МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ
АГРАРНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ОБЛІКУ І ФІНАНСІВ

ЗБІРНИК ТЕЗ

науково-практичної конференції

«ОБЛІКОВО-ФІНАНСОВЕ, ІНФОРМАЦІЙНЕ ТА МОВНО-КОМУНІКАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ СТАЛОГО РОЗВИТКУ АГРАРНОГО СЕКТОРУ: ПЕРСПЕКТИВИ ТА РЕАЛІЇ»

18-20 березня 2025 року

Дніпро 2025

РОЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЗАБЕЗПЕЧЕННІ УПРАВЛІННЯ СИСТЕМОЮ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Сергій ЮРЧЕНКО, к. е. н., доцент, доцент кафедри обліку, оподаткування та управління фінансово-економічною безпекою,
Тетяна МАЧАК, старший викладач кафедри обліку, оподаткування та управління фінансово-економічною безпекою
Дніпровський державний аграрно-економічний університет, м. Дніпро, Україна

На сьогодні вагомий вплив на безпеку підприємств має інформаційна складова економічної безпеки. Це пояснюється тим, що в сучасному світі обмін інформацією став ключовим елементом економічної діяльності. Розвиток інформаційних технологій, автоматизація робочих місць, введення електронного документообігу та ряд інших чинників сприяють ефективному використанню як людських так і матеріальних ресурсів. Поряд з цим у підприємств виникає залежність від інформаційних технологій при виробництві продукції, маркетингу, обслуговування клієнтів та інших аспектів свого бізнесу. Це створює унікальні виклики і загрози, такі як кібератаки, витоки даних та інші форми кіберзлочинності, які можуть серйозно підірвати довіру клієнтів, призвести до фінансових втрат і пошкодити репутацію компанії. Таким чином, забезпечення безпеки інформації є необхідною умовою для забезпечення економічної безпеки підприємства та успішної діяльності будь-якого сучасного підприємства.

Економічна безпека виступає важливим елементом успіху і стабільності підприємств і залежить від здатності керівників вчасно реагувати на потенційні загрози та швидко адаптуватися до змін в економічному середовищі. При цьому, кожна складова економічної безпеки, включаючи фінансову, правову, кадрову, технологічну та інформаційну, має свою вагу і впливає на загальний стан підприємства. Досліджуючи структуру економічної безпеки, важливо враховувати, що всі компоненти взаємопов'язані між собою і є основою для стабільного розвитку підприємства.

Кожна з цих складових є важливою для забезпечення ефективності економічної безпеки підприємства. Взаємодія між ними і формування комплексного підходу дозволяє підприємству оптимізувати свою діяльність, зменшити ризики та забезпечити стійкість у складних умовах ринкової конкуренції.

В законодавстві України, питання інформаційної безпеки знайшли своє відображення у Законі України «Про основні принципи розвитку інформаційного суспільства в Україні на період 2007–2015 років», в якому визначено поняття «інформаційна безпека» як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження,

використання і порушення цілісності, конфіденційності та доступності інформації.

Забезпечення інформаційної безпеки стає дедалі важливішим аспектом управління підприємством в сучасному світі. Швидкі темпи технологічного розвитку та поширення цифрових інструментів створюють нові можливості для бізнесу. Сучасні підприємства активно використовують передові технології та автоматизовані системи обліку для оптимізації своєї роботи та забезпечення конкурентоспроможності. Використання різних технічних засобів комунікації для передачі і зберігання інформації, перехід до автоматизованих систем обліку і документообігу, впровадження аналітичних систем для обробки даних - все це призводить до накопичення значного обсягу інформації, яка обробляється та зберігається для подальшого аналізу і використання. Зростаючий обсяг даних та його розміщення на цифрових носіях створює нові загрози безпеки інформації. Тому, важливо створити умови для забезпечення збереження інформації, щоб запобігти її витоку, викривлення, викрадення або знищення, особливо враховуючи конфіденційний характер інформаційних даних. Це вимагає від керівництва ретельного планування, постійного моніторингу та готовності до оперативного реагування на можливі загрози.

Загрози інформаційній безпеці охоплюють усі наявні та потенційні чинники, які можуть створювати небезпеку і загрожувати інтересам підприємства у різних сферах діяльності. Основою ефективного захисту є глибоке розуміння різноманітності загроз, які можуть виникнути, та методів їх класифікації. Залежно від критеріїв, можливо виділити різні підходи до розуміння та боротьби з потенційними небезпеками.

В залежності від джерела походження, загрози поділяють на екзогенні, що виникають зовні підприємства та зазвичай не залежать від його діяльності та ендогенні, які виникають всередині самого підприємства через його власну діяльність або недоліки у внутрішніх процесах.

Розглядаючи загрози за способом виникнення, можна розділити їх на активні і пасивні. Активні загрози включають в себе навмисне втручання атакуючих, наприклад, хакерські атаки, вірусні пошкодження, фішингові атаки тощо. Пасивні загрози, навпаки, виникають без безпосередньої участі зловмисників, наприклад, втрата даних через несправність обладнання, несанкціонований доступ через некомпетентність працівника тощо.

За способами протидії загрозам розрізняють превентивні заходи та реагувальні. Превентивні заходи, що спрямовані на запобігання виникненню загроз, наприклад, встановлення брандмауерів, оновлення програмного забезпечення. Реагувальні заходи, спрямовані на виявлення і ліквідацію вже існуючих загроз, наприклад, резервне копіювання даних, антивірусні системи тощо.

Особливу увагу слід звернути на типи шкоди, яку можуть завдати загрози, серед яких виділяють фінансові та репутаційні наслідки. Фінансові загрози призводять до фінансових втрат, наприклад, крадіжка даних для

фінансових транзакцій, несанкціонований доступ до конфіденційної інформації тощо. Репутаційні ризики впливають на репутацію підприємства, такі як розголошення конфіденційної інформації, порушення законодавства з захисту даних тощо.

Для забезпечення інформаційної безпеки підприємства та сталого розвитку бізнесу, важливо виконати ряд завдань, серед яких створення та впровадження комплексного плану інформаційної безпеки, розробка якого дозволить не тільки передбачити потенційні загрози, але й ефективно адаптуватися до них, враховуючи особливості діяльності і потреб компанії.

Структура та основні напрямки дій у рамках розробки комплексного плану забезпечення інформаційної безпеки підприємства повинні передбачати регулярне оновлення заходів безпеки і включати в себе не тільки технічні аспекти, такі як захист від вірусів та шкідливого програмного забезпечення, але й організаційні заходи, такі як навчання персоналу основам кібергігієни та встановлення чітких правил реагування на інциденти.

Важливою складовою для підвищення ефективності плану є також розробка стратегії відновлення після настання можливих інцидентів, яка повинна включати в себе наступні практики:

1. Організація системного резервного копіювання важливих даних, зокрема конфіденційної інформації та облікових даних у надійні хмарні сховища;
2. Захист даних, що зберігаються в хмарі, шляхом їх шифрування для забезпечення конфіденційності;
3. Впровадження корпоративної електронної пошти для обміну інформацією та спільної роботи з документами, що забезпечує додатковий рівень захисту;
4. Розподіл прав доступу до важливих інформаційних ресурсів, в тому числі облікових даних між визначеними співробітниками;
5. Застосування двофакторної аутентифікації для надійного підтвердження особистості користувачів;
6. Використання сучасних комунікаційних платформ для забезпечення ефективної взаємодії між співробітниками під час дистанційної роботи;

Додатково, важливим аспектом забезпечення інформаційної безпеки підприємства. є посилення вимог до співробітників, особливо бухгалтерів, у сфері обробки інформації та використання сучасних технічних.

Розробка та впровадження навчальних програм, спрямованих на підвищення обізнаності та навичок персоналу щодо коректного використання технологій та обробки конфіденційної інформації, може допомогти пристосувати співробітників до нових вимог та підтримати високий рівень їхньої кваліфікації.

Це допоможе уникнути можливих ризиків безпеки, пов'язаних з недбалістю або неправильним використанням технічних засобів, а також збільшить загальний рівень захищеності інформації на підприємстві.

ІНФОРМАЦІЙНІ СИСТЕМИ І ТЕХНОЛОГІЇ

РОЗУМНІ МІСТА: ВИКОРИСТАННЯ ІОТ ДЛЯ УПРАВЛІННЯ ІНФРАСТРУКТУРОЮ МІСТА

Олександр КАРАМУШКА, к. е. н., доцент, в. о. завідувача кафедри інформаційних систем і технологій
Дніпровський державний аграрно-економічний університет, м. Дніпро, Україна

Розумні міста – це концепція, яка набирає все більшої популярності в умовах стрімкого розвитку технологій та урбанізації. Вона полягає у використанні інформаційно-комунікаційних технологій для покращення якості життя жителів міста, підвищення ефективності управління та оптимізації використання ресурсів. Одним із важливих аспектів розумних міст є Інтернет речей (IoT), який дозволяє інтегрувати різні елементи інфраструктури міста в єдину систему, що дозволяє автоматизувати процеси та приймати рішення на основі даних у реальному часі. У цьому контексті використання IoT для управління інфраструктурою міста відіграє ключову роль у забезпеченні ефективності функціонування таких мегаполісів.

Інтернет речей у розумних містах являє собою мережу датчиків, пристроїв та інших об'єктів, які збирають і обмінюються даними між собою. Ці дані можуть стосуватися різних аспектів міського життя: від стану дорожнього руху і рівня забруднення повітря до використання енергоресурсів і безпеки громадян. IoT дає можливість здійснювати моніторинг і контроль за багатьма параметрами інфраструктури міста в режимі реального часу, що дозволяє своєчасно реагувати на зміни та оптимізувати роботу міських систем.

Одним із важливих напрямків використання IoT є управління транспортною інфраструктурою. Для цього в різних точках міста встановлюються сенсори, які фіксують швидкість руху транспорту, кількість автомобілів, інтенсивність заторів тощо. Ці дані передаються до центральної системи, яка аналізує інформацію і на основі цього приймає рішення про регулювання світлофорів, зміну маршрутів автобусів чи тролейбусів або введення тимчасових обмежень на певних ділянках доріг.

Інша важлива галузь, де IoT використовує свій потенціал – це енергетика. Важливим аспектом сталого розвитку розумних міст є раціональне використання енергетичних ресурсів. Завдяки IoT можна здійснювати моніторинг споживання електроенергії в реальному часі, що дозволяє як приватним користувачам, так і підприємствам оптимізувати свої витрати на енергію. У розумних будинках встановлюються датчики, які регулюють температуру, освітлення та інші параметри в залежності від потреби. Крім того, можна використовувати технології для інтеграції відновлюваних джерел енергії, таких як сонячні панелі чи вітряки, з енергосистемою міста. Це дозволяє зменшити залежність від традиційних джерел енергії та знижує витрати на електроенергію.

Управління водними ресурсами є ще однією важливою сферою застосування IoT в розумних містах. Використання сенсорів для моніторингу рівня води, витрат води та її якості дозволяє знижувати витрати на

ІНФОРМАЦІЙНІ СИСТЕМИ І ТЕХНОЛОГІЇ