної інфраструктури, а також продемонструвала, що сучасні кіберзагрози можуть завдати катастрофічних наслідків, і вимагатиме посиленого підходу до безпеки та співпраці на міжнародному рівні.

Генеральний директор Monobank у січні 2023 року підтвердив атаку на банк, яка включала 580 мільйонів запитів, зазначивши, що Monobank є однією з найбільш атакованих ІТ-цілей в Україні. Незважаючи на масштаби атаки, робота послуг онлайн-банку не була порушена, хоча ця атака стала другою за останній тиждень, після аналогічної DDoS-атаки. Існує висока вірогідність загроз, з якими стикається банківський сектор. Здатність Monobank витримати такі атаки без втрати працездатності демонструє надійність їхніх систем безпеки та готовність до подібних інцидентів. Того ж року великі компанії: Нафтогаз України, Державна служба України з безпеки на транспорті, Укрпошта та Укрзалізниця повідомили про технічні збої у роботі своїх сайтів та електронних послуг, причиною цих збоїв стала кібератака на датацентр "Парковий". Дані інциденти підкреслюють значний вплив кібератак на повсякденне життя громадян і економіку країни. Відмова у наданні послуг даних підприємств піднімає питання про безпеку критичних інфраструктур і необхідність їхньої постійної захищеності.

Процес відновлення сервісів Нафтогазу, який тривав до 28 лютого, свідчить про складність відновлювальних робіт після масштабних кібератак. Цей випадок підкреслює важливість мати ефективні плани відновлення та резервні системи для мінімізації наслідків подібних інцидентів. Відновлення послуг після атаки займає значний час і ресурси, що вимагає координації між різними відомствами та компаніями. Це також ставить питання про ефективність існуючих систем захисту та необхідність їхнього вдосконалення [5].

Ці атаки демонструють постійну загрозу, яку представляють кіберзлочинці для державних та приватних організацій. Важливо, щоб організації регулярно оцінювали свої системи безпеки, проводили навчання персоналу та вдосконалювали свої стратегії кіберзахисту. Співпраця між державними установами та приватним сектором також є ключовим фактором у боротьбі з кіберзлочинністю [6].

Кібератаки такого масштабу підкреслюють необхідність міжнародної співпраці в сфері кібербезпеки. Обмін інформацією про загрози, розробка спільних стратегій захисту та спільні

Передплатний індекс 21847

навчання можуть значно підвищити рівень готовності до подібних інцидентів. Україна повинна активно залучатися до міжнародних ініціатив з кібербезпеки та співпрацювати з іншими країнами для посилення своєї захищеності. Таким чином, кібератаки на Monobank, Нафтогаз України та інші установи демонструють високий рівень загрози та необхідність постійного вдосконалення систем кібербезпеки. Важливо, щоб державні та приватні організації працювали разом для захисту критичної інфраструктури та забезпечення безперебійного надання послуг громадянам.

Дослідження показують, що для ефективного функціонування інформаційної безпеки в умовах глобалізації необхідно розглядати її як комплекс взаємодії державних і приватних систем захисту [7; 8]. Державні органи можуть надавати нормативну та законодавчу підтримку, розробляти стандарти безпеки і забезпечувати їх дотримання, а також координувати дії у випадку глобальних кіберзагроз. Приватні компанії, зі свого боку, повинні інвестувати в сучасні технології захисту, розробляти і впроваджувати власні політики безпеки, а також активно співпрацювати з державними структурами.

Організаційний підхід до інформаційної безпеки передбачає розробку чітких процедур і політик, які регулюють всі аспекти захисту інформації. Це включає регулярні аудити систем безпеки, навчання персоналу, створення планів реагування на інциденти та їх регулярне тестування. Важливо також мати механізми для постійного моніторингу та аналізу роботи системи безпеки, що дозволить своєчасно виявляти і усувати вразливості [9].

Ефективне управління інформаційною безпекою вимагає інтеграції технічних засобів захисту з організаційними заходами, а також постійного вдосконалення на основі нових загроз і викликів. Лише такий підхід дозволить забезпечити надійний захист інформаційних ресурсів в умовах швидкоплинного технологічного розвитку і глобальних змін.

Основними компонентами комплексної системи інформаційної безпеки є кілька важливих елементів: законодавча, економічна, програмно-технічна та адміністративно-управлінська складові. У межах єдиної системи забезпечення інформаційної безпеки корпорацій можна виділити державну та недержавну підсистеми.

Державна система представлена правоохоронними органами, спецслужбами та іншими державними установами, що мають на меті регулювання та контроль інформаційної безпеки. Ці органи розробляють законодавчі та нормативні акти, забезпечують дотримання стандартів безпеки та координацію дій у випадку масштабних кіберзагроз. Крім того, державні установи часто здійснюють моніторинг критичних інформаційних інфраструктур і надають підтримку в розслідуванні інцидентів. Недержавна система включає приватні охоронні компанії, охоронно-технічні підприємства, комерційні служби безпеки, інформаційні бюро, служби безпеки банків, а також профільні факультети та кафедри вищих навчальних закладів. Ці організації пропонують широкий спектр послуг: від консалтингу та аудиту безпеки до розробки і впровадження програмно-технічних рішень. Вони часто виступають партнерами державних органів у питаннях інформаційної безпеки, забезпечуючи оперативність і гнучкість реагування на нові загрози.

Законодавча складова відіграє ключову роль у створенні нормативно-правової бази, яка регулює аспекти інформаційної безпеки. Ефективні закони і нормативні акти забезпечують правову основу для дій державних та недержавних організацій, встановлюють вимоги до захисту інформації та визначають відповідальність за порушення.

Економічна складова включає фінансування заходів з інформаційної безпеки, розподіл ресурсів на розвиток і підтримку систем захисту, а також оцінку економічної ефективності впроваджених рішень. Інвестиції в інформаційну безпеку повинні бути виправданими та сприяти мінімізації ризиків для бізнесу.

Програмно-технічна складова охоплює впровадження сучасних технологій захисту інформації, розробку і використання програмного забезпечення, яке забезпечує шифрування, автентифікацію, моніторинг і виявлення загроз. Важливою є інтеграція різних технічних рішень у єдину систему, яка дозволяє ефективно управляти інформаційною безпекою.

Адміністративно-управлінська складова включає розробку політик і процедур, навчання персоналу, управління ризиками та координацію дій між різними підрозділами організації. Важливим аспектом є створення культури інформаційної безпеки серед співробітників, що забезпечить їхню залученість і відповідальність за захист інформаційних ресурсів.

Узгоджена взаємодія державної та недержавної систем забезпечення інформаційної безпеки, а також комплексний підхід до вирішення питань захисту інформації є запорукою надійного функціонування корпоративних

Передплатний індекс 21847

інформаційних систем в умовах глобалізаційних викликів.

До законодавчої компоненти слід віднести розроблення єдиної комплексної системо-утворюючої нормативно-правової бази, яка б регулювала функціонування та сприяла стимулюванню розвитку інформаційної безпеки корпоративної економіки. Законодавча база повинна включати стандарти, правила, положення та інструкції, що забезпечують правовий захист інформації, а також відповідальність за порушення цих норм. Це важливо для встановлення чітких рамок діяльності як для державних, так і для приватних установ, що забезпечують інформаційну безпеку.

Таким чином, інтегрований підхід до забезпечення інформаційної безпеки, що включає законодавчу та адміністративно-управлінську компоненти, дозволить створити ефективну та надійну систему захисту інформаційних ресурсів корпорацій. Це забезпечить не лише захист від кіберзагроз, але й сприятиме стійкому розвитку корпоративної економіки в умовах глобалізаційних викликів.

Значну увагу слід приділити економічній складовій, яка в умовах сучасної глобалізації повинна відігравати ключову роль у забезпеченні стабільного економічного зростання та підвищення конкурентоспроможності корпоративного сектору. Це включає створення умов для залучення інвестицій, забезпечення необхідних ресурсів для розвитку інформаційної безпеки та сприяння загальному економічному розвитку.

Економічна складова також має забезпечувати стабільне економічне зростання та підвищення конкурентоспроможності компанії; забезпечення пошуку та виділення необхідних ресурсів для розвитку інформаційної безпеки. Основною складовою для забезпечення інформаційної безпеки, на нашу думку, є програмно-технічна компонента. Загалом, інтеграція економічної та програмно-технічної компонент у стратегію інформаційної безпеки забезпечить надійний захист інформаційних ресурсів, сприятиме сталому економічному розвитку та підвищенню конкурентоспроможності корпоративного сектору в умовах глобалізації.

Необхідний рівень інформаційної безпеки забезпечується комплексом політичних, економічних та організаційних заходів, спрямованих на попередження, виявлення та нейтралізацію факторів і дій, що можуть завдати шкоди або перешкодити реалізації інформаційних прав, потреб та інтересів держави та її громадян. Ці заходи мають охоплювати всі аспекти управління інформаційною безпекою, забезпечуючи всебічний захист від можливих загроз.

З цього випливає, що для досягнення належного рівня інформаційної безпеки корпоративної економіки необхідно застосовувати широкий спектр політичних, економічних, організаційних та інших заходів. Ці заходи повинні сприяти реалізації інформаційних прав та інтересів корпорацій, забезпечуючи їхню безпеку та стійкий розвиток.

Впровадження процедур управління і забезпечення інформаційної безпеки компаній дозволяє: оптимізувати і обгрунтувати витрати на інформаційну безпеку; підвищити ефективність забезпечення інформаційної безпеки; забезпечити відповідність інформаційної безпеки як законодавчим, галузевим, внутрішньо-корпоративним вимогам, так і бізнес-цілям; знизити операційні витрати за рахунок формалізації і стандартизації управління інформаційною безпекою; підвищити довіру партнерів і клієнтів компанії; підвищити капіталізацію і вартість акцій корпорації; підвищити міжнародні рейтинги корпорації, необхідні для залучення зарубіжних інвестицій і виходу на міжнародні ринки; захистити інвестиції.

Таким чином, забезпечення інформаційної безпеки вимагає комплексного підходу, який включає політичні, економічні та організаційні заходи. Впровадження таких заходів не лише захищає корпоративні активи, але й сприяє сталому економічному розвитку, підвищенню конкурентоспроможності та залученню інвестицій.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Аналіз кібератак, підкреслив необхідність міжнародної співпраці в сфері кібербезпеки, обміну інформацією про загрози, розробці спільних стратегій захисту та спільні навчання, які могли б значно підвищити рівень готовності до подібних інцидентів. Для ефективного функціонування інформаційної безпеки в умовах глобалізації необхідно розглядати її як комплекс взаємодії державних і приватних систем захисту. Державні органи можуть надавати нормативну та законодавчу підтримку, розробляти стандарти безпеки і забезпечувати їх дотримання, а також координувати дії у випадку глобальних кіберзагроз. Приватні компанії, зі свого боку, повинні інвестувати в сучасні технології захисту, розробляти і впроваджувати власні політики безпеки, а також активно співпрацювати з державними структурами.

Передплатний індекс 21847

Ефективне управління інформаційною безпекою вимагає інтеграції технічних засобів захисту з організаційними заходами, а також постійного вдосконалення на основі нових загроз і викликів. Лише такий підхід дозволить забезпечити надійний захист інформаційних ресурсів в умовах швидкоплинного технологічного розвитку і глобальних змін.

В статті запропоновано розглянути основні компоненти комплексної системи інформаційної безпеки, які складаються з: законодавчої, економічної, програмно-технічної та адміністративно-управлінської складової. У межах єдиної системи забезпечення інформаційної безпеки корпорацій можна виділити державну та недержавну підсистеми. Інтегрований підхід до забезпечення інформаційної безпеки, що включає законодавчу та адміністративно-управлінську компоненти, дозволить створити ефективну та надійну систему захисту інформаційних ресурсів корпорацій. Це забезпечить не лише захист від кіберзагроз, але й сприятиме стійкому розвитку корпоративної економіки в умовах глобалізаційних викликів.

Література:

1. Концепція інформаційної безпеки України. URL: http://mip.gov.ua/files/banners/Final%20Проект%20концепції%20(Текст)%20-%2030.09.15.pdf.

2. Лужецький В. А., Кожухівський А. Д" Войтович О. П. Основи інформаційної безпеки: навч. посіб. Вінниця: ВНТУ, 2013. 221 с.

3. Маркіна І. А., Дячков Д. Н. Основи формування системи менеджменту інформаційної безпеки підприємства. Проблеми і перспективи розвитку підприємництва. 2016. № 3 (1). С. 80—88.

4. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видав. дім "Гельветика", 2017. 168 с.

5. Низенко Е. І., Каленяк Е. І. Забезпечення інформаційної безпеки підприємництва: навч. посіб. Київ: МАУП, 2006. 134 с.

6. Печенюк А. Особливості організації інформаційної безпеки сучасного підприємства. URL: http://sophus. at.ua/publ/2014_04_-17_18_kampodilsk/sekcija_4_2014_04_17_18/osoblivosti_organizaciji_informacijnoji_bezpeki_suchasnogo_pidpriemstva/54-1-0-931.

7. Сороківська О. А., Гевко Л. В, Інформаційна безпека підприємства: нові загрози та перспективи. Вісник Хмельницького нац. ун-ту. 2010. № 2, т. 2. С. 32—35.

8. Степанов В. Ю. Інформаційна безпека як складова державної інформаційної політики. Державне будівництво. 2016. № 2. С. 19.

9. Про Доктрину інформаційної безпеки України: Указ Президента України Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. URL: https://zakon.rada.gov.ua/laws/ show/47/2017.

References:

1. Ministry of Information Policy (2015), "The concept of information security of Ukraine", Available at: http://mip.gov.ua/files/banners/Final%20Проект%20Концепції%20(Текст)%20-%2030.09.15.pdf (Accessed 25 June 2024).

2. Luzhetskyi, V. A., Kozhukhivskyi, A. D., Voitovych, O. P. (2013), Osnovy informatsiinoi bezpeky. [Fundamentals of Information Security], VNTU, Vinnytsia, Ukraine.

3. Markina, I. A., Diachkov, D. V. (2016), "Fundamentals of formation of enterprise information security management system", Problemy i perspektyvy rozvytku pidpryiemnytstva, vol. 3 (1), pp. 80—88, available at: http,//nbuv.gov.ua/UJRN/piprp_2016_3(1)__18 (Accessed 25 June 2024).

4. Nashynets-Naumova, A. Yu. (2017), Informatsiina bezpeka, pytannia pravovoho rehuliuvannia, monohrafiia [Information security, issues of legal regulation], Helvetyka, Kyiv, Ukraine.

5. Nyzenko, E. I. and Kaleniak, V. P. (2006), Zabezpechennia informatsiinoi bezpeky pidpryiemnytstva, Navch. posib. [Ensuring information security of entrepreneurship], MAUP, Kyiv, Ukraine.

6. Pecheniuk, A. (2014), "Features of organization of information security of the modern enterprise", available at: http,//sophus.at.ua/publ/2014_04_ 17_18_kampodilsk/sekcija_4_-2014_04_17_18/osoblivosti_organizaciji_-informacijnoji_bezpeki_ suchasnogo_pidpriemstva/54-1-0-931 (Accessed 25 June 2024).

7. Sorokivska, O.A. and Gevko, V.L. (2010), "Enterprise Information Security, New Threats and Prospects", Visnik Hmelnickogo nacionalnogo universitetu, vol. 2 (2), pp. 32—35.

8. Stepanov, V. Yu. (2016), "Information security as a component of state information policy", Derzhavne budivnytstvo, vol. 2, pp. 1—9.

9 President of Ukraine (2016), Decree "On the decision of the National Security and Defense Council of December 29, "On the Doctrine of Information Security of Ukraine", available at: https,//zakon.rada.gov.ua/laws/show/47/2017 (Accessed 25 June 2024).

Стаття надійшла до редакції 10.07.2024 р.

Передплатний індекс 21847