КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (21), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.21.223233
УДК 004.056

Ворохоб Максим Віталійович
викладач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0001-5160-7134
m.vorokhob@kubg.edu.ua

Киричок Роман Васильович
доктор філософії, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID: 0000-0002-9919-9691
r.kyrychok@kubg.edu.ua

Яскевич Владислав Олександрович
Кандидат технічних наук,
доцент кафедри комп'ютерних наук
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID ID:0000-0002-5796-2521
v.yaskevych@kubg.edu.ua

Добришин Юрій Євгенович
кандидат технічних наук, доцент
ORCID ID: 0000-0003-2473-9507
Національна академія Служби безпеки України, м. Київ
ydobryshyn@gmail.com

Сидоренко Сергій Миколайович
старший викладач
ORCID ID: 0009-0003-1185-1505
Національна академія Служби безпеки України, м. Київ
s.s.m.ukr@gmail.com

СУЧАСНІ ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ КОНЦЕПЦІЇ ZERO TRUST ПРИ ПОБУДОВІ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Анотація. Сучасні підприємства зазнали значної трансформації в зв'язку з цифровим прогресом та нещодавньою пандемією COVID-19. Зокрема збільшилася кількість працівників, які працюють віддалено і використовують особисті цифрові пристрої наряду з корпоративними, а сам бізнес, бізнес-процеси переходять до хмарного середовища, або використовують гібридні середовища, які поєднують як хмарні, так локальні служби. В поєднанні, все це призводить до збільшення взаємодії між пристроями та сервісами саме через відкриті мережі, що створює нові ризики кібернетичних атак. Саме така ситуація обумовила актуальність та напрям даного дослідження. В роботі було проведено аналізу поточного стану ефективності застосування політики інформаційної безпеки підприємства, зокрема визначено основні обмеження, які пов'язані з важкістю, а іноді і неможливістю контролювати поведінкові аспекти працівників підприємства щодо дотримання основних положень політики безпеки та загального забезпечення інформаційної безпеки. Проаналізовано основні принципи концептуального підходу Zero Trust та визначено основні перевага його застосування при формуванні політики безпеки, як стратегічного підходу до забезпечення інформаційної безпеки підприємства в умовах динамічного зростання нових загроз та трансформації сучасного бізнесу. Водночас, визначено, що однією з ключових складових архітектури Zero Trust є саме система керування доступом. В наслідок цього, формуючи перспективи застосування концепції Zero Trust при побудові та впровадженні політики інформаційної безпеки, було визначено необхідність у проведенні супутнього

дослідження ефективності сучасних механізмів ідентифікації/автентифікації суб'єктів доступу.

Ключові слова: забезпечення інформаційної безпеки; політика безпеки; концепція zero trust; архітектура zero trust; керування доступом; суб'єкт доступу; ідентифікація; автентифікація; периметр безпеки; хмарне середовище; byod

ВСТУП

Постановка проблеми. Цифровий прогрес та інші фактори, як то нещодавня пандемія COVID-19, докорінно змінили сучасний організаційний ландшафт ведення бізнесу. Дана трансформація призвела до збільшення кількості працівників підприємств, які виконують свої функціональні обов'язки віддалено, поза традиційних умов офісної праці. Крім того, спостерігається зростаюча тенденція до використання працівниками особистих цифрових пристроїв наряду, або в поєднанні з корпоративними, що часто називають Bring Your Own Device (BYOD). В той же час, фіксується сплеск впровадження технологій хмарних обчислень. Велика кількість підприємств або повністю переходять на хмарне середовище, або використовують гібридні середовища, які поєднують як хмарні, так локальні служби [11]. В результаті, збільшується кількість пристроїв працівників і корпоративних сервісів, які взаємодіють між собою через відкриті мережі, що створює нові ризики та можливості для проведення кібернетичних атак.

Так, до прикладу, згідно з доповіддю [8] Агентства Європейського Союзу з кібербезпеки (ENISA), за період 2020-2021 років спостерігалося зростання кількості кібератак на інформаційні системи організації та забезпечення дистанційної роботи. Це призвело до значного збільшення загроз витоку корпоративної інформації, з 8,7% в 2020 році до 81% у другому кварталі 2021 року. Якщо ж брати більш масштабний період активної та стрімкої цифровізації суспільства, розпочинаючи з 2001 року, згідно останнього звіту Surfshark [7], кількість жертв інтернет-злочинів зросла в 16 разів, а фінансові втрати за цей же період (2001-2022 років) зросли у понад 570 разів, що зараз вартують світові приблизно 1 млн. доларів на годину.

В результаті, виникає необхідність у впровадженні скоординованого комплексу заходів із захисту інформаційних активів підприємства, що зазвичай називають діяльністю з управління інформаційною безпекою [10]. Основною складовою цього процесу вважається політика безпеки, яка є фундаментом для ефективного управління інформаційною безпекою та забезпечення безпеки інформаційних активів, а також бізнес-процесів на підприємстві.

Аналіз останніх досліджень і публікацій.

Вважається, що розробка та впровадження універсальної, функціональної та досить простої політики інформаційної безпеки є одним із найбільш ефективних та економічно доцільних рішень щодо захисту конфіденційних даних підприємства. Однак, задля підтвердження цього, відразу ж виникає питання щодо визначення ефективності політики безпеки, оскільки без чіткого слідування викладеним в ній положенням, вона залишається лише на папері та не несе реального впливу на стан забезпечення інформаційної безпеки на підприємстві.

В контексті цього, багато фахівців з інформаційної безпеки вважають, що успіх політики безпеки залежить від розуміння багатогранної природи людини так само, як і від технічних знань [16]. Саме тому, більшість досліджень щодо ефективного

застосування політики інформаційної безпеки зосереджені на визначенні чинників, які впливають на поведінку працівників та їхню мотивацію дотримуватися положень політики ІБ.

Зокрема в дослідженні [1] стверджується, що погляд працівників на інформаційну безпеку формується на основі переплетіння організаційних, технологічних та індивідуальних факторів. Тим часом автори іншого дослідження [9], припускають, що працівники неохоче ставитимуться до політики безпеки, якщо бачитимуть, що дотримання її положень будуть дещо обмежувати звичні для них дії при виконанні робочих обов'язків. Такі працівники можуть сприймати дотримання політики ІБ як обтяжливе, таке, що заважає їх повсякденній роботі, забирає час і зусилля, або навіть перешкоджає їхньому вільному діловому спілкуванню. Тобто, коли співробітники стикаються з суперечливими вимогами щодо ефективності роботи та дотримання процедур інформаційної безпеки, зазвичай бізнес стає в пріоритеті [1, 5, 13]. Крім того, одна з найкритичніших проблем, з якими стикаються підприємства, полягає в тому, що погляди більшості людей на реальність суперечать деяким положенням, визначеним політикою інформаційної безпеки [3]. До прикладу, співробітник може надати доступ до конфіденційних документів колезі, який не має необхідних облікових даних (зокрема прав та повноважень доступу) просто через роботу над спільним проєктом, або може поділитися паролем виключно на основі довіри чи особистої спорідненості з колегою.

Саме тому, більшість авторів стверджує, що побудова політики безпеки має ґрунтуватися на розумінні того, як поведінка людини, яка безпосередньо працює з інформаційними активами підприємства, може впливати на забезпечення дотримання основних її положень, і навпаки. Тобто, переважна більшість досліджень зосереджується на розгляді проблематики формування ефективної політики інформаційної безпеки підприємства в контексті організаційного рівня.

Водночас, сформована та прийнята політика інформаційної безпеки в більшості сучасних підприємствах орієнтована на захист від зовнішніх загроз, оскільки базується на основі припущення, що дії, які відбуваються всередині периметра корпоративної мережі, є безпечними, всі решта – підозрілими. Тобто, така політика втілює підхід до організації інформаційної безпеки на основі периметра (або, його ще називають мережною безпекою) [6], коли мережа умовно поділяється на «внутрішню – довірену» та «зовнішню – недовірену» мережу. В рамках даного підходу передбачається, що ресурси підприємства, сервіси, інформаційні системи, дані тощо знаходяться в межах саме внутрішньої мережі, забезпечення захисту якої (умовно кажучи її ізоляції) здійснюється шляхом розміщення по периметру брандмауерів (в тому числі брандмауерів веб-застосунків (WAF)), засобів контролю доступу до мережі (NAC) та інших систем захисту, які дозволяють виявляти, аналізувати та блокувати несанкціонований доступ ззовні. Таким чином, даний підхід ґрунтується на певній довірі та донедавна був досить ефективним.

Проте в сучасних умовах, поведінкові аспекти працівників щодо забезпечення інформаційної безпеки все ще залишаються важко контрольованими або навіть непередбачуваними, а впевненість в тому, що користувачі інформаційних систем або служби насправді є тими, за кого себе видають, або що їхні наміри доброзичливі, стала вразливою для підприємств, виникає необхідність у застосуванні концепцій, методів, які б нівелювали дані обмеження.

Одним із найперспективніших підходів, який дозволяє вирішувати вищенаведену проблематику є відносно нова концепція «нульової довіри» (в перекладі з англ. Zero Trust). Дана концепція зміщує акцент інформаційної безпеки від захисту

статичних мережевих периметрів до зосередження уваги на користувачах, активах та ресурсах, стверджуючи, що нічого не може бути автоматично довіреним, навіть якщо вони находяться в межах периметру підприємства.

Мета статті. Метою даної статті є визначення основних переваг застосування концепції Zero Trust при формуванні політики безпеки, як стратегічного підходу до забезпечення інформаційної безпеки підприємства в умовах динамічного зростання загроз та трансформації сучасного бізнесу в бік застосування практики віддаленої роботи співробітників та BYOD.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Слід відзначити, що на даний момент відсутнє загальноприйняте визначення для терміну «політика інформаційної безпеки». Так, ґрунтовний огляд літератури щодо політики інформаційної безпеки дозволив виявити три фундаментальні складові даного терміну.

Перша складова підкреслює суто технічний аспект щодо встановлення технічних вимог інформаційної безпеки, яким повинна відповідати система або окремий продукт. Зокрема, в контексті цієї складової, політика безпеки може визначати та регламентувати набір правил, що використовуються системою керування доступом суб'єктів до об'єктів інформаційної системи [2].

Друга складова підкреслює стратегічний аспект інформаційної безпеки всередині підприємства. В даному випадку, політика безпеки інтерпретується як високорівневе декларування організаційних переконань оформлене у вигляді документа, що інкапсулює рішення щодо управління інформаційною безпекою, зокрема щодо цілей та завдань підприємства, а також загальних заходів, пов'язаних із захистом інформаційних активів підприємства [12].

А третя – підкреслює поведінковий аспект, де політика безпеки розглядається як керівний принцип або керівництво для дій організаційних суб'єктів у сфері інформаційної безпеки. Тобто, політика інформаційної безпеки підприємства декларує ролі та обов'язки працівників щодо захисту інформаційних і технологічних ресурсів даного підприємства. По суті, визначає, що дозволено, а що заборонено в інформаційних системах і мережах підприємства [5].

Водночас, основною метою політики безпеки вважається зниження інформаційних ризиків, захист важливих інформаційних активів, а також мінімізація витрат, пов'язаних із управлінням інформаційною безпекою на підприємстві [15]. В результаті, можна сформувати узагальнююче визначення поняття «політики інформаційної безпеки».

Політика інформаційної безпеки (ІБ) – це комплекс заходів, правил та принципів превентивного характеру, спрямованих на захист інформаційних процесів окремого підприємства та циркулюючих там конфіденційних даних.

Відносно нова парадигма кібербезпеки, яка орієнтована на захист ресурсів і виходить із того, що довіра ніколи не надається беззастережно, вона має постійно оцінюватись (перевірятися), називається Zero Trust (ZT) [14].

Архітектура Zero Trust (ZTA) – це комплексний наскрізний підхід до забезпечення безпеки корпоративних ресурсів підприємства (при цьому, до ресурсів відносяться як дані, так і обчислювальні сервіси та їх апаратна складова), який охоплює ідентифікацію суб'єктів (осіб та неособових об'єктів, зокрема процесів, сервісів, служб та ін.), облікові дані, керування доступом (зокрема політики доступу), робочі процеси, операції, кінцеві точки, середовища їх розміщення та з'єднувальну інфраструктуру [14].

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

В порівнянні з традиційними принципами захисту інформації на основі периметру, Zero Trust пропонує ряд рішень, які значно знижують ризик виникнення внутрішніх загроз, а також мінімізують загрозу поширення навіть успішної зовнішньої атаки на всю IT інфраструктуру, коли зловмисник скомпрометувавши обліковий запис користувача та отримавши доступ до системи в межах периметра, намагається розвивати таку атаку [4].

Незважаючи на те, що Zero Trust – це все ще концепція, однак основи її структури вже визначені Національним інститутом стандартів і технологій (NIST) та аналітичними компаніями, такими як Gartner, Forrester, IDC та ESG. Зокрема в SP 800-207: Zero Trust Architecture [14], NIST визначає основні аспекти реалізації принципів ZT та пропонує сценарії розгортання архітектури ZT з відповідними прикладами. Дана спеціальна публікація зосереджена на проблематиці запобігання несанкціонованому доступу до всіх корпоративних ресурсів, включаючи не лише дані (тобто інформаційні ресурси), але й такі елементи, як принтери, обчислювальні ресурси та Інтернет речей (IoT), у поєднанні з максимально деталізованим забезпеченням контролю доступу.

Так, абстрактна модель надання доступу (рис. 1), сформована згідно архітектури ZT демонструє, що доступ до корпоративного ресурсу надається через умовний «контрольно-пропускний пункт», який складається з точки прийняття рішення щодо доступу на основі політики безпеки (Policy Decision Point, PDP) та точки застосування політики (Policy Enforcement Point, PEP), що відповідає за звернення до PDP та правильну обробку відповіді.

Зокрема під PDP мають на увазі точку, яка аналізує та оцінює запити на доступ, враховуючи закладені авторизаційні політики, перед прийняттям рішення щодо надання доступу, а під PEP – точку, яка перехоплюючи запит доступу суб'єкта до корпоративного ресурсу ініціює звернення до PDP з метою отримання рішення (дозволу або відмови) щодо доступу та відповідним чином реагує на нього.

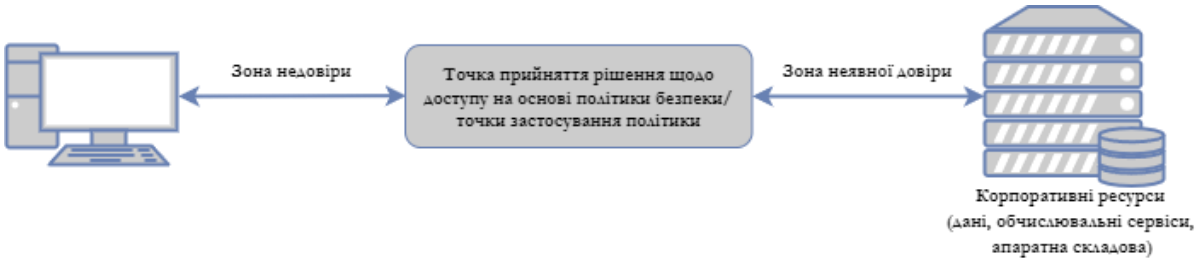

Рис. 1. Модель надання доступу згідно архітектури Zero Trust

Функціональність системи керування доступом повинна охоплювати як перевірку автентичності суб'єкта, так і підтвердження легітимності самого запиту. Тобто, це означає, що концепція ZT застосовується до двох основних областей забезпечення ІБ: автентифікації та авторизації.

В контексті автентифікації, це стосується рівня впевненості в достовірності суб'єкта для конкретного запиту, що передбачає відповідну оцінку достовірності суб'єкта на основі різних факторів, таких як ім'я користувача/пароль, біометричні дані, дані багатофакторної автентифікації або інші автентифікаційні дані неособових об'єктів (до прикладу, електронні криптографічні ключі).

В контексті авторизації, це передбачає визначення того, чи суб'єкту дозволено доступ до запитуваного корпоративного ресурсу з огляду на визначений рівень

впевненості в достовірності суб'єкта. Система оцінює, чи відповідає рівень доступу суб'єкта його «особистості» та вимогам безпеки ресурсу. Крім того, система повинна враховувати стан безпеки самого пристрою, який використовується для запиту, та інші контекстуальні фактори, які можуть змінювати рівень достовірності як-от час, місцезнаходження та загальний рівень безпеки суб'єкта.

Водночас, ключовим моментом нульової довіри є те, що така система повинна забезпечувати послідовне й точне застосування сформованих авторизаційних політик для кожного окремого запиту на доступ до корпоративного ресурсу, а не покладатися на припущення, що попередня автентифікація гарантує постійну надійність. Крім того, «зона неявної довіри», яку NIST визначає як область, де всім об'єктам довіряють, принаймні, до рівня останнього шлюзу PDP/PEP [14], має бути якомога меншою задля того, щоб PDP/PEP був максимально конкретним. Такі зони являють собою так звані мікропериметри безпеки.

Загалом концептуальний підхід Zero Trust ґрунтується на наступних принципах:

- Всі типи джерел даних, безпосередньо самі дані, а також обчислювальні сервіси вважаються корпоративними ресурсами. Тобто, будь-який пристрій або система, яка генерує, обробляє або зберігає дані (це можуть бути сервери, робочі станції, пристрої Інтернету речей, датчики та інших джерел, що генерують дані), сервіси, які забезпечують обчислення, зберігання або інші функції в мережі (зокрема хмарні обчислювальні сервіси, віртуальні машини, контейнери та ін.), вважаються ресурсами. Крім того, підприємства самостійно можуть визначити особисті пристрої (BYOD) як ресурси за умови, що вони мають доступ до корпоративних ресурсів. Це означає, що навіть пристрої, які не належать підприємству, але використовуються в мережі, можуть вважатися ресурсами в контексті концепції нульової довіри.
- Довіра до суб'єкта, в жодному разі, не повинна ґрунтуватися на основі присутності пристрою, через який здійснюється взаємодія, в межах інфраструктури корпоративної мережі. Тобто вся взаємодія суб'єктів має бути захищеною в незалежності від їхнього розташування в мережі. Запити на доступ, що надходять від суб'єктів у межах корпоративної мережевої інфраструктури, навіть у межах застарілого мережевого периметра (який за стандартної моделі безпеки може вважатися цілком безпечним – довіреним), мають відповідати ідентичним стандартам безпеки, що й доступ і зв'язок із будь-якої зовнішньої мережі, що не належить підприємству. Зокрема передбачається обов'язкова автентифікація всіх з'єднань і шифрування всього трафіку.
- Доступ до окремих корпоративних ресурсів надається після оцінки достовірності запитуючої сторони і лише в рамках одного сеансу. Водночас, доступ має бути надано з якомога найменшими привілеями, достатніми для виконання завдання.
- Доступ до корпоративних ресурсів визначається динамічною політикою, яка враховує такі фактори, як спостережуваний стан ідентичності клієнта, програми/сервісу чи будь-якого іншого активу (апаратного забезпечення), що здійснює запит, а також інші поведінкові атрибути або атрибути середовища. Зокрема стан ідентичності клієнта може визначатися обліковими записами користувача (або ідентифікатором служби), будь-якими пов'язаними атрибутами, а також шаблонами поведінки, які дозволяють виявити підозрілу активність. Стан ідентичності активу може

визначатися такими характеристиками пристроїв, як встановлені версії програмного забезпечення, розташування в мережі, час/дата запиту, поведінка, що спостерігалася раніше, і встановлені облікові дані. Водночас, поведінкові атрибути можуть охоплювати ряд автоматизованих аналізів предметів і пристроїв, а також відхилення від спостережуваних шаблонів їх використання. А атрибути середовища можуть враховувати такі елементи, як мережеве розташування запитуючої сторони, час, повідомлення про активні атаки та ін.

- Забезпечення максимально можливого безпечного стану, завжди враховуючи можливість витоку даних. Передбачається постійний аналіз наскрізного трафіку, забезпечуючи максимальну видимість активності суб'єктів, відстежування і визначення (тобто оцінювати) цілісності та стану безпеки всіх корпоративних активів або активів пов'язаних з підприємством, не довіряючи жодному з них.
- Всі ресурси автентифікації та авторизації є динамічними та суворо контрольованими. Дані процеси включають безперервні цикли запитів на доступ, сканування та оцінку потенційних загроз, коригування заходів безпеки та послідовну переоцінку рівня довіри до поточних взаємодій. Зокрема передбачається необхідність впровадження надійної системи керування ідентифікацією, обліковими даними та доступом, включаючи багатофакторну автентифікацію, а також системи управління активами.
- Дослідження поточного стану активів, мережевої інфраструктури та взаємозв'язків задля підвищення загальної безпеки. Зокрема передбачається збір та обробка інформації про стан безпеки активів, мережевий трафік та запити на доступ, а результати повинні використовуються для покращення сформованої політики безпеки та її безпосереднього застосування.

Слід зазначити, що сама архітектура Zero Trust може формуватися з різних програмних та програмно-технічних компонентів, які можуть бути як локальними, так і хмарними сервісами. При цьому більшість експертів наголошують, що універсальної архітектури Zero Trust не існує. Кожне підприємство особливе, а отже і кожна реалізація принципів Zero Trust теж має бути особливою.

Таким чином, виходячи з проведеного аналізу концепції Zero Trust, можна сформувати наступні переваги застосування її принципів та архітектури, як базової основи при формуванні політики інформаційної безпеки підприємства:

- сприяння підвищенню безпеки даних завдяки безперервному контролю та перевірці достовірності суб'єкта доступу, що зокрема дозволяє масштабувати застосування політики безпеки без залежності від місця розташування джерела запиту на доступ;
- покращення можливостей безпечного масштабування самого підприємства за рахунок глобального моніторингу із розширенням «видимості» мережі, що дозволяє вчасно виявляти підозрілу активність на великих відстанях, враховуючи можливості використання бізнес-процесами хмарних середовищ;
- покращення користувацької «дружелюбності» (практичності), що дає змогу забезпечувати безпечний доступ до корпоративних ресурсів, не перешкоджаючи виконанню їх функціональних обов'язків та загальної продуктивності;

– зниження ризиків ІБ зменшуючи площину атак за рахунок мінімізації можливості зловмисником бічного переміщення інформаційно-комунікаційною інфраструктурою підприємства, зокрема в контексті цього, концепція Zero Trust є досить дієвою при боротьбі зі шкідливим програмним забезпеченням, фішинговими атаками і навіть сучасними таргетованими атаками (APT-атаками).

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

З проведеного дослідження слідує, що одним із ключових, навіть критичних компонентів архітектури Zero Trust є система керування доступом, адже при ненадійному механізмі ідентифікації/автентифікації (перевірці ідентичності, справжності суб'єкта доступу), вся модель політики безпеки сформована на концептуальному підході Zero Trust втрачає цінність через подолання його основного принципу.

Водночас, слід також відзначити складність механізмів багатофакторної автентифікації, використання якої рекомендується при реалізації архітектури Zero Trust. Адже, чим більше факторів, тим складніша і сама реалізація такої системи керування доступом, і це може викликати труднощі у рядових працівників при користуванні такою системою, що також може призводити до потенційних порушень безпеки і відповідно знизити ефективність прийнятої політики інформаційної безпеки на підприємстві.

В результаті, подальшим вектором розвитку даного дослідження є глибинний аналіз інформаційних джерел щодо практики побудови та впровадження політики інформаційної безпеки на підприємстві з використанням основних принципів концептуального підходу Zero Trust та інтегруванням його архітектури в загальну модель безпеки. При цьому, слід додатково провести дослідження щодо ефективності використовуваних у визначених практиках механізмів ідентифікації/автентифікації суб'єктів доступу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Albrechtsen, E. (2007). A qualitative study of users' view on information security. Computers & Security, 26(4), 276–289. https://doi.org/10.1016/j.cose.2006.11.004
2 Bosch, C., Eloff, J., & Carroll, J. (1993). International Standards and Organizational Security Needs: Bridging the Gap. Proceedings of the IFIP TC11 Ninth International Conference on Information Security, Amsterdam, 171-183.
3 Bosworth, S., Kabay, M. E., & Whyne, E. (Ред.). (2012). Computer Security Handbook. John Wiley & Sons, Inc. https://doi.org/10.1002/9781118820650
4 Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. Computers & Security, 110, 102436. https://doi.org/10.1016/j.cose.2021.102436
5 Bulgurcu, Cavusoglu & Benbasat. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly, 34(3), 523. https://doi.org/10.2307/25750690
6 Chen, Y., Hu, H.-c., & Cheng, G.-z. (2019). Design and implementation of a novel enterprise network defense system bymaneuveringmulti-dimensional network properties. Frontiers of Information Technology & Electronic Engineering, 20(2), 238–252. https://doi.org/10.1631/fitee.1800516
7 Cybercrime statistics. (2023). Surfshark. https://surfshark.com/research/data-breach-impact/statistics
8 ENISA Threat Landscape 2021. (2021). ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

9 Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106–125. https://doi.org/10.1057/ejis.2009.6

10 Information technology. Security techniques. Information security management systems. Overview and vocabulary (ISO/IEC 27000:2018). (2018). https://www.iso.org/standard/73906.html

11 Mandal, S., Khan, D. A., & Jain, S. (2021). Cloud-Based Zero Trust Access Control Policy: An Approach to Support Work-From-Home Driven by COVID-19 Pandemic. New Generation Computing. https://doi.org/10.1007/s00354-021-00130-6

12 Peltier, T. R. (2002). Information security policies, procedures, and standards: Guidelines for effective information security management. Auerbach.

13 Puhakainen, P. (2006). A design theory for information security awareness [Doctoral thesis, University of Oulu]. http://urn.fi/urn:isbn:9514281144

14 Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-207

15 Shoraka, B. (2011). An Empirical Investigation of the Economic Value of Information Security Management System Standards [NSUWorks]. http://nsuworks.nova.edu/gscis_etd/304

16 Soo Hoo, K. J. (2000). How much is enough? A risk-management approach to computer security. In Proceedings of the Workshop on Economics and Information Security, (pp. 1–99).

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (21), 2023
ISSN 2663 - 4023

Vorokhob Maksym
Lecturer of the Department of Information and Cyber Security
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0001-5160-7134
m.vorokhob@kubg.edu.ua

Roman Kyrychok
PhD, Associate Professor
Associate Professor of the Department of Information and Cyber Security
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0002-9919-9691
r.kyrychok@kubg.edu.ua

Vladyslav Yaskevych
Ph.D,
Associate Professor of the Department of Computer Science
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID:0000-0002-5796-2521
v.yaskevych@kubg.edu.ua

Dobryshyn Yurii
Ph.D., associate professor
ORCID ID: 0000-0003-2473-9507
National Academy of the Security Service of Ukraine, Kyiv
ydobryshyn@gmail.com

Sydorenko Serhii
Senior Lecturer
ORCID ID: 0009-0003-1185-1505
National Academy of the Security Service of Ukraine, Kyiv
s.s.m.ukr@gmail.com

MODERN PERSPECTIVES OF APPLYING THE CONCEPT OF ZERO TRUST IN BUILDING A CORPORATE INFORMATION SECURITY POLICY

Abstract. Modern businesses have undergone significant changes as a result of digital advances and the recent COVID-19 pandemic. In particular, there has been an increase in the number of employees working remotely, using personal digital devices alongside corporate devices, and the enterprise itself moving business processes to the cloud or using hybrid environments that combine both cloud and on-premises services. Taken together, this leads to increased interaction between devices and services over open networks, creating new risks of cyber-attack. It is this situation that has led to the relevance and direction of this research. The paper analyzes the current state of effectiveness of the application of enterprise information security policy, in particular, identifies the main limitations associated with the difficulty, and sometimes impossibility, to control the behavioral aspects of enterprise employees to comply with the basic provisions of security policy and general information security. The basic principles of the Zero Trust conceptual approach are analyzed and the main advantages of its application in the formation of the security policy as a strategic approach to ensuring the information security of the enterprise in the conditions of dynamic growth of new threats and transformation of modern business are determined. At the same time, it is established that one of the key components of the Zero Trust architecture is the access control system. As a result, forming the prospects of applying the concept of Zero Trust in the construction and implementation of the information security policy, the necessity of conducting an accompanying study of the effectiveness of modern mechanisms of identification/authentication of access subjects was determined.

Keywords: information security; security policy; zero trust concept; zero trust architecture; access control; access subject; identification; security perimeter; authentication; cloud environment; byod

REFERENCES

1 Albrechtsen, E. (2007). A qualitative study of users' view on information security. Computers & Security, 26(4), 276–289. https://doi.org/10.1016/j.cose.2006.11.004
2 Bosch, C., Eloff, J., & Carroll, J. (1993). International Standards and Organizational Security Needs: Bridging the Gap. Proceedings of the IFIP TC11 Ninth International Conference on Information Security, Amsterdam, 171-183.
3 Bosworth, S., Kabay, M. E., & Whyne, E. (Ред.). (2012). Computer Security Handbook. John Wiley & Sons, Inc. https://doi.org/10.1002/9781118820650
4 Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. Computers & Security, 110, 102436. https://doi.org/10.1016/j.cose.2021.102436
5 Bulgurcu, Cavusoglu & Benbasat. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly, 34(3), 523. https://doi.org/10.2307/25750690
6 Chen, Y., Hu, H.-c., & Cheng, G.-z. (2019). Design and implementation of a novel enterprise network defense system bymaneuveringmulti-dimensional network properties. Frontiers of Information Technology & Electronic Engineering, 20(2), 238–252. https://doi.org/10.1631/fitee.1800516
7 Cybercrime statistics. (2023). Surfshark. https://surfshark.com/research/data-breach-impact/statistics
8 ENISA Threat Landscape 2021. (2021). ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
9 Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106–125. https://doi.org/10.1057/ejis.2009.6
10 Information technology. Security techniques. Information security management systems. Overview and vocabulary (ISO/IEC 27000:2018). (2018). https://www.iso.org/standard/73906.html
11 Mandal, S., Khan, D. A., & Jain, S. (2021). Cloud-Based Zero Trust Access Control Policy: An Approach to Support Work-From-Home Driven by COVID-19 Pandemic. New Generation Computing. https://doi.org/10.1007/s00354-021-00130-6
12 Peltier, T. R. (2002). Information security policies, procedures, and standards: Guidelines for effective information security management. Auerbach.
13 Puhakainen, P. (2006). A design theory for information security awareness [Doctoral thesis, University of Oulu]. http://urn.fi/urn:isbn:9514281144
14 Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-207
15 Shoraka, B. (2011). An Empirical Investigation of the Economic Value of Information Security Management System Standards [NSUWorks]. http://nsuworks.nova.edu/gscis_etd/304
16 Soo Hoo, K. J. (2000). How much is enough? A risk-management approach to computer security. In Proceedings of the Workshop on Economics and Information Security, (pp. 1–99).