УДК 338.4

М. В. Болдуєв,
д. держ. упр., професор, НУ "Запорізька політехніка"
ORCID ID: https://orcid.org/0000-0002-8889-6555
О. В. Болдуєва,
д. е. н., доцент, Запорізький національний університет
ORCID ID: https://orcid.org/0000-0001-5267-1816
О. Г. Лищенко,
к. е. н., доцент, НУ "Запорізька політехніка"
ORCID ID: https://orcid.org/0000-0001-9211-9567

DOI: 10.32702/2306-6792.2024.13.40

СУЧАСНІ ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ТА БЕЗПЕКИ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

M. Bolduiev,
Doctor of Public Administration, Professor, National University "Zaporizhzhia Polytechnic"
O. Bolduieva,
Doctor of Economic Sciences, Associate Professor, Zaporizhzhia National University
O. Lyshchenko,
PhD in Economics, Associate Professor, National University "Zaporizhzhia Polytechnic"

MODERN APPROACHES TO ENSURING THE RELIABILITY AND SECURITY OF INFORMATION IN CORPORATE TELECOMMUNICATIONS SYSTEMS

Стаття зосереджена на аналізі надійності та безпеки телекомунікаційних мереж, з особливим акцентом на корпоративні системи, які використовуються в електронній комерції. Описуються ключові параметри оцінки ефективності мереж, такі як продуктивність, надійність, безпека, масштабованість та можливість розширення. Також розглядається важливість врахування міжнародних та національних стандартів у телекомунікаціях для забезпечення узгодженості та відповідності систем світовим вимогам.

В статті аналізуються різні методи та стратегії, що забезпечують надійність телекомунікаційних мереж, включаючи технічні і організаційні заходи безпеки. Обговорюються сучасні підходи до захисту даних, такі як багатошарова модель безпеки, криптографія, регулярний аудит, фізичний захист обладнання та розробка комплексних політик безпеки в компанії. Вказується на важливість резервного копіювання та відновлення даних як елемента підвищення надійності систем. Зазначається, що залучення міжнародних практик та стандартів може значно підвищити захищеність та стійкість інформаційних ресурсів компанії, що є критично важливим для підтримки її конкурентоспроможності.

The article provides a thorough analysis of the reliability and security of telecommunication networks, especially in the context of their use in corporate systems and electronic commerce. The key parameters for evaluating the effectiveness of networks are highlighted, such as performance, reliability, security, extensibility and scalability. Particular attention is paid to the analysis of standards and regulations regulating international and national activities in the field of telecommunications, as this contributes to the unification of technical requirements and facilitates the integration of Ukrainian systems into global networks.

Передплатний індекс 21847

The study expands by examining in detail the technical and organizational strategies that enhance the reliability of telecommunication systems. Considerable attention is paid to modern methods of data protection, including a multi-layered security model, cryptography, regular monitoring and auditing, physical protection of equipment, and the development and implementation of internal security policies. Particular emphasis is placed on the importance of a comprehensive approach to data backup and recovery to ensure business continuity and protection against potential cyber threats.

The authors emphasize the need for strategic planning and active risk management in the field of corporate information security. This involves not only implementing advanced technical solutions, but also regularly updating security policies to adapt to dynamically changing conditions and threats in the digital environment. Such an approach allows companies not only to respond to challenges, but also to proactively anticipate potential problems, thereby increasing their resilience and ability to quickly recover from incidents.

Conclusions were made about the importance of a comprehensive approach to ensuring the reliability and security of corporate telecommunications networks. The authors claim that the effectiveness of system protection increases significantly when using various defense layers, which include both physical and software security measures. Emphasis is also placed on the importance of using international practices and standards, which contributes to increasing the security of information resources and ensures the competitiveness of companies on the global market.

Ключові слова: телекомунікаційні мережі, надійність, безпека, електронна комерція, мережева ефективність, стандарти, управління ризиками.

Key words: telecommunication networks, reliability, security, electronic commerce, network efficiency, standards, risk management.

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

Актуальність досліження проблематики забезпечення надійності та безпеки інформації в корпоративних телекомунікаційних системах обумовлена стрімким розвитком технологій та збільшенням залежності бізнесу від стабільності та безпеки інформаційних систем. У контексті глобалізації та цифровізації економіки, корпоративні мережі стають ключовим елементом управління, продажів, збору даних і комунікацій між підрозділами компаній, розташованими у різних географічних локаціях. Надійність та безпека цих систем напряму впливають на оперативність реагування на зміни ринкових умов, захист конфіденційної інформації та стійкість бізнесу до кіберзагроз.

Поширення мережевих технологій зумовлює зростання кіберзагроз, які можуть призвести до витоку даних, втрати інформації або навіть повного паралічу діяльності підприємства. Тому вивчення сучасних методів та засобів забезпечення надійності і безпеки інформації стає важливим завданням для підвищення ефективності управління ризиками та захисту стратегічних ресурсів компаній. Розробка нових підходів, які включають використання передових технологій криптографічного захисту, систем детекції вторгнень та автоматизованих інструментів для моніторингу стану мереж, є критично важливою для адаптації підприємств до швидкозмінних умов кіберпростору.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

До провідних західних науковців, які зробили суттєвий внесок у дослідження надійності та безпеки інформації в корпоративних телекомунікаційних системах слід віднети вчених, які відомі своїми доробками у цій сфері: Bruce Schneier, Ross Anderson, Whitfield Diffie, Martin Hellman, Ronald Rivest, Adi Shamir, Leonard Adleman, Charlie Miller, Dan Boneh, Kevin Mitnick, Gene Spafford, Stefan Savage. Ці вчені та їх роботи значно вплинули на розвиток концепцій і технологій у сфері надійності та безпеки інформації в корпоративних мережах.

Дослідженню проблематики підвищення ефективності та забезпечення безпеки корпоративних інформаційних мереж присвятили свою увагу багато українських науковців. Так пошуку шляхів удосконалення методичного інструментарію, технологій та стратегій, що використовуються для підвищення надійності та безпе-

Передплатний індекс 21847

ки інформації у корпоративних мережах присвятили свої роботи Вівчар О. І., Князєва Н. О., Копитін Ю., Креденцер Б. П., Лежнюк П. Д., Могилевич Д. І., Остапенко В. О., Пермяков О. Ю., Танцюра Л. І., Цуркан В., Шатарський А. Я., Шолом П. С. та ін. Водночас зважаючи на багатогранність зазначеної проблематики наявна потреба подальших комплексних досліджень з метою розробки нових і інтеграції існуючих технологій побудови та управління корпоративними мережами з огляду на поточні та майбутні потреби бізнесу в контексті глобалізації та цифрової трансформації

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Метою статті є дослідження та аналіз різноманітних методів, технологій та стратегій, що використовуються для підвищення надійності та безпеки інформації у корпоративних мережах. Стаття покликана виявити, оцінити та порівняти ефективність сучасних алгоритмів, апаратних засобів і програмних рішень, здатних мінімізувати ризики витоку даних, кібератак та інших загроз. Окрема увага приділяється вивченню інтеграції цих технологій в існуючі корпоративні системи, з огляду на поточні та майбутні потреби бізнесу в контексті глобалізації та цифрової трансформації.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Телекомунікаційні мережі охоплюють такі системи, як комп'ютерні мережі, телефонні мережі, радіомережі та мережі телебачення. Вивчення теоретичних та практичних аспектів цих мереж вказує на ключові параметри для оцінки їх ефективності, включаючи продуктивність, надійність, безпеку, можливість розширення, масштабованість, прозорість, підтримку різноманітних видів трафіку, управління та сумісність. Зазвичай під "якістю обслуговування" мережі розуміють такі важливі атрибути, як продуктивність та надійність.

В аналізі безпеки та надійності мереж важливо враховувати такі показники, як частота збоїв, середній час роботи до першого збою, інтенсивність збоїв, готовність до роботи, захист та збереження даних від спотворень, узгодженість даних, гарантія доставки пакетів без спотворень, ризик втрати пакетів, імовірність спотворення даних, співвідношення втрачених і доставлених пакетів, здатність системи захищати інформацію від несанкціонованого доступу та її відмовостійкість [4].

Для оцінки надійності мереж необхідно виділити приватні аспекти — апаратурну (елементарну) та функціональну (структурну) надійність, відповідні методи їх оцінки та розглянути методичні питання надійності з урахуванням QoS, міжнародних і національних стандартів в телекомунікаціях. Ці стандарти встановлюють рамки для розвитку, імплементації та експлуатації телекомунікаційних систем та технологій. До ключових стандартів та організацій, що регулюють ці аспекти на міжнародному рівні слід віднести:

1. ITU (International Telecommunication Union). ITU-T — відділ, що відповідає за стандартизацію телекомунікаційних технологій. ITU-R регулює радіокомунікації, включаючи асигнацію частотних діапазонів та стандарти супутникового зв'язку. ITU-D сприяє розвитку телекомунікацій, особливо в країнах, що розвиваються [10].

2. IEEE (Institute of Electrical and Electronics Engineers) — розробляє стандарти для широкого спектру електроніки та телекомунікацій, зокрема Wi-Fi (802.11) та Ethernet (802.3) [7].

3. IETF (Internet Engineering Task Force) — відповідає за розробку та схвалення стандартів, які впливають на функціонування Інтернету, включаючи протоколи такі як TCP/IP [8].

4. ISO (International Organization for Standardization) та IEC (International Electrotechnical Commission) — спільно розробляють міжнародні стандарти для інформаційних технологій та телекомунікацій [9].

До національних інституцій слід віднести:

1. Національну комісію, що здійснює державне регулювання у сферах зв'язку та інформатизації (НКРЗІ) — орган, що регулює телекомунікації в Україні, включаючи ліцензування, контроль за частотним спектром і технічні стандарти [2].

2. ДСТУ (Державні стандарти України) — адаптовані та оригінальні українські стандарти, що визначають параметри та характеристики різних телекомунікаційних технологій і послуг [1].

Українські стандарти часто базуються на міжнародних, що сприяє гармонізації технічних вимог і спрощує інтеграцію українських телекомунікаційних систем з глобальними мережами.

Базова надійність є характеристикою, яка дозволяє компоненту зв'язкової мережі зберігати свою функціональність на належному рівні протягом певного періоду часу. З іншого боку, структурна надійність описує здатність мережі загалом підтримувати з'єднання між користу-

Передплатний індекс 21847

вачами на відповідному рівні протягом визначеного часу.

Оцінка надійності включає аналіз таких ключових параметрів, як готовність системи до роботи, її безпека, а також стійкість до збоїв. Надійність телекомунікаційних мереж залежить не тільки від надійності фізичних каналів передачі даних, але й від мережевого обладнання. Адекватне оцінювання такого складного об'єкта, як телекомунікаційні мережі, потребує врахування цілого ряду параметрів надійності, адже одиничні показники часто недостатні для повного характеристики системи. Тому розрізняють окремі та комплексні показники надійності, де останні описують декілька властивостей одночасно.

Теорія надійності пропонує різні інтервальні, інтегральні та точкові показники для вимірювання якості роботи мереж та обладнання. Оцінюючи надійність, кожний об'єкт можна описати через вектор окремих та комплексних показників. У ситуаціях, де порівнюються альтернативні варіанти, важливо вибрати показник, який найкраще відображає необхідну властивість надійності у даному контексті, та використовувати його як основний критерій оцінки. Оцінка надійності також може включати специфічні критерії, такі як ремонтопридатність та термін служби обладнання, що визначаються як галузевими стандартами, так і індивідуальними вимогами споживачів.

У таблиці 1 представлено класифікацію систем за рівнем надійності [5].

Корпоративні телекомунікаційні мережі, особливо ті, що використовуються у сфері електронної комерції, мають унікальні характеристики. Вони структуровані таким чином, що розподіл ролей і відповідальностей між різними підрозділами відбувається горизонтально, зі зменшеним рівнем ієрархічних зв'язків. Ці корпорації часто описуються в сучасній західній літературі як "організації з модульною структурою" (modular organization) або "динамічні мережеві організації" (dynamic network organizations). Координація між відділами зазвичай здійснюється через інтернет з центрального офісу, що включає самоорганізацію та децентралізоване керування, із мінімальною кількістю ієрархічних рівнів.

Створення такої мережі є значно простішим, оскільки не потребує розробки складних інтеграційних проектів. Замість цього, різні підрозділи можуть розробляти власні підсистеми з використанням локальних мереж та серверів, які легко інтегруються з загальною системою корпорації. Це сприяє гнучкості та адаптивності організаційної структури.

Таблиця 1. Класифікація систем за рівнем надійності

Коефіцієнт готовності	Типи систем	
0,99	Звичайна	Conventional
0,999	Висока надійність	Highavailability
0,9999	Відмовостійка	Faultresilient
0,99999	Безвідмовна	Faulttolerant

Особливості цих мереж також включають вдосконалення доступу до інтернету, мобілізацію інтернет-сервісів, впровадження нових стандартів для спрощення доступу, використання швидкісних технологій передачі даних, інтеграцію з іншими телекомунікаційними системами, а також створення резервних каналів і дублювання ключових компонентів для забезпечення високої продуктивності, надійності та здатності до розширення [11].

У контексті ведення комерційних транзакцій важливо дотримуватися таких основних принципів: забезпечення конфіденційності, збереження цілісності даних, надійна автентифікація та авторизація учасників, а також гарантії та збереження комерційної таємниці. Технічні засоби можуть забезпечити перші чотири вимоги, тоді як реалізація останніх двох вимог залежить не тільки від технічних рішень, але й від відповідальності особистостей та організацій, а також від дотримання юридичних норм.

Телекомунікаційні системи та мережі, глобальна мережа Інтернет, комерційні та корпоративні мережі, а також інформаційні та телекомунікаційні технології служать фундаментом для розгортання електронної комерції. Ці технологічні платформи сприяють впровадженню та розвитку електронних торгових систем.

Електронні торгові майданчики (ЕТМ) є ключовим елементом систем електронної торгівлі, призначеними для автоматизації процесів підготовки та проведення електронних аукціонів і конкурентних закупівель. Ці платформи спрощують взаємодію між покупцями та продавцями на всіх етапах угод, що важливо для ефективної реалізації комерційних операцій. Важливу роль в розвитку ЕТМ відіграє становлення законодавчої бази, що регулює державні закупівлі. З часом, ЕТМ можуть еволюціонувати в більш складні системи управління, що використовують телекомунікаційні мережі для забезпечення всіх аспектів торговельно-закупівельної діяльності.

Передплатний індекс 21847

Електронні торгові майданчики виконують низку ключових функцій: забезпечують доступ до даних про компанії, що приймають участь у майданчику, дозволяють отримувати інформацію про конкретні організації, підтримують маркетингові та рекламні ініціативи, фасилітують торгівельні операції, і здійснюють аналіз діяльності різних учасників. Також, ЕТМ забезпечують безпеку інформаційних потоків за допомогою застосування криптографічних методів для захисту документообігу.

Переваги використання ЕТМ для замовників та компаній включають значне скорочення часу, необхідного для робочих процесів, зниження витрат на організацію і проведення закупівель, забезпечення прозорості у закупівельних процедурах, змагальність та чесність торгів. ЕТМ дозволяють брати участь у торгах з будь-якої точки світу, не виходячи з офісу, що робить їх доступними для бізнесу будь-якого розміру, забезпечуючи вільний доступ до торгів без обмежень по ціні чи умовах лотів.

Процедура використання електронних торговельних майданчиків (ЕТМ) для державних та комерційних закупівель регулюється законодавством України і включає кілька ключових кроків:

1. Електронний підпис (ЕП) — організації, що бажають узяти участь у електронних торгах, мають отримати кваліфікований електронний підпис, виданий акредитованим центром сертифікації.

2. Реєстрація на майданчику — організація реєструється на обраному електронному торговому майданчику, укладає угоду з оператором майданчика та проходить авторизацію.

3. Участь у аукціонах — організації можуть подавати свої пропозиції на торги за допомогою цих майданчиків, використовуючи свій електронний підпис для забезпечення легітимності та безпеки процесу.

Українські ЕТМ можна класифікувати на такі категорії:

1. Для розміщення державного замовлення:

— Prozorro — головний державний електронний майданчик в Україні, що використовується для проведення публічних закупівель усіх рівнів.

— SmartTender — ще одна популярна платформа, яка працює в рамках системи Prozorro.

2. Для комерційних замовників:

— Zakupivli Pro — ЕТМ, що надає можливості для комерційних закупівель, дозволяючи приватним компаніям проводити електронні тендери.

— Rialto — платформа, що обслуговує комерційні та корпоративні закупівлі.

Ці майданчики дозволяють замовникам публікувати тендери, а постачальникам — подавати свої пропозиції в електронному форматі, забезпечуючи прозорість і конкуренцію у процесах закупівель.

Для створення ефективних телекомунікаційних мереж і систем можливе використання різноманітних підходів до забезпечення, включаючи економічні, тимчасові, організаційні, структурні, технологічні, експлуатаційні, соціальні та алгоритмічні стратегії.

Забезпечення технічної надійності часто передбачає такі заходи, як резервування (дублювання) технічних засобів, включаючи комп'ютери, їхні компоненти та мережеві сегменти, використання стандартних протоколів для пристроїв телекомунікаційних систем, а також впровадження спеціалізованих засобів технічного захисту. Захист телекомунікаційних систем, в тому числі систем електронних торгів, включає використання технічних, криптографічних, програмних та інших засобів для захисту інформації, а також засобів для контролю ефективності цього захисту. Засоби захисту інформації поділяються на фізичні, апаратні, програмні, криптографічні та комбіновані, деталі яких описані в третьому розділі цієї роботи.

Загалом, підвищення надійності системи полягає у впровадженні заходів, спрямованих на запобігання збоям, несправностям та відмовам. Основний метод досягнення високої готовності — використання надмірності, яка дозволяє реалізувати різні варіанти стійких до відмов архітектур.

Для бізнес-структур важливість безпеки вимірюється економічними показниками. В даний час розробляються інтегровані стратегії забезпечення інформаційної безпеки компаній. Формуються стратегії та політики безпеки організацій. В системах телекомунікацій особливо вразливими є мережеві протоколи, пристрої, які складають мережу, операційні системи, бази даних та програмне забезпечення. Заходи забезпечення надійності та безпеки інформації у телекомунікаційних мережах розділені на організаційні та технічні підходи.

Організаційні методи включають керування персоналом, забезпечення фізичної безпеки, підтримання операційної готовності та планування відновлювальних заходів.

Технічні стратегії охоплюють правильне налаштування мережевих вузлів, застосування методів резервування, використання компо-

Передплатний індекс 21847

нентів, що забезпечують безпеку при проектуванні мереж, використання надійних комп'ютерів із відмовостійкими компонентами, кластеризацію для забезпечення високої доступності, дзеркальне відображення дисків, автоматичне відновлення з'єднань, дублювання файлових систем, моніторинг транзакцій, використання брандмауерів, системи ідентифікації та аутентифікації, управління доступом, аудит, та криптографічне шифрування даних.

Вивчення мережевої надійності ведеться вже багато років. Навіть для малих мереж немає точного рішення для визначення їх надійності, хоча можна оцінити верхні та нижні межі надійності, що потребує складних математичних розрахунків [6]. Через високу складність цих розрахунків, багато дослідників обмежуються лише оцінкою потенційних меж надійності.

Через те, що мережі тісно інтегровані, аналітичний розрахунок їх надійності є складним. Єдиним числовим методом для розрахунку надійності таких мереж є метод повного перебору, але навіть з використанням швидкодіючих комп'ютерів, він не дозволяє аналізувати мережі, які містять понад 50 випадкових елементів, тому часто вдаються до методу часткового перебору.

Іноді надійність та її розподіл визначаються на емпіричній основі. Використовуються також алгоритмічні та логіко-імовірнісні методи аналізу мереж. Через відсутність належної моделі для механізму втрат в мережі та загальної складності розрахунків, застосовуються часозалежні моделі з дискретними ймовірностями. Точні алгоритми обчислення надійності включають алгоритми з експоненційним часом для загальних мереж та поліноміальним часом для обмежених класів мереж.

Методи структурної надійності мереж включають точні методи аналізу, статистичну оцінку, розкладання, двосторонню оцінку, метод перерізів або сукупності шляхів [3]. Моделі безвідмовності включають експонентний розподіл, розподіл Вейбулла та усічений нормальний розподіл.

Простий і ефективний спосіб підвищення апаратурної надійності корпоративних телекомунікаційних мереж полягає в резервуванні, яке забезпечує підвищення надійності системи за рахунок використання додаткових ресурсів. Резервування буває структурним, функціональним, тимчасовим і інформаційним.

Інші підходи та моделі також застосовуються для забезпечення технічної надійності мережевих систем. Кожен з цих методів та моделей має свої сильні та слабкі сторони, що вносить певні обмеження на їх використання під час розробки спеціалізованих корпоративних телекомунікаційних мереж. Тому розробка нових моделей та алгоритмів для розрахунку надійності цих мережевих пристроїв, враховуючи існуючий досвід у цій галузі, залишається актуальною науковою задачею.

Основні вимоги, які ставляться до мережевих моделей, включають універсальність, точність, адекватність та ефективність. Додатково, при оцінці технічної надійності корпоративних телекомунікаційних мереж необхідно враховувати вимоги до економічності, наочності та обчислювальної здатності моделей, а також забезпечувати можливість розробки відповідних алгоритмів та програмного забезпечення для реалізації моделей на електронно-обчислювальних машинах, де алгоритм розв'язання задачі є інтегрованим.

Велика кількість наукових і технологічних інститутів та організацій працювала над вирішенням питання оцінки надійності мереж та обчислювальних систем, що призвело до створення складних програмно-технічних комплексів. Проте багато з цих систем є складними у використанні та коштовними.

Серед різноманітних іноземних програмних продуктів, призначених для оцінювання надійності, доступності та можливості ремонту, варто виокремити такі системи, як AnyGraph, CRISS, AggreGateNetworkManager, BlockSim, ITEMSoftware, ReliabilityWorkbench, і Windchill.

AnyGraph, наприклад, розроблено для полегшення створення системних моделей, які застосовуються для аналізу надійності складних технічних систем. Програма використовує логіко-імовірнісні методи моделювання як теоретичну основу і дозволяє представляти модель як взаємопов'язану мережу технічних елементів з логічними зв'язками, створену за допомогою графічного редактора, що забезпечує високий рівень наочності.

Система AggreGateNetworkManager функціонує для моніторингу компонентів мережі, перевіряючи їх доступність через стандартні процедури, такі як пінгування мережевих пристроїв або перевірка підключення до сервісів через порти. Цей моніторинг дозволяє забезпечити всебічну перевірку стану керованих елементів, підтверджуючи їх належну роботу.

На ринку захисту інформації пропонується багато окремих інженерно-технічних, програмно-апаратних, криптографічних засобів захисту:

Передплатний індекс 21847

1. Symantec Data Loss Prevention (DLP) — комплексне рішення для запобігання витоку даних, яке дозволяє контролювати та захищати конфіденційні дані всередині організації та за її межами.

2. McAfee Total Protection for Data Loss Prevention — забезпечує захист від витоку даних, виявляючи і контролюючи конфіденційну інформацію у файлових системах, базах даних та інших сховищах.

3. Microsoft Azure Information Protection — рішення для класифікації та захисту документів і електронної пошти за допомогою міток та політик, що автоматично застосовують шифрування, доступ до даних, і управління правами на користування даними.

4. Cisco SecureX — інтегрована платформа безпеки, яка об'єднує різноманітні інструменти для забезпечення комплексного захисту корпоративних мереж і ресурсів.

Українськими розробками є:

1. InvisibleCRM — компанія, що розробляє рішення для інтеграції корпоративних систем з персональними продуктивними інструментами, такими як Microsoft Office і Salesforce, з фокусом на захисті даних та ефективності користувача.

2. StarForce Content — рішення для захисту контенту від несанкціонованого доступу і розповсюдження, яке забезпечує ефективне шифрування та управління доступом.

Ці системи охоплюють різні аспекти інформаційної безпеки, включаючи захист від витоку даних (DLP), управління доступом, шифрування даних і віртуалізацію. Вони дають можливість компаніям захищати свої конфіденційні дані від несанкціонованого доступу, використання та витоку, в той час як виртуалізація та криптографічні технології допомагають забезпечити безпеку даних при їх зберіганні та передачі.

На основі аналізу даних, можна запропонувати наступні заходи для підвищення надійності та безпеки інформації:

1. Впровадження багатошарової моделі безпеки (Layered Security Model). Цей підхід передбачає використання декількох рівнів захисту, що ускладнює проникнення зловмисників до системи та дозволяє контролювати безпеку на кожному етапі обробки інформації.

2. Застосування сучасних методів криптографічного захисту. Криптографія є основою захисту даних при передачі через незахищені канали. Використання надійних алгоритмів шифрування і цифрових підписів допомагає захистити дані від несанкціонованого доступу та зміни.

3. Регулярний аудит і моніторинг мережі. Постійний моніторинг мережевого трафіку та аудит систем на предмет вразливостей дозволяє вчасно виявляти та усувати потенційні загрози, а також контролювати ефективність вжитих заходів безпеки.

4. Забезпечення фізичного захисту обладнання. Фізичний захист серверів та іншого критичного обладнання запобігає можливості фізичного втручання та крадіжки даних, що є важливим компонентом загальної стратегії безпеки.

5. Розробка та впровадження політики безпеки на підприємстві. Наявність чіткої політики безпеки, що включає правила поведінки співробітників, процедури обробки даних та відповідальності за порушення, є ключовою для створення безпечного інформаційного середовища.

6. Використання механізмів ідентифікації та аутентифікації. Дієві методи аутентифікації користувачів та пристроїв, такі як багатофакторна аутентифікація, допомагають забезпечити, щоб доступ до ресурсів мали лише уповноважені особи.

7. Резервне копіювання та відновлення даних. Забезпечення належного резервного копіювання та стратегій відновлення допомагає уникнути втрати інформації у випадку фізичних пошкоджень або кібератак, а також сприяє швидкому відновленню нормальної роботи системи.

Ці заходи дозволять не тільки підвищити надійність та безпеку інформації в корпоративних телекомунікаційних системах, а й забезпечити адаптацію до постійно змінюваних умов цифрового середовища і загроз.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

На підставі аналізу сучасних підходів до забезпечення надійності та безпеки інформації в корпоративних телекомунікаційних системах, можна зробити декілька ключових висновків. Перш за все, комплексний підхід до безпеки, який включає застосування багатошарової моделі безпеки, є вирішальним у захисті корпоративних даних. Це означає, що ефективність захисту системи значно зростає, коли використовуються різні рівні захисту, що включають як фізичні, так і програмні заходи безпеки, від моніторингу мережі до криптографічного шифрування.

Друге важливе спостереження стосується необхідності регулярного аудиту та оновлен-

Передплатний індекс 21847

ня політик безпеки для адаптації до змінних умов і загроз. Наукові дослідження та практичний досвід показують, що корпорації, які постійно аналізують та оновлюють свої методи захисту, краще захищені від кібератак і технологічних вразливостей. Особливо це стосується використання новітніх технологій для ідентифікації та реагування на інциденти, які дозволяють оперативно локалізувати та усунути проблеми безпеки.

Підкреслюється роль стратегічного планування та управління в сфері корпоративної інформаційної безпеки. Зокрема, важливість розробки та впровадження комплексних систем оцінки надійності та захисту інформації, що включають як технічні, так і організаційні компоненти. Ефективне управління ризиками та використання передових міжнародних практик та стандартів може значно покращити стан захисту інформаційних ресурсів компанії, сприяючи її стійкості та конкурентоспроможності на ринку.

Література:

1. Державні стандарти України (ДСТУ). URL: https://ukrpatent.org/uk/articles/dstu (Дата звернення 22.02.2024).

2. Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв`язку. URL: https://nkrzi.gov.ua (Дата звернення 26.04.2024).

3. Остапенко В. О. Методи оцінки функціональної безпеки бездротових сенсорних мереж. Наукоємні технології. 2018. № 1. С. 28—36.

4. Цуркан В., Шаповал О. Аналіз методів оцінювання ризику безпеки комп'ютерних мереж. Information Technology and Security. 2022. Vol. 10, Iss. 2. С. 204—215.

5. Черкасов Д. І. Висока доступність мережевих сервісів: визначення та основні фактори впливу. Наукові записки. 2014 Том 163. С. 98—102.

6. Шолом П. С., Міскевич О. І., Мельник К. В. Аналіз загроз та оцінка ризиків безпеки інформації в безпровідних мережах. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2013. № 13. С. 66—70.

7. IEEE Engineering. URL: https://ieeer8.org (Дата звернення 5.03.2024).

8. IETF. Internet Engineering Task Force. URL: https://www.ietf.org (Дата звернення 21.02.2024).

9. ISO — International Organization for Standardization. URL: https://www.iso.org/home.html (Дата звернення 23.04.2024).

10. ITU: Committed to connecting the world. URL: https://www.itu.int (Дата звернення 03.05.2024).

11. What is a Modular Organization? HR Glossary — AIHR. URL: https://www.aihr.com/hr-glossary/modular-organization/#:~:text=-A%20modular%20organization%20is%20a,-are%20required%20within%20the%-20organization (Дата звернення 19.03.2024).

References:

1. State Standards of Ukraine (DSTU) (2024), "The state system of intellectual property legal protection", available at: https://ukrpatent.org/uk/articles/dstu (Accessed 22 Feb 2024).

2. National commission for the state regulation of electronic communications, radio frequency spectrum and the provision of postal services (2024), available at: https://nkrzi.gov.ua (Accessed 26 Apr 2024).

3. Ostapenko, V. O. (2009), "Methods of assessing the functional security of wireless sensor networks", Naukoiemni tekhnolohii. vol. 1. pp. 28—36.

4. Tsurkan, V. and Shapoval, O. (2022), "Analysis of computer network security risk assessment methods", Information Technology and Security, vol.10, no. 2. pp. 204—215.

5. Cherkasov, D. I. (2014), "High availability of network services: definition and main influencing factors", Naukovi zapysky. vol. 163. pp. 98—102.

6. Sholom, P. S., Miskevych, O. I. and Mel'nyk, K. V. (2013), "Threat analysis and risk assessment of information security in wireless networks", Komp'iuterno-intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo, vol. 13. pp. 66—70.

7. IEEE Region 8 (2024), "IEEE Engineering", available at: https://ieeer8.org (Accessed 5 Mar 2024).

8. IETF. Internet Engineering Task Force (2024), available at: https://www.ietf.org (Accessed 21 Feb 2024).

9. ISO (2024), "ISO — International Organization for Standardization", available at: https://www.iso.org/home.html (Accessed 23 Apr 2024).

10. ITUCouncil (2024), available at: https://www.itu.int (Accessed 3 May 2024).

11. AIHR. Academyto innovate HR (2024), "What is a Modular Organization? HR Glossary — AIHR", available at: https://www.aihr.com/hr-glossary/modular-organization/#:~:text=A%-20modular%20organization%20is%20a,are%2-0required%20within%20the%20organization (Accessed 19 Mar 2024).

Стаття надійшла до редакції 24.06.2024 р.

Передплатний індекс 21847