УДК 004.056:658
DOI: 10.31673/2409-7292.2024.020012

Кицюк В. М., Пупинін О. С.

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА: ТЕОРЕТИЧНИЙ АСПЕКТ

З підвищенням ролі інформації формується інформаційний простір, який вимагає захисту від несанкціонованого чи ненавмисного впливу як на рівні держави, регіону так і на рівні підприємств. В процесі функціонування підприємств захист інформації дає можливість отримувати високі доходи, укладати вигідні контракти з контрагентами, суттєво підвищує рівень конкурентоспроможності підприємства, а також дозволяє значно підвищити ефективність діяльності організації загалом. У зв'язку з цим інформаційна безпека є невід'ємним елементом системи управління підприємством, а всі питання з цього напряму є актуальними. Мета статті полягає у проведенні аналізу статистичних даних щодо стану кібербезпеки на світовому ринку, дослідженні теоретичних аспектів сутності поняття «інформаційна безпека» та формуванні переліку принципів забезпечення інформаційної безпеки суб'єктів господарювання в умовах сьогодення. У статті розглянуто проблему забезпечення інформаційної безпеки в сучасних умовах. У процесі дослідження опрацьовано широкий перелік визначень поняття «інформаційна безпека» підприємства та надано авторське погляд щодо суті даної категорії. Описано внутрішні та зовнішні загрози, що виникають в інформаційному середовищі підприємства. Наведено класифікацію загроз інформаційної безпеки за головними ознаками. Особливу увагу приділено принципам інформаційної безпеки підприємства, застосування яких дозволить фахівцям побудувати та впровадити якісну систему забезпечення інформації у виробничі процеси підприємства.

Ключові слова*:* інформаційна безпека, загрози, принципи, підприємство.

Вступ

В умовах активного та безперервного розвитку інформаційних технологій, трансформації та цифровізації світової економіки ядром всіх державних та бізнес-процесів стає інформація. Щодня, потік інформації, збільшується в геометричній прогресії. Керівники підприємств не можуть уявити свого функціонування без інформації та інформаційних технологій: соціальні мережі, месенджери, інтернет-магазини, онлайн-банкінг тощо. Всі ці засоби зв'язку та комунікацій використовує підприємство в залежності від запитів ринку та споживачів, але всі ці точки доступу потенційно є вразливими. Дійсно, з підвищенням ролі інформації формується інформаційний простір, який вимагає захисту від несанкціонованого чи ненавмисного впливу як на рівні держави, регіону так і на рівні підприємств. В процесі функціонування підприємств захист інформації дає можливість отримувати високі доходи, укладати вигідні контракти з контрагентами, суттєво підвищує рівень конкурентоспроможності підприємства, а також дозволяє значно підвищити ефективність діяльності організації загалом. У зв'язку з цим інформаційна безпека є невід'ємним елементом системи управління підприємством, а всі питання з цього напряму є актуальними.

Аналіз публікацій

Під час проведення аналітичного огляду науково-теоретичної бази, присвяченої проблемам інформаційної безпеки, виявлено прогалину в роботах вчених, що систематизують розрізнені матеріали. Поняття «інформаційної безпеки підприємства» розглядали І.М. Близнюк, О.Р. Братель, В.О. Бондаренко, І.Л. Бучило, С.О. Гахов, О.М. Горбатюк, М.О. Гуцалюк, Г.І. Гайдур, В.А. Козачок, С.В. Легомінова, О.В. Олійник, В.П. Пономарьов, А.А. Стрельцов, В.А. Савченко, В.Л. Цимбалюк, Т.І. Чубарук, В.І. Шульга, Ю.М. Якименко та інші. Однак на суб'єктивну думку авторів цієї статті, ступінь наукової розробленості різних аспектів інформаційної безпеки підприємств України залишається на низькому рівні. Зокрема, під час проведення аналітичного огляду науково-теоретичної бази, присвяченої проблемам інформаційної безпеки, виявлено прогалину в роботах з теоретичних питань, що становлять теоретичну основу інформаційної безпеки. Подібні роботи є теоретичним фундаментом для фахівців, які займаються вивченням вузьких проблем інформаційної безпеки. Отже, через безперервне зростання значимості інформаційної безпеки в діяльності підприємств, дане дослідження є актуальним та необхідним.

Мета статті полягає у проведенні аналізу статистичних даних щодо стану кібербезпеки на світовому ринку, дослідженні теоретичних аспектів сутності поняття «інформаційна

безпека» та формуванні переліку принципів забезпечення інформаційної безпеки суб'єктів господарювання в умовах сьогодення.

Виклад основного матеріалу.

У світі інформаційна безпека відіграє важливу роль. В умовах сьогодення статистика кібербезпеки змінюється щохвилини, кіберзагрози стають все більш небезпечними, більш складними та важкими для виявлення. Згідно зі Звітом про кіберзагрози за 2023 рік від SonicWall, вперше з 2018 року атаки шкідливих програм знову набирають обертів. За їх даними, кількість атак зросла до 5,5 мільярдів, що на 2% більше, ніж у попередньому 2022 році. Таке суттєве зростання спричинене значним зростанням інтенсивності криптоджекінгу та шкідливого програмного забезпечення для Інтернету речей (IoT). Дослідження, доводять, що людський фактор є причиною приблизно 88% всіх витоків даних. Особливо це стосуються працівників, які виконують роботу дистанційно. За даними IBM Security, середній час виявлення та усунення витоку даних у 2021 році становив 287 днів. Тривалий час реагування пов'язаний зі зростаючою складністю кібератак, обмеженим досвідом у сфері безпеки та складним IT-середовищем. Згідно зі Звітом Black Kite 2023 Ransomware Landscape Report, кількість постраждалих від програм-вимагачів, зареєстрованих у березні 2023 року, майже вдвічі перевищила показник квітня 2022 року та в 1,6 рази – показник найвищого місяця 2022 року [1].

Враховуючи важливість інформаційної безпеки у діяльності підприємств, проведемо дослідження щодо сутності цієї дефініції. Вченими доведено, що трактування поняття «інформаційна безпека» на рівні підприємства досить неоднозначне. Це свідчить про те, що немає єдиного підходу до її визначення, оскільки сутність даної категорії залежить від багатьох обставин, якими характеризується інформаційна система підприємства Найбільш поширені визначення поняття «інформаційна безпека» представлені у табл. 1.

Таблиця 1

Зміст поняття «інформаційна безпека підприємства»

Автори	Визначення
Закон України «Про телекомунікації»	здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації [2]
Якименко Ю.М., Савченко В.А., Легомінова С.В.	стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій, держав [3]
Козачок В.А., Гайдур Г.І., Гахов С.О.	події, які шляхом потенційно можливого впливу на інформаційну систему прямо та/або опосередковано завдають збитку її власникам і користувачам [4]
Шульга В. І.	стан інформаційної системи, у якому вона може протистояти впливу внутрішніх і зовнішніх ризиків, не ініціюючи їхнє виникнення для елементів системи й зовнішнього середовища [5]
Забродський В.А.	кількісна і якісна характеристика властивостей фірми, що відбиває здатність «самовиживання» і розвитку в умовах виникнення зовнішньої і внутрішньої економічної загрози [6, с.35]
Камлика М.І.	стан розвитку суб'єкта господарювання, який характеризується стабільністю економічного та фінансового розвитку, ефективністю нейтралізації негативних факторів і протидії їх впливу на всіх стадіях його діяльності [7, с. 9].
Гладченко Т.Н.	захищеність життєво важливих інтересів підприємства від внутрішніх і зовнішніх загроз, організація якої здійснюється адміністрацією й колективом підприємства шляхом реалізації системи заходів правового, економічного, організаційного, інженернотехнічного й соціально-психологічного характеру [8, с.111-113]
Ніколаюк С.І., Никифорчук Д.Й.	стан юридичних, виробничих відносин і організаційних зв'язків, матеріальних і інтелектуальних ресурсів, щодо яких гарантується стабільність функціонування, фінансово-комерційний успіх, прогресивний науково-технічний і соціальний розвиток [9, с. 15].
Могильний А.І., Безчастний В.М., Винокуров Ю.О.	забезпечення стану життєдіяльності, при якому реалізуються його основні інтереси, воно захищено від внутрішніх та зовнішніх загроз і дестабілізуючих чинників [10, с.9].

Теоретичний аналіз доводить, що сутність поняття «інформаційна безпека» є неоднорідною та багатогранною в її трактуванні. На погляд авторів, «інформаційна безпека» - це стан інформаційного середовища господарюючого суб'єкта, при якому зберігаються властивості інформації й інформаційних потоків, та створюються умови протистояння впливу внутрішніх і зовнішніх загроз з метою досягнення бізнес-цілей підприємства.

У випадку із зовнішніми атаками здійснюється пошук вразливості в інформаційній структурі для доступу до основних вузлів, сховищ, персональних комп'ютерів співробітників, організаційної мережі тощо. Його використовують для завдання шкоди об'єктам копіювання, видозміни, шпигунства, відключення систем захисту, знищення тощо. До зовнішніх загроз відносять: шкідливе програмне забезпечення; спам; промислове шпигунство; мережеві вторгнення; крадіжка мобільних пристроїв та великого обладнання; таргетовані (цільові) атаки; злочинне шкідництво тощо.

До внутрішніх загроз відносять дії чи бездіяльність (навмисні чи не навмисні) співробітників, що протидіють інтересам діяльності підприємства, наслідком яких може бути нанесення економічних збитків компанії, втрата інформаційних ресурсів, підрив ділового іміджу компанії, виникнення проблем у відносинах з реальними чи потенційними партнерами тощо. До внутрішніх загроз відносять: вразливість у програмному забезпеченні; випадкові витікання з вини співробітників; наміри витоку через співробітників; витоку або неналежному обміну інформацією через мобільні пристрої; втрата мобільних пристроїв працівниками; шахрайство працівників. Класифікацію загроз безпеки за основними ознаками представлено на рис. 1.

Рис. 1. Класифікація загроз інформаційної безпеки [4]

Порушення інформаційної безпеки за результатами впливає на загрози, зокрема:

даним підприємства в системі управління ним: втрата даних; викривлення даних; відмова у даних; порушення конфіденційності; крадіжка даних; атаки; хибні ідентифікації;

обладнанню підприємства: відмови; вихід з ладу; завади; перегрів; електромагнітні наведення; волога.

Інформаційна безпека на будь-якому рівні управління формується на основі фундаментальних принципів, які є вихідними положеннями, нормами і правилами поведінки, які диктують усім суб'єктам господарювання (рис. 2).

Рис. 2. Принципи забезпечення інформаційної безпеки [11]

Принцип законності в контексті захисту інформаційної безпеки передбачає використання механізмів, що гарантують дотримання підприємствами правових норм та забезпечення відповідності чинного законодавства України в цій сфері. Також підприємствам важливо дотримуватися пріоритету міжнародних норм та принципів, які стосуються захисту інформації, що може включати укладення міжнародних договорів та співпрацю з іноземними державами.

Принцип права власності в контексті захисту інформаційної безпеки передбачає забезпечення прав суб'єктів на інформацію, яка створена ними або належить їм на законних підставах. Важливо, щоб обмеження прав на таку інформацію були встановлені тільки чинним законодавством та не перевищували необхідних меж для забезпечення інформаційної безпеки підприємства. Один з аспектів проблеми захисту прав власності на об'єкти промислової власності полягає у зіткненні інтересів між створювачем такого об'єкту та суспільством в цілому, яке може мати претензії на певну частину вартості цього об'єкту. Необхідно знайти баланс між цими інтересами та гарантувати забезпечення прав власника на його об'єкт інтелектуальної власності. Другий аспект пов'язаний з умовами застосування патенту - обмеженої строком монополії на певне технічне рішення. При цьому важливо встановлювати чіткі підстави для видання патенту та не допускати зловживання монопольним становищем. Дотримання цих принципів дозволить запобігти обмеженням конкуренції та забезпечити ефективне функціонування антимонопольного законодавства.

Принцип економічної доцільності в системі забезпечення інформаційної безпеки передбачає оцінювання секретності та конфіденційності як ключових параметрів продукту та їх включення до загальної ціни продукту на підставі законодавства. Даний принцип передбачає необхідність всебічного аналізу можливої економічної шкоди для суб'єкта господарювання та врахування усіх негативних наслідків, пов'язаних з порушенням захисту

© Кицюк, В. М., & Пупинін, О. С. (2024). Інформаційна безпека підприємства: теоретичний аспект. Сучасний захист інформації, 2(58), 103–108. https://doi.org/10.31673/2409-7292.2024.020012.

інформації. Цей принцип має прямий вплив на фінансову діяльність підприємств, оскільки розмір економічної шкоди, пов'язаної з можливим порушенням захисту інформації, може бути значним. Це допомагає зменшити ризики, пов'язані з можливими порушеннями захисту інформації, та забезпечити стабільність фінансової діяльності підприємства.

Принцип комплексного підходу до організації забезпечення інформаційної безпеки передбачає створення взаємозв'язаної системи заходів, розроблених для забезпечення безпеки інформації на підприємстві. Цей принцип передбачає використання сил, засобів та методів, спрямованих на забезпечення захисту інформації підприємства, які повинні бути взаємодіючими та взаємозалежними.

Комплексний підхід у системі забезпечення інформаційної безпеки дозволяє створити єдину цілісну систему, яка включає у себе заходи з організації фізичної та технічної безпеки інформації, захисту від електронних атак, контролю доступу, а також забезпечення безпеки персоналу та кадрових рішень. Врахування принципу комплексного підходу до забезпечення інформаційної безпеки дозволяє підприємствам забезпечити єдність в рішеннях, пов'язаних з виробничою, комерційною та фінансовою діяльністю підприємства. Цей підхід допомагає забезпечити спільність підходів до забезпечення інформаційної безпеки та координацію роботи всіх підрозділів підприємства. Крім того, комплексний підхід сприятиме зменшенню можливих помилок, що виникають при взаємодії окремих елементів системи захисту інформації. В результаті, це створить умови до надійності та ефективності системи забезпечення інформаційної безпеки на підприємстві.

Принцип безперервності забезпечення інформаційної безпеки передбачає використання загальних та спеціальних засобів та методів для забезпечення безперебійного захисту інформації на всіх етапах її життєвого циклу. Врахування даного принципу у системі забезпечення інформаційної безпеки підприємства передбачає регулярне застосування активних, превентивних, ефективних та різноманітних заходів і спеціальних методів для забезпечення безпеки інформації.

Безперервність забезпечення інформаційної безпеки допоможе забезпечити безпеку інформації та її обігу в будь-який час та в будь-яких умовах. Цей принцип передбачає регулярне проведення аудитів та тестувань системи забезпечення інформаційної безпеки з метою виявлення потенційних проблем та вдосконалення системи захисту. Врахування принципу безперервності забезпечення інформаційної безпеки дозволяє забезпечити надійний та стійкий захист інформації та зменшити ризики порушення її конфіденційності, цілісності та доступності. Цей принцип дозволяє підприємствам забезпечувати безпеку інформації в будь-який час та в будь-яких умовах, що сприяє забезпеченню континуїтету бізнесу та стійкості діяльності підприємства.

Принцип єдиноначальності передбачає, що відповідальність за забезпечення інформаційної безпеки покладається на керівників підприємств, які здійснюють діяльність, що пов'язана з захистом конфіденційної інформації. Даний принцип передбачає, що кожен суб'єкт господарювання несе відповідальність за забезпечення безпеки своєї інформації та покладає обов'язки інших суб'єктів у сфері захисту своєї інформації. Керівники організацій, де зберігається конфіденційна інформація, зобов'язані забезпечувати високий рівень захисту даних та приймати необхідні заходи для запобігання можливих загроз. Принцип єдиноначальності передбачає активну взаємодію між різними суб'єктами господарювання з метою обміну досвідом та координації дій. Це сприяє забезпеченню високого рівня захисту інформації в рамках всієї системи, а також зменшенню ризиків порушення конфіденційності, цілісності та доступності інформації.

Висновки

Неможливо переоцінити значущість інформаційної безпеки у світі як для світового суспільства, окремої держави чи підприємства. Безліч підходів до розуміння основ інформаційної безпеки дозволяє зробити висновок про дискусійний характер цієї проблеми.

© Кицюк, В. М., & Пупинін, О. С. (2024). Інформаційна безпека підприємства: теоретичний аспект. Сучасний захист інформації, 2(58), 103–108. https://doi.org/10.31673/2409-7292.2024.020012.

Інформаційна безпека – критично важлива та багатогранна проблема, складність та глибина якої потребує безперервного проведення якісних наукових досліджень. Останні дозволять як сформувати велику науково-теоретичну базу щодо стану та перспектив застосування інформаційної безпеки на рівні суб'єктів господарювання, а й стане серйозною теоретичною підмогою для фахівців з інформаційної безпеки.

У досліджені з'ясовано, що єдиної оптимальної структури захисту інформації немає, оскільки кожна організація – учасник інформаційних процесів – має свій власний набір вимог, проблем та пріоритетів, продиктованих об'єктивними економічними, виробничими, соціальними умовами функціонування цього підприємства. З цього приводу надано характеристику принципів забезпечення інформаційної безпеки, застосування яких в діяльності підприємств сприятиме розробці вихідних положень, норм і правил поведінки, що допоможе керівникам створити ефективний механізм захисту даних та безпеки інфраструктури підприємства.

Перелік посилань

1. Топ 20 приголомшливих статистичних фактів пов'язаних з витоками даних у 2023 році. Режим доступу: http://surl.li/meqsk
2. Закон України «Про телекомунікації» № 1089-IX від 16.12.2020. ВВР 2020.
3. Якименко, Ю. М., Савченко, В. А., Легомінова, С. В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: Державний університет телекомунікацій, 2022. 308 с.
4. Козачок, В. А., Гайдур, Г. І., Гахов, С. О., Хмелевський, Р. М., Чумак, Н. С. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів. Київ: ДУТ ННІЗІ, 2020.167 с.
5. Шульга, В. І. Сучасні підходи до трактування поняття інформаційна безпека. Ефективна економіка № 4, 2015. Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=5514
6. Забродський, В. А., Кізім, Н. А., Янов, Л. І. Сучасні методи організації та управління промисловим виробництвом. Харків: АТ «Бізнес-Інформ», 1997. 64.
7. Камлик, М. І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект [Текст] : навч. посіб. К. : Атіка, 2005. 432 с
8. Гладченко, Т. М. Індикатори економічної безпеки підприємницької діяльності. Донецьк: ДонДАУ. Менеджер. 2000. №12. С.111-113.
9. Ніколаюк, С. І., Никифорчук, Д. Й. Безпека суб'єктів підприємницької діяльності [Текст] курс лекцій К. : КНТ, 2005. 320с.
10. Могильний, А. І., Безчастний, В. М., Винокуров, Ю. О. Основи безпеки бізнесу. Донецьк: Регіон, 2000. 130 с.
11. Олійник, О. В. Принципи забезпечення інформаційної безпеки України. Науковий вісник Ужгородського університету. 2012. Випуск 18. С. 170-173.

Надійшла 18.05.2024