УДК 004.056.5:004.732
DOI: 10.31673/2409-7292.2024.010006

Скибун О. Ж., Гайдур Г. І., Гахов С. О.

АНАЛІЗ ВИКОРИСТАННЯ КОНЦЕПЦІЇ BYOD В КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

У статті розглянуто питання розширення рівня використання приватних кінцевих (термінальних) програмованих пристроїв в корпоративних інформаційних системах та мережах. Відзначено, що основним споживачем концепції «принеси свій пристрій» (концепція BYOD) є освітня сфера, сфера послуг та сфера розваг. Що стосується державної сфери та сфери бізнесу, то питання поширення концепції BYOD визначається інформацією, яка циркулюється в інформаційних корпоративних системах та мережах, де використовується. А це у свою чергу пов'язане із такими питаннями безпеки: витік через власні мобільні пристрої чутливої для компанії інформації або державної інформації з обмеженим доступом; проникнення до корпоративної інформаційної системи та мережі. Також зазначено, що поширення концепції BYOD носить не стільки технічний характер, як суспільно-цивілізаційний, оскільки фронтменами такої концепції виступають міленіали – люди які народилися та виросли в цифрову епоху і які не уявляють свого життя без приватного мобільного пристрою, а також зовсім по іншому ставляться до традиційних підходів щодо навчання та роботи. Забезпечення високого рівня кібербезпеки під час використання концепції BYOD можливо за умови формалізації та інституалізації усіх питань використання приватних мобільних пристроїв у корпоративних інформаційних системах та мережах. Крім того, концепція BYOD визначає необхідність встановлення певних обмежень, спеціального програмного забезпечення, можливості віддаленого доступу та адміністрування приватних мобільних пристроїв, що в свою чергу звужує його можливості та зменшує кордони використання усього існуючого спектру послуг, програм та контенту. Також впровадження концепції BYOD потребує готовності самих працівників до підвищення рівня самоконтролю, самодисципліни та дозволу на віддалений доступ до свого приватного мобільного пристрою, а також обмежень.

Ключові слова: інформаційна система, корпоративна мережа, кінцевий (термінальний) програмований пристрій, концепція BYOD, кібербезпека.

Вступ

На сьогодні завдяки широкому використанню результатів технічного та технологічного прогресу під час проєктування та виробництва кінцевих (термінальних) програмованих пристроїв (далі – приватний мобільний пристрій), вони за своїми технічними та споживацькими характеристиками опинилися поряд із традиційними потужними персональними комп'ютерами, ноутбуками, нетбуками, планшетами тощо. А завдяки їх програмованості на них можна встановлювати програмне забезпечення ідентичне тому, що використовується на комп'ютерах, ноутбуках, нетбуках, що дає можливість використовувати кінцеві (термінальні) програмовані пристрої замість них. Отже, сучасний мобільний телефон, смартфон стає для пересічних громадян не тільки засобом комунікацій через дзвінки та SMS, а і «замінником» великої комп'ютерної техніки, адже не всім користувачам потрібні їх додаткові можливості для повсякденного життя. Наступним важливим фактором поширення використання мобільних телефонів, смартфонів, а також нетбуків та планшетів стало поширення впровадження технологій безпроводового підключення до мережі Інтернет в громадських місцях, установах та організаціях, що дало можливість отримання послуг на базі електронних комунікацій через просте та швидке підключення до інформаційно-комунікаційних мереж приватного та державного секторів. Поштовхом для поширення вказаного став не тільки науково-технічний прогрес разом із інформатизацією та цифровізацією, а і певні обставини, через які виник попит на це. В першу чергу це карантинні заходи, що охопили увесь світ під час пандемії коронавірусу COVID-19, коли в екстреному порядку були введені обмежені заходи для людей і переважна більшість комунікацій приватного, освітнього та виробничого характеру перешли у віртуальний простір у режим онлайн. Таким чином, використання власних мобільних пристроїв (телефонів, смартфонів, планшетів тощо) для навчання, роботи та отримання послуг (адміністративних) створило передумови до впровадження нової концепції «принеси на роботу та/або навчання свій пристрій» (Bring Your Own Device) (далі – концепція BYOD).

Аналіз останніх публікацій показав, що питанням використання концепції BYOD приділяють увагу як зарубіжні, так і вітчизняні науковці та дослідники, як-от: Н. Алімін, В. Андрієвська, Н. Бахаруддін, Л. Білоусова, Т. Бондаренко, Х. Бланко, Е. Вігер, Х. Гевальд, Є. Дроздова, Н. Іззаті, Г. Кожевніков, В. Козел, А. Ляшенко, О. Масальська, О. Приходько, Н. Разлан, М. Росман, А. Сафар, Я. Сікора, Л. Стасівський, Ф. Цивільський тощо.

Не зважаючи на досить широкий спектр проведених досліджень, питання використання концепції BYOD у корпоративних інформаційних системах та мережах, **виступає частиною загальної проблеми,** котрій присвячується означена стаття.

Метою статті є розгляд рівня використання концепції BYOD у корпоративних інформаційних системах та мережах з огляду на сфери, до яких вони відносяться.

Методи дослідження, використані у процесі написання статті, передбачають застосування загальнонаукових та емпіричних прийомів, що ґрунтуються на системному підході. Крім цього, у процесі роботи застосовувались такі загальні методи досліджень, як узагальнення та порівняння. У результаті проведеного аналізу використання концепції BYOD у корпоративних інформаційних системах було сформовано практичні рекомендації щодо збільшення рівня використання приватного мобільного пристрою.

Виклад основного матеріалу

На сьогодні постійно збільшується рівень комбінування/поєднання фізичного та віртуального просторів як у освітній, так і в професійній сферах. Так, для офлайн навчання/роботи необхідна наявність облаштованого стаціонарного фіксованого постійного місця навчання/роботи зі стаціонарним персональним комп'ютером та проводовим підключенням до мережі Інтернет та/або корпоративної мережі. У той же час для онлайн навчання/роботи необхідно ноутбук/нетбук/планшет та точка доступу до Інтернет/корпоративної мережі. При цьому ефективність такого дублювання є сумнівною, зважаючи на те, що в самого користувача також є власне обладнання, яке за своїми технічними, органомічними та естетичними показниками досить часто переважає корпоративний. Тобто, виникає дилема щодо потреби дублювання місця навчання/роботи в режимі офлайн та онлайн. В першу чергу це стосується закладів освіти, невеликих організацій, установ та підприємств. Таким чином, тенденція «принеси свій пристрій на навчання та/або роботу» стає досить привабливою та цікавою як для адміністрації закладів освіти, так і для керівництва компаній, установ та організацій, а це є причиною того, що концепція BYOD стає все більш популярною та постійно оновлюється та поширюється, а тому «загальний термін «візьміть свій власний пристрій» (BYOD) також став позначати кілька інших ініціатив, таких як «візьміть із собою власну технологію» (BYOT), «візьміть із собою власний телефон» (BYOP) і «візьміть із собою власний ПК» (BYOPC)», адже «ці ініціативи з'явилися, щоб розширити можливості робочої сили та узгодити їх з концепцією «користування IT» [7].

Треба також зважати на те, що концепція BYOD має не стільки технічне коріння як соціальне, суспільне та тісно залежить від нового етапу цивілізаційного розвитку суспільства, де «основний клас працівників, який винен у феномені BYOD, – це міленіали робочої сили», адже «саме вони тиснуть на керівництво, щоб воно дозволило їм використовувати власні мобільні пристрої на роботі», оскільки «вони працюють у непарні години та у вихідні» і «хочуть, щоб їхнє особисте та ділове життя поєднувалося» [7]. Так, як показує аналіз досліджень та публікацій, широкого розповсюдження BYOD набуває якраз у сфері освіти.

Що стосується сфери бізнесу та сферу послуг, то тут все не так однозначно. Як відзначає К. Обжелян, «Вимоги до комп'ютерів часто різні навіть усередині одного відділу, що вже говорити про різницю між дизайнерами та менеджерами з продажу. Менеджер з дешевим та важким ноутбуком, що регулярно виїжджає на різні зустрічі та презентації, програє у презентабельності своєму конкуренту зі стильним Sony VAIO або Apple MacBook Air. Та й ті, кому доводиться часто носити із собою ноутбук, готові доплатити за меншу вагу, привабливий дизайн та інші важливі деталі свого девайсу. Висока зарплата багатьох менеджерів дозволяє

© Скибун, О. Ж., Гайдур, Г. І., & Гахов С. О. (2024). Аналіз використання концепції BYOD в корпоративних інформаційних системах. Сучасний захист інформації, 1(57), 50–56. https://doi.org/10.31673/2409-7292.2024.010006.

це зробити, однак це не означає, що стандартизовані робочі місця відійшли в минуле», наприклад, фінансова служба та бухгалтерія [1]. Також треба зважати на певні національні особливості, менталітет та підходи, адже, як показують дані, рівень лояльності до концепції різний, підтвердженням цьому є інформація, представлена на рис. 1. [2].

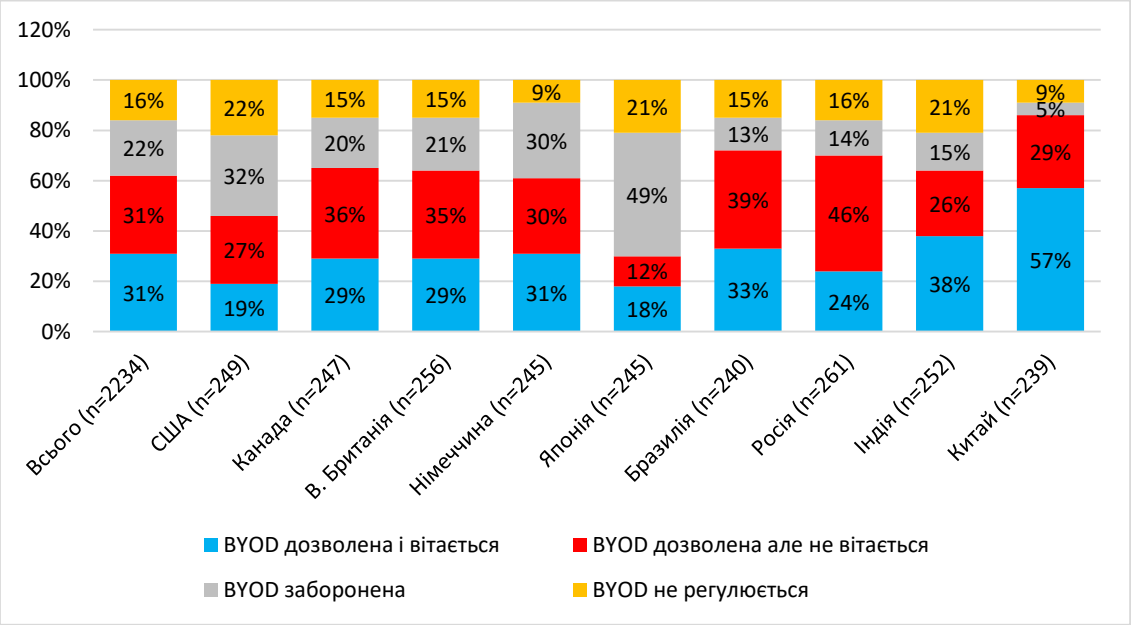

Рис. 1. Розподіл рівня лояльності компаній до концепції BYOD в різних країнах [2]

Ось чому дуже важливо «при прийнятті рішення про перехід компанії на використанні концепції BYOD необхідно проаналізувати наслідки впровадження даної технології», оцінюючи при цьому «забезпечення заходів безпеки, оцінити вплив BYOD на всю систему мережевої безпеки компанії, мати уявлення про проблеми які можуть виникнути» [2].

Перш за все це питання сталості та стійкості функціонування самих інформаційних корпоративних мереж, а також циркуляції інформації, яка в них циркулює, адже в багатьох компаніях є досить чутлива інформація, витік якої є небажаним. Нижче наведено варіант класифікації інформації, яка поділяється на відкриту, закриту та яка належить особі чи державі (рисуноку 2). На наш погляд вказану класифікацію необхідно розширити за рахунок відкритої інформації та чутливої інформації, яка належить компанії/корпорації/підприємству.

Рис. 2. Класифікація інформації [3]

Таким чином, необхідно дуже уважно ставитися до інформації, яка циркулює в інформаційній корпоративній мережі, де використовується концепція BYOD. Так, доречним було б дозволити користуватися відкритою інформацію на усіх пристроях (власних,

© Скибун, О. Ж., Гайдур, Г. І., & Гахов С. О. (2024). Аналіз використання концепції BYOD в корпоративних інформаційних системах. Сучасний захист інформації, 1(57), 50–56. https://doi.org/10.31673/2409-7292.2024.010006.

корпоративних), а що стосується інформації з обмеженим доступом, то для її циркуляції необхідно створювати окрему мережу, залучати відповідне спеціальне обладнання та програмне забезпечення. З огляду на це доречною є побудова двох незалежних інформаційних мереж, в яких буде циркулювати інформація відповідно до визначеної класифікації з урахуванням поділу на приватну, корпоративну, державну та відкриту і закриту. Як відзначає А. Моннаппа, «BYOD може бути катастрофічним, якщо потрапить у чужі руки. Майже в кожній компанії є незадоволені співробітники, які готові піти і забрати з собою конфіденційні дані» [7]. Вказане вище більшою мірою стосується інформаційних мереж та інформації, яка стосується сфери бізнесу, сфери безпеки і оборони. Більш відкритими будуються освітні інформаційні системи та мережі, де концепція BYOD досить стрімко розвивається та застосовується.

Так, група дослідників (М. Росман, С. Бахаруддін, Н. Алімін, Н. Рослі, А. Шукрі) відзначають, що «більшість дискусій зосереджено на безпеці корпоративних даних, які зберігаються на приватних пристроях», адже «надання приватним пристроям доступу до корпоративної інформації може призвести до кількох проблем», а саме: «приватні пристрої можуть бути чутливими до атак кібербезпеки через механізми низького рівня безпеки на персональному обладнанні; нестерті корпоративні дані, що зберігаються на приватних пристроях, можуть бути передані стороннім особам, коли співробітники викидають або продають свої пристрої» [8]. Також важливими є відповіді на такі питання: «що станеться, коли працівник покине організацію з пристроєм, дозволеним згідно з політикою BYOD. Як керівництво примусово видалить усі маркери доступу, дані, доступ до електронної пошти та іншу конфіденційну інформацію та програми?» та «чи зможуть користувачі завантажувати, встановлювати та використовувати програми, які можуть спричинити проблеми з безпекою або юридичні ризики на пристрої, який має доступ до конфіденційних корпоративних ресурсів» [7]. Адже «підхід організації до безпеки BYOD залежить від захищених пристроїв», коли «компанія може мати можливість керувати деякими пристроями, як-от тими, що належать працівникам організації, за контрактами», а «інші пристрої, як-от ті, що належать стороннім користувачам, здебільшого некеровані, і до них потрібно підходити інакше» [6].

У свою чергу Л. Стасівський відзначає, що одним із рішенням «проблеми інформаційної безпеки є використання спеціального інструментарію для управління мобільними пристроями (MDM)», яка «за рахунок розмежування доступу» повинна допомогти «знайти баланс між перевагами працівників і потребою компаній захистити корпоративні дані організації», але разом з цим вказане «ПЗ негативно позначається на» певній свободі користувача щодо власного мобільного пристрою оскільки «установка на особистий апарат деякий фрагмент коду, за допомогою якого можливо відправляти будь-які команди і налаштування, викликає неприйняття персоналу», адже «смартфони та планшети спочатку розроблялися під споживчий сегмент, тобто з урахуванням максимальної зручності використання, і їх власники просто не готові миритися з появою» певних елементів управління ззовні, встановлення спеціалізованого ПЗ, а також введення певних обмежень [2]. Наприклад «Zero Trust: «перевіряє, чи лише авторизовані пристрої, люди та процеси мають доступ до корпоративних ресурсів»; «перевіряє безпеку кінцевих точок пристрою та програм (локальних або хмарних)»; «працює для контролю програмного забезпечення, яке отримує доступ до корпоративної інформації»; «захищає структуровані та неструктуровані корпоративні дані» [5].

Крім того, треба враховувати, що «сторонні користувачі - підрядники, фрілансери, аутсорсингові R&D тощо» разом із своїми некерованими пристроями «створюють більші проблеми для безпеки BYOD», але при цьому «установа агента на пристроях користувача для організації може бути неможливою або недоцільною», а тому «організація може запровадити безпеку BYOD, обмеживши доступ цих користувачів до корпоративних ресурсів», коли «рішення безагентного доступу до мережі з нульовою довірою (ZTNA) може суворо обмежувати та контролювати доступ цих пристроїв до корпоративних ресурсів, зменшуючи

© Скибун, О. Ж., Гайдур, Г. І., & Гахов С. О. (2024). Аналіз використання концепції BYOD в корпоративних інформаційних системах. Сучасний захист інформації, 1(57), 50–56. https://doi.org/10.31673/2409-7292.2024.010006.

потенційний ризик, який ці пристрої становлять для організації та її систем» [6]. Наприклад, «любителям соціальних мереж подобається ініціатива BYOD», але при цьому «спілкуватися в соціальних мережах стає легше під час роботи, і це викликає занепокоєння щодо продуктивності співробітників», а тому є компанії, які заборонять «Facebook та інші мережеві сайт» [7]. Так, співробітники повинні мати високий рівень самоконтролю та самодисципліни для уникнення ситуації, коли приватне переважає робоче.

З огляду на вказане вище, можна виділити такі ризики безпеки BYOD: «слабка безпека: у системах BYOD може бути відсутній цей захист, що підвищує їх уразливість до фішингу та подібних атак»; «зараження зловмисним програмним забезпеченням: пристрої BYOD можуть бути заражені шкідливим програмним забезпеченням, яке може отримати доступ до корпоративних даних, мереж або ресурсів»; «зламані дані: пристрої BYOD можуть використовуватися для доступу або зберігання конфіденційних і цінних корпоративних даних»; «незахищений Wi-Fi: працівники з пристроями BYOD, ймовірно, підключають їх до публічної Wi-Fi та інших незахищених мереж під час роботи поза офісом»; «застарілі пристрої: на пристроях BYOD можуть працювати застарілі версії програмного забезпечення, які містять невиправлені вразливості, які можна використовувати» [6]. Вказані ризики потребують врахування з боку фахівців з IT та кібербезпеки компанії під час упровадження концепції BYOD [9].

Таблиця 1

Узагальнені дані щодо ризиків концепції BYOD [9]

PRIMARY RISK CATEGORY	BYOD RISKS FROM THE LITERATURE REVIEW	BYOD RISKS IDENTIFIED DURING INTERVIEWS	PERCIEVED CRITICALITY OF IDENTIFIED RISKS
Implementational	Protecting data, ensuring security, providing support	YES	LOW (5)
Technological	Malware	YES	HIGH (13)
	Risks and vulnerabilities due to installation of malicious software	YES	HIGH (13)
	Cross-over threats	YES	HIGH (13)
	Contamination of data kept in cloud storage	NO	N/A
	Jailbreaking	NO	N/A
	Compromised user accounts	YES	HIGH (13)
	Phishing and social engineering	YES	HIGH (13)
	Compromised network	YES	HIGH (13)
Human aspects	Lack of control over data and devices	YES	MEDIUM (8)
	Stolen or lost devices	YES	MEDIUM (8)
	Identity theft	YES	MEDIUM (8)
Organisational	Inadequate user education / Organisational security culture	YES	LOW (5)
	Lack of organisational polices (e.g. security, governance, etc.)	YES	LOW (5)
Legislation, regulation and privacy	POPI, ethical issues, tracking of data, breach of normal working hours, liability due to loss of organisational data, etc.	YES	MEDIUM (7)

Усунення ризиків BYOD

Усунення виявлених ризиків BYOD є обов'язковим, тому що якщо не врахувати належним чином, усі потенційні переваги, пов'язані з BYOD, зменшаться. У зв'язку з цим було проведено огляд літератури, щоб визначити можливі корисні теорії та моделі, здатні впоратися з виявленими ризиками.

Такі стандарти, як COBIT 5, ISO 27001, NIST1 або ENISA2, які вважаються загальними стандартами кібербезпеки, популярні серед багатьох організацій у всьому світі. Однак не всі

© Скибун, О. Ж., Гайдур, Г. І., & Гахов С. О. (2024). Аналіз використання концепції BYOD в корпоративних інформаційних системах. Сучасний захист інформації, 1(57), 50–56. https://doi.org/10.31673/2409-7292.2024.010006.

ці структури безпосередньо вирішують питання безпеки BYOD. У той час як COBIT 5 або ISO27001 лише неявно вирішують проблеми BYOD через розділ безпеки мобільних пристроїв, дві інші структури явно декларують безпеку BYOD.

ENISA опублікувала цінний набір засобів контролю та найкращих практик для управління ризиками в програмі BYOD, класифікувавши їх на три групи [9]:

• управління;

• правові, нормативні та кадрові рішення;

• технологічні рішення (пристрій, програма, користувач і дані).

Національний інститут стандартів і технологій США (NIST) у 2016 році опублікував «Посібник користувача з дистанційної роботи та захисту власного пристрою», у якому представлені конкретні вказівки щодо вирішення проблем безпеки BYOD. Відповідно, захист пристрою, який використовується для BYOD, включає такі дії:

• використання комбінації програмного забезпечення безпеки, наприклад антивірусного програмного забезпечення, особистих брандмауерів, фільтрації спаму та веб-вмісту, а також блокування спливаючих вікон, щоб зупинити більшість атак, зокрема зловмисне програмне забезпечення;

• обмеження, хто може використовувати ПК, шляхом створення окремого стандартного облікового запису користувача для кожної особи, призначення пароля кожному обліковому запису користувача, використання стандартних облікових записів користувачів для щоденного використання та захисту сеансів користувачів від неавторизованого фізичного доступу;

• забезпечення регулярного оновлення операційної системи та основних програм, таких як веб-браузери, клієнти електронної пошти, клієнти обміну миттєвими повідомленнями та програмне забезпечення безпеки;

• вимкнення непотрібних мережевих функцій на ПК та безпечне налаштування бездротової мережі;

• налаштування основних програм для фільтрації вмісту та припинення інших дій, які можуть бути шкідливими;

• встановлення та використання лише відомого та надійного програмного забезпечення;

• налаштування програмного забезпечення віддаленого доступу відповідно до вимог і рекомендацій організації;

• постійне забезпечення безпеки ПК, наприклад, регулярна зміна паролів і періодична перевірка стану програмного забезпечення безпеки.

Наявність належної організаційної політики кібербезпеки, яка включає політику, пов’язану з BYOD, і відповідність вимогам безпеки є обов’язковою для усунення ризиків, виявлених у цьому дослідженні. Крім того, багато досліджень вказують на те, що співробітники часто є найслабшою ланкою кібербезпеки, отже, освіта та навчання співробітників повинні бути основною частиною успішного усунення ризиків BYOD.

Нарешті, організації, які прагнуть досягти задовільного рівня безпеки BYOD, повинні уважно стежити за розвитком і підтримкою організаційної культури безпеки. Це варіюється від видимої підтримки вищого керівництва до формування у співробітників звички, наприклад, використовувати шифрування, не активувати невідомі посилання або повідомляти про будь-які підозрілі дії через співпрацю з іншими співробітниками (колективна соціалізація).

Висновки

У цілому можна відзначити, що концепція BYOD у контексті «візьміть із собою власну технологію» (BYOT), «візьміть із собою власний телефон» (BYOP) і «візьміть із собою власний ПК» (BYOPC)» має свою цільову аудиторію та географію поширення. Так, на сьогодні широко використовується концепція BYOD в освітніх процесах, де немає чутливої

© Скибун, О. Ж., Гайдур, Г. І., & Гахов С. О. (2024). Аналіз використання концепції BYOD в корпоративних інформаційних системах. Сучасний захист інформації, 1(57), 50–56. https://doi.org/10.31673/2409-7292.2024.010006.

інформації, яка циркулює в освітніх інформаційних системах та мережах, а тому питання безпеки є більш лояльними до користувачів. Що стосується державного та бізнес секторів, то тут вимоги до безпеки потребують ретельної підготовки та врегулювання усіх питань, що стосується дозволу на широке використання концепції BYOD. Разом з тим, як і всі нові технології, інструменти, та методи удосконалення функціонування корпоративних інформаційних систем та мереж потребує відповідної інституалізації, стандартизації та врегулювання на корпоративному рівні із формуванням нових підходів до питань безпеки в цілому та кібербезпеки як основи сталого та стійкого функціонування компаній, установ, закладів та підприємств. Також необхідно враховувати готовність самих співробітників до широкого використання концепції BYOD, адже, окрім позитиву, це накладає певні зобов'язання, межі, заборони і навіть віддалений доступ до приватного мобільного пристрою.

У цілому необхідно зважати, що «BYOD – це лише концепція, перехідна форма між класичним нерухомим комп'ютером на робочому столі і новим підходом до організації роботи з метою забезпечити максимальний комфорт і продуктивність працівника, давши йому можливість працювати там, тоді й таким чином, як йому буде зручно» [2]. А отже, подальший вплив техніко-технологічного розвитку, формації нового типу суспільства, нових підходів до роботи впливатимуть на концепцію BYOD, що в кінцевому результаті потребуватиме нових розвідок.

Перелік посилань

1. Обжелян, К. BYOD – чотири літери здатні налякати навіть велику компанію. Google Plus. 2012. URL: http://vido.com.ua/article/3112/byod-chietyrie-bukvy-sposobnyie-napughat-dazhie-krupnuiu-kompaniiu/

2. Стасівський, Л. С., Масальська, О. О. Дослідження можливості використання концепції BYOD в захищених інформаційних системах. URL: https://ir.nmu.org.ua/bitstream/handle/123456789/148755/masalska_stasiv.pdf?sequence=1/

3. Тертичний, В. О. Дослідження і обґрунтування вибору методів інформаційної безпеки ІТ компанії. Харківський національний університет радіоелектроніки, Харків, 2020, 81 с.

4. Цивільський, Ф. М., Козел, В. М., Дроздова, Є. А., Приходько, О. О. Практична реалізація концепції BYOD у закладах вищої освіти. Інформаційні технології та засоби навчання, 2021, том 81, № 1. URL: https://www.researchgate.net/publication/349652905_practical_implementation_of_the_byod_concept_in_higher_educational_institutions.

5. Blanco, J. M. XOCE What is BYOD? The Benefits of Bringing Your Own Device to Work. (2023). Режим доступу: https://www.plainconcepts.com/byod/.

6. BYOD Security. (2023) URL: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-byod-bring-your-own-device/byod-security/

7. Monnappa, A. What is BYOD (Bring Your Own Device) and Why Is It Important? (2022). URL: Режим доступу: https://www.simplilearn.com/what-is-byod-and-why-it-is-important-article.

8. Rosman, M. R. M., Baharuddin, N. S., Alimin, N. A., Rosli, N. N. I. N., Shukry, A. I. M., Razlan, N. M. Bring-Your-Own-Device (BYOD) and Productivity: A Conceptual Framework. Proceedings. 2022; 82(1):10. URL: https://doi.org/10.3390/proceedings2022082010.

9. Veljkovic, I. & Budree, A. (2019). Development of Bring-Your-Own-Device Risk Management Model: Case Study From a South African Organisation. 22. 1–14.

Надійшла 19.01.2024