DOI: 10.18372/2225-5036.30.18574

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ ПРИ ВПРОВАДЖЕННІ НЕЮ КОНЦЕПЦІЇ BYOD

Наталія Кухарська, Андрій Лагун

Національний університет "Львівська політехніка", Україна

КУХАРСЬКА Наталія Павлівна, кандидат фізико-математичних наук, доцент
Рік та місце народження: 1971 рік, Тернопільська область, Теребовлянський район, с. Жовтневе, Україна.
Освіта: Львівський державний університет імені Івана Франка (з 1999 року – Львівський національний університет імені Івана Франка), 1993 рік.
Посада: доцент кафедри безпеки інформаційних технологій.
Наукові інтереси: управління інформаційною безпекою, криптографія, стеганографія.
Публікації: більше 130 наукових публікацій, серед яких навчальні посібники, наукові статті, матеріали та тези доповідей на конференціях.
E-mail: nataliia.p.kukharska@lpnu.ua.
Orcid ID: 0000-0002-0896-8361.

ЛАГУН Андрій Едуардович, кандидат технічних наук, доцент
Рік та місце народження: 1969 рік, м. Львів, Україна.
Освіта: Львівський політехнічний інститут (з 2000 року - Національний університет "Львівська політехніка"), 1993 рік.
Посада: завідуючий кафедрою інформаційних систем і технологій.
Наукові інтереси: управління інформаційною безпекою, криптографія, стеганографія, теорія інформації.
Публікації: більше 100 наукових публікацій, серед яких навчальні посібники, наукові статті, матеріали та тези доповідей на конференціях.
E-mail: andrii.e.lahun@lpnu.ua.
Orcid ID: 0000-0001-7856-9174.

Анотація. *Концепція BYOD передбачає використання працівниками організації особистих електронних пристроїв (ноутбуків, планшетів, смартфонів) для службових потреб. Ідея такої концепції з'явилася в середині 2000-х років, проте лише останнім часом вона набула популярності. Це пов'язано з зростанням залежності бізнес-процесів від сервісів, розташованих у мережі Інтернет, досягненнями у сфері виробництва мобільних пристроїв, розширенням їх можливостей та збільшенням продуктивності, а також з розвитком мережевих технологій та хмарних сховищ. Як і будь-яка концепція BYOD має свої плюси та мінуси. До позитивних сторін такого підходу до організації робочого процесу можна, зокрема, віднести зручність для користувача та можливість віддаленої роботи, що дозволяє організаціям ефективніше використовувати робочий час працівників, збільшувати оперативність розв'язання різних завдань і таким чином добиватися підвищення продуктивності праці. Основною проблемою, пов'язаною із впровадженням концепції BYOD, є забезпечення безпеки інформаційної системи організації. Чим більше свободи отримують працівники, що використовують особисті пристрої для взаємодії з мережею організації, тим більших потенційних збитків вони можуть їй завдати. У статті розглянуто загрози інформаційної безпеки, пов'язані з використанням BYOD. А також сформульовано рекомендації, метою застосування яких є зниження їх негативного впливу на організацію. Зокрема, пропонується використовувати NAC для управління мережевим доступом; встановити MDM для керування безпекою мобільних пристроїв; впровадити DLP для захисту від інформаційних витоків; використовувати надійні паролі з регулярним їх оновленням для запобігання несанкціонованому доступу; встановити на пристроях, що належать працівникам, схвалене організацією антивірусне програмне забезпечення; здійснювати шифрування даних; встановити обмеження на скачування та інсталяцію програм; впровадити комплексну IT-політику.*

Ключові слова*: інформаційна безпека, концепція Bring Your Own Device (BYOD), захист інформації, контроль доступу до мережі, захист мобільних пристроїв, запобігання витокам.*

Постановка проблеми

З кожним роком щораз більше організацій впроваджують концепцію BYOD (Bring Your Own Device – принеси свій власний пристрій), і це є цілком логічно. Особливо враховуючи поширену практику роботи з дому під час пандемії COVID-19, а згодом, що стосується України, дистанційну роботу через повномасштабне вторгнення Російської Федерації. Якщо говорити більш конкретно, то таких організацій, які дозволяють працівникам використовувати свої власні пристрої для робочих цілей, включаючи доступ до корпоративних сервісів та застосунків, а саме: електронної пошти, месенджерів та CRM, за даними Cybersecurity Insider є 82 % [1]. BYOD-підхід дає можливість організаціям заощаджувати щорічно 341 долар з розрахунку на одного працівника [2]. Нещодавнє дослідження Research and Markets показало: глобальний ринок BYOD та корпоративної мобільності станом на 2022 рік оцінюється у 84,4 мільярда доларів. Очікується, що цей показник зростатиме і у 2030 році досягне позначки – 296,4 мільярдів доларів [3].

Можливість виконувати робочі завдання за допомогою власних ґаджетів (смартфонів, планшетів чи ноутбуків) багато хто сприймає як елемент свободи, виявом прогресивного підходу до побудови взаємовідносин компанія-працівник, типовим прикладом стратегії win-win. Працівники із задоволенням використовують для вирішення робочих завдань обладнання, яке обрали самі, а організація, у свою чергу, отримує працівників, які завжди на зв'язку та за потреби можуть виконати завдання у позаурочний час. Користувач, який використовує для роботи власний пристрій, опиняється у звичному та комфортному для нього робочому середовищі, налаштованому та персоналізованому відповідно до його уподобань. Використання BYOD-технологій дає можливість виконати більше завдань за менший проміжок часу – так вважають 61 % представників покоління Y та 50 % працівників віком від 30 років [4]. Як свідчать результати досліджень Frost & Sullivan, BYOD додає в середньому 58 хвилин щодня до робочого часу працівника та збільшує продуктивність праці на 34 % [5].

Аналіз останніх досліджень та публікацій

Аналіз існуючих досліджень як у сфері інформаційної безпеки, так і у суміжних з нею областях (комп'ютерні мережі, інформаційні технології, соціальна інженерія) дає розуміння того, що питання забезпечення конфіденційності, цілісності і доступності інформації в організаціях з урахуванням сучасних реалій та використання більшістю з них концепції Bring Your Own Device потребують додаткового опрацювання.

Мета та постановка завдання

Неформальна тенденція, якою ще донедавна була модель BYOD, стала свого роду феноменом. Дехто її сприймає як майбутнє IT. Прихильники цієї моделі організації праці вважають її природним етапом розвитку сучасних організацій. Для працівників, що використовують свої особисті мобільні пристрої для службових цілей, вираз "бути на роботі" отримав новий сенс. Для роботодавців використання BYOD означає повну зміну підходів до управління мережею, портативними пристроями, а також самими працівниками. Бо хоча концепція BYOD забезпечує переваги для працівників та бізнесу, вона також створює низку проблем, які обов'язково повинні бути вирішені. Основна проблема – забезпечення безпеки інформаційної системи організації. Майже всі працівники, які приносять на роботу власні пристрої, мають вихід в Інтернет, що робить організацію вразливою для потенційних атак, які проникають через пристрої. І навіть, якщо BYOD-пристрій не підключений до мережі, він все одно створює ризик для безпеки. Завдання захисту корпоративних інформаційних активів та конфіденційних даних від злому, втрати чи неправомірного використання, яке стоїть перед IT-відділом організації, є непростим, оскільки пристрої знаходяться у приватній власності. Також не менш важливим завданням IT-відділу є технічна підтримка працівників. У випадку стандартної моделі організації праці IT-відділ має вирішальний вплив на рішення щодо придбаного обладнання, операційних систем та встановлених на ньому застосунків. У випадку моделі BYOD IT-відділ стає перед новим викликом, яким є забезпечення інформаційної безпеки (ІБ) багатьох операційних систем, застосунків, а також різноманітних моделей та типів пристроїв, що належать працівникам.

Метою статті є розглянути загрози ІБ організації, пов'язані із впровадженням концепції BYOD, та сформулювати рекомендації для мінімізації ризиків.

Виклад основного матеріалу дослідження

Аналіз загроз ІБ, пов'язаних із впровадженням BYOD

Ризики, пов'язані з BYOD, закономірний наслідок переваг концепції. Чим більше свободи отримують працівники, що використовують власні пристрої для взаємодії з мережею організації, тим більших потенційних збитків вони можуть завдати.

Загроза 1. Втрата або крадіжка пристрою.

Якщо працівник втратить, наприклад, ноутбук, на якому виконував роботу для організації, це створить багато проблем. З часом на пристрої неодмінно накопичяться корпоративні документи, у тому числі такі, що містять конфіденційну інформацію. Якщо такого роду інформація потрапить до сторонніх осіб, це може призвести до значних небажаних наслідків для організації – штрафів через порушення нормативних вимог GDPR та CCPA, розголошення комерційної таємниці, втрати даних клієнтів та репутаційних збитків. Цією інформацією можуть скористатися конкуренти чи зловмисники з метою шантажу, її можуть продати на чорному ринку кіберзлочинцям, що займаються організацією цільових чи фішингових атак.

На пристроях, крім файлів, що містять інформацію з обмеженим доступом, зберігаються також облікові дані для доступу до корпоративної мережі та/або ключі шифрування, записані в реєстр. Використовуючи ці відомості, зловмисник може проникнути в мережу, викрасти все, до чого зможе дотягнутися, встановити шкідливе програмне забезпечення. Як показують результати досліджень Kingston Technology: 40 % усіх витоків даних стаються саме через втрату або крадіжку пристроїв [6].

Другий рік поспіль спостерігається тенденція до зростання кількості електронних пристроїв, втрачених у громадському транспорті. Так, у Лондоні за період 2022-2023 рр. цей показник, про що свідчать дані Управління громадського транспорту міста, зріс більше ніж на 25% [7].

Загроза 2. Несанкціонований доступ.

Згідно з опитуванням, проведеним Bitdefender, 30 % користувачів BYOD діляться своїми особистими пристроями з родичами та друзями, 40 % не застосовують механізму безпечного екрану і лише 9 % використовують біометричний механізм аутентифікації для доступу до пристрою [8]. Ці дослідження показують, що користувачі BYOD не розуміють ризиків безпеки, які можуть виникнути внаслідок несанкціонованого доступу до їх пристроїв третіх осіб. Автори роботи [9] наголошують: використання захищених паролем екранних заставок разом із гарною практикою використання паролів (дотримання вимог щодо їх складності, періодична зміна їх тощо) є важливими для зменшення кількості інцидентів інформаційної безпеки.

Загроза 3. Втрата цілісності даних.

Під час роботи на власних пристроях працівники можуть випадково модифікувати або вилучити чутливу інформацію організації [10-11]. Оскільки користувачі використовують BYOD як для особистих, так і для бізнес-цілей, обидва середовища повинні гармонійно співіснувати на одному пристрої [12]. Потрібно впроваджувати процедури безпеки для запобігання випадкової модифікації чи вилучення чутливої інформації організації. Ними можуть бути: заборона завантаження корпоративної інформації на особисті пристрої; резервне копіювання та контроль змін документів; застосування техніки віртуалізації для відокремлення на таких пристроях корпоративного простору від особистого [13].

Загроза 4. Зараження пристроїв шкідливим програмним забезпеченням.

Очевидно, що працівники, які працюють за концепцією BYOD, будуть використовувати свої пристрої для вирішення не тільки робочих, а й особистих повсякденних завдань. Завершивши роботу, вони будуть дивитися онлайн-відео, шукати реферати для дітей та грати в ігри, завантажені з торрент-трекерів. У результаті таких дій на пристроях можуть з'явитися шкідливі програми – шпигуни, шифрувальники та бекдори. При підключенні до корпоративної мережі весь цей набір шкідливих програм шукатиме собі нові жертви. І не виключено, що знайде.

У 2020 році частка атак на мобільні пристрої через застосунки становила вражаючі 96 % [6]. Річ у тім, що майже 4 з 5 застосунків містять сторонні бібліотеки, а вони можуть створювати вразливості.

Навіть якщо працівник поводитиметься відповідально, не відвідуватиме підозрілі сайти і не скачуватиме піратське програмне забезпечення, залишається проблема фішингових листів, а також підтримка операційних систем та програмного забезпечення в актуальному стані. Шкідливі програми, використовуючи вразливості, можуть проникнути на пристрій самостійно або з мінімальною участю користувача, що перейшов за посиланням у листі, дуже схожому на звичайний лист контрагента.

Загроза 5. Використання незахищених публічних мереж.

Працівники хочуть мати доступ до внутрішніх мереж організації, таких як корпоративні інтрамережі та сервери електронної пошти, із своїх BYOD-пристроїв навіть у той час, коли перебувають поза організацією. Такі підключення вони можуть здійснювати через мережі загального користування, використовуючи Wi-Fi-точки доступу, які зазвичай є безкоштовними і поширеними в громадських місцях: ресторанах, готелях та аеропортах. M. Souppaya і K. Kent [14] застерігають: громадські Wi-Fi-точки доступу вразливі до атак типу "людина посередині", підслуховування, що можуть призвести до компрометації цілісності та конфіденційності корпоративної інформації. Організації можуть знизити цей ризик, якщо працівники будуть підключатися через загальнодоступні мережі із застосуванням процедури шифрування каналу зв'язку на основі використання віртуальної приватної мережі (VPN) [15].

Загроза 6. Непоінформованість працівників щодо заходів ІБ та їх недбалість.

Згідно з звітом Verizon "Дослідження витоку даних за 2023 рік", 74 % усіх витоків спричинені персоналом організації [16]. Працівники, не маючи відповідних знань щодо інформаційної безпеки, не звертають уваги у своїй повсякденній трудовій діяльності на очевидні ризики, такі як віруси або крадіжка інтелектуальної власності; через свою необізнаність, а подекуди і недбалість, вони можуть здійснювати небезпечні дії.

Заходи щодо забезпечення інформаційної безпеки

Для того, щоб коректно мінімізувати ці та інші ризики BYOD, в ІБ-інфраструктурі організації має бути у повній мірі реалізовано функціональність системи контролю і управління доступом до мережі (Network Access Control, NAC). Інструменти NAC проактивні та призначені для запобігання несанкціонованому доступу до того, як це станеться. Вони захищають периметр мережі організації, включаючи фізичну інфраструктуру, пристрої, програмне забезпечення та хмарні ресурси. NAC пропонують зараз усі великі виробники засобів мережевого захисту: Cisco, Juniper, Microsoft, Symantec, Trend Micro. Свого часу ці системи створювалися саме для полегшення переведення бізнесових процесів на технології BYOD. Але в якийсь момент замовники все частіше стали впроваджувати та перепрофілювати їх під перспективніші завдання, такі як Інтернет речей. У результаті, у той час, коли в більшості організацій реалізовані так звані AAA-процеси ІБ (автентифікація, авторизація та аудит), не всі залучають засоби, за допомогою яких здійснюється автентифікація профілів безпеки кінцевих пристроїв.

У нинішніх умовах ІТ-відділам слід по максимуму використовувати системи управління мережевим доступом відповідно до їхнього початкового призначення. У NAC передбачено механізми контролю та перевірки пристроїв, які намагаються отримати доступ до корпоративної мережі, на відповідність політикам безпеки. У разі невідповідності система автоматично запускає на такому пристрої необхідні процедури нормалізації параметрів доступу відповідно до внутрішніх вимог ІБ. Якщо узгодження здійснити не вдасться, NAC заблокує йому доступ до корпоративної мережі.

Можливий інший варіант: пристрій, що не повністю відповідає політикам ІБ, отримає обмежений доступ до мережі, наприклад, до ізольованих обла-

стей, що не містять критично важливої інформації. Щоправда, для цього корпоративна мережа повинна бути сегментованою за підрозділами чи рівнями доступу або в рамках традиційних підходів з використанням віртуальних мереж (VLAN) та даних з каталогу Active Directory, або за допомогою програмно-визначених методів, наприклад, на основі технології Cisco TrustSec.

Крім NAC організаціям також слід звернути увагу ще на два класи рішень, націлених на контроль дій користувачів: системи управління мобільними пристроями (Mobile Device Management, MDM) та захисту від інформаційних витоків (Data Leak Prevention, DLP).

Як правило, MDM входять до складу ширшого корпоративного пакету EMS (Enterprise Mobility Suite), вони можуть відрізнятися за набором функцій, але більшість з них дозволяють:

- контроль доступу;
- управління програмами;
- забезпечення дотримання політик;
- оновлення "на льоту" (OTA-оновлення);
- виправлення неполадок пристроїв;
- відстеження пристроїв;
- дистанційне видалення інформації.

MDM – це, по суті, можливість контролю того, що користувач робить з пристроєм і що відбувається з корпоративними даними на ньому, а також того, як пристрої використовуються для доступу до корпоративної мережі.

У свою чергу DLP-системи дають організації можливість аналізувати поведінку працівників, зокрема прослідковувати куди відправляється конфіденційна інформація, чи не порушують користувачі встановлені правила інформаційного обміну. З допомогою DLP-систем можна навіть аналізувати, як працівники розпоряджаються робочим часом. Ці заходи навряд чи є першочерговими, проте їх можна розглядати як другий етап після побудови каркасу безпеки в організаціях, що впроваджують BYOD.

Безумовно, технічні процедури будуть максимально результативними, якщо їх підкріплювати організаційними діями: слід ввести внутрішньо-корпоративні регламенти та інструкції щодо роботи у віддаленому та гібридному режимі, оформляти додаткові угоди з працівниками, що стосуються поводження з конфіденційною інформацією, проводити спільні заходи по роз'ясненню відповідальності щодо виконання вимог інформаційної безпеки під час роботи з корпоративними ресурсами, сервісами та даними.

Рекомендується створити перелік програмного забезпечення, що дозволяється встановлювати працівникам на особистих пристроях, які використовуються у корпоративних цілях, та перелік забороненого програмного забезпечення. Бо в іншому випадку працівники матимуть усі підстави обрати його на свій розсуд, не переймаючись при цьому, що є цілком ймовірно, рівнем його захисту.

Необхідно чітко визначити, до яких програм та корпоративних мереж працівники можуть мати доступ зі своїх особистих пристроїв, а до яких підключення є забороненими. Контроль за виконанням цієї політики слід доручити здійснювати ІТ-відділу та відділу кібербезпеки.

Також необхідно виробити регламент щодо контролю безпеки BYOD-пристроїв, визначивши: яке захисне програмне забезпечення слід використовувати, які параметри його налаштування мають бути та які правила захисту доступу до інших встановлених на пристроях програм. Обов'язково потрібно прописати права організації у випадку втрати або крадіжки пристрою, розробити сценарії для віддаленого видалення даних з загублених пристроїв та заздалегідь визначити категорії даних, які можуть бути видалені.

Слід встановити жорсткі вимоги до паролів для облікових записів та корпоративних ресурсів, до яких працівники можуть отримувати доступ з мобільних пристроїв. Необхідно ретельно прописати політику щодо використання паролів, визначити правила, які стосуються їх складності та періодичності зміни. Встановити додаткові вимоги, наприклад, обов'язковість використання двофакторної аутентифікації. Узгодити умови щодо технічного обслуговування, ремонту пристроїв, включаючи можливість отримання тимчасового ноутбука чи планшета взамін основного пристрою на період ремонту.

У рамках політики ІБ необхідно чітко визначити вимогу щодо проходження тренінгів з кібербезпеки для всіх працівників, незалежно від того, чи використовують вони для роботи власний пристрій чи ні. Зрозуміло, що у випадку використання ця вимога набуває особливого значення.

Важливо обговорити з працівниками, які погодились застосовувати власні пристроїв для вирішення робочих завдань, принципові питання, що стосуються даних, розташованих на цих пристроях, зокрема, слід розглянути можливі ризики втрати конфіденційності особистих даних користувача. Це спростить подальшу взаємодію як для працівника, так і для технічних фахівців. Якщо контроль за дотриманням інформаційної безпеки в організації передбачає аналіз онлайн-активності користувача, встановлення програмного забезпечення для моніторингу конкретних процесів, то працівник повинен бути про це поінформований, він повинен розуміти усі пов'язані з цим ризики. Важливо, щоб працівник усвідомлював: якщо під час свого робочого часу він переглядатиме соцмережі чи працюватиме з контентом особистого характеру, то роботодавець, ймовірно, про це знатиме.

У BYOD-політику можна включити деякі вимоги, які не стосуються кібербезпеки. Наприклад, можна ввести заборону використання робочого пристрою під час водіння автомобіля, а також заборону на фото- та відеозйомку робочих приміщень, колег чи робочих процесів. При розробленні політики BYOD варто також прописати відповідальність працівника за недотримання ІБ і під час найму, і після його звільнення.

Необхідно розробити протокол звільнення – перелік дій, які слід виконати: видалення з особистого пристрою працівника програм та даних, позбавлення доступу до робочих акаунтів.

Потрібно мати чітке розуміння того, що відбувається, коли звільняється незадоволений працівник, який мав доступ до чутливих даних організації [17], а також що відбувається, коли розривається контракт з обслуговуючим розробником.

У цьому випадку ІТ-відділ повинен дати відповіді на низку запитань:

– Як довго триватиме процес, необхідний, щоб видалити дані з пристрою або змінити паролі?

– Чи відомо, які пристрої використовувалися?

– Чи використовувалися лише підтверджені політиками пристрої чи були й інші?

– Які програми використовувалися?

– Який рівень доступу вони мали?

– Де зберігалися дані?

– Хто ще мав доступ до даних на смартфонах працівників?

– Чи можна законно видалити інформацію на їхніх пристроях?

Потрібен план не лише для екстрених ситуацій, коли працівник звільняється терміново або заднім числом, але й для стандартних ситуацій, бо згідно з недавніми дослідженнями, 87% опитаних працівників зізналися, що після звільнення на їх комп'ютерах та мобільних телефонах залишилася інформація, пов'язана з попередньою роботою [15]. Що буде, якщо вони використовуватимуть ці дані зловмисно або якщо вони самі постраждають від фішингатаки, і в результаті шахрайства ці дані потраплять третім особам? Потрібно бути готовим до будь-якого розвитку подій.

Тому у випадку звільнення працівника необхідно:

– переконатися, що відділи HR та IT працюють синхронно;

– переконатися, що діють угоди про нерозголошення та безпекову політику;

– повернути пристрої, надані організацією;

– видалити корпоративні програми та дані з особистих пристроїв;

– вимкнути доступ до корпоративної електронної пошти;

– вимкнути доступ до корпоративних систем та застосунків;

– змінити паролі до корпоративних облікових записів;

– моніторити підозрілу активність.

У кризовій ситуації слід:

– документувати ризики та активи;

– створити та навчити команду реагувати на інциденти;

– створити систему звітів про інциденти;

– підготувати список повідомлень про інциденти;

– провести резервне копіювання важливих даних;

– переконатися, що інциденти можуть бути опрацьовані дистанційно;

– пропрацювати реагування на інциденти.

Випередити загрози непросто, але чіткий план дій допоможе звільнити працівників з мінімальним ризиком для організації і, у разі виникнення кризи, мінімізувати завдану шкоду.

Висновки. Організації повинні усвідомлювати, що не існує єдиного універсального засобу, здатного водночас вирішити усі проблеми інформаційної безпеки, пов'язані з дозволом використання BYOD. Запорукою успішного рішення може стати лише системний підхід, орієнтований на застосування ефективних практик у сфері технологій захисту інформації; рішень з безпеки мережевої інфраструктури. Також не менш важливим чинником є використання низки організаційних заходів – створення комплексу правил та інструкцій для роботи з мобільними пристроями, спрямованих на забезпечення інформаційної безпеки. У той же час слід розуміти: різні організації мають різні пріоритети інформаційної безпеки, які залежать від бізнес-цілей організації. Наступні дослідження стосуватимуться вивчення стратегій, що застосовуються організаціями для зниження ризиків інформаційної безпеки, з врахуванням їхньої сфери діяльності.

Список літератури

[1]. 2021 BYOD Security Report. URL: https://pages.bitglass.com/rs/418-ZAL-815/images/CDFY21Q2-BYOD2021.pdf.

[2]. Howarth J. 24+ Fascinating BYOD Statistics (2024). URL: https: // explodingtopics.com/blog/byod-stats.

[3]. Global BYOD and Enterprise Mobility Market. Global Strategic Business Report. URL: https://www.researchandmarkets.com/reports/4804695/byod-and-enterprise-mobility-global-strategic.

[4]. Юстус М. (2020). Як керувати пристроями співробітника, що працює віддалено. URL: https://ko.com.ua/kak_upravlyat_ustrojstvami_sotrudnika_rabotayushhego_udalenno_132967.

[5]. Employees Say Smartphones Boost Productivity by 34 Percent: Frost & Sullivan Research. URL: https: // insights. samsung. com / 2016 / 08 / 03 / employees-say-smartphones-boost-productivity-by-34-percent-frost-sullivan-researc.

[6]. Принеси власний пристрій: заходи безпеки при використанні особистих пристроїв на роботі. URL: https: // www.kingston.com / ua/blog/data-security/bring-your-own-device-workplace-security.

[7]. Збільшення випадків втрати пристроїв на 25% вказує на ризик для мандрівників. URL: https: //www.kingston.com/ua/blog/data-security/commuters-lost-devices-security-threat.

[8]. Donovan, F. (2014). Employees Fail to Take Basic Steps to Secure BYOD Devices, Data, Fierce Mobile IT, 9, 1.

[9]. Cappelli, D., Moore, A., & Trzeciak, R. (2012). The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). Upper Saddle River, NJ Addison-Wesley.

[10]. Dong, Y., Mao, J., Guan, H., Li, J., & Chen, Y. (2015). A Virtualization Solution for BYOD with Dynamic Platform Context Switching, IEEE Micro, 35(1), pp. 34-43. https://doi.org/10.1109/MM.2015.3.

[11]. Miller, K.W., Voas, J., & Hurlburt, G.F. (2012). BYOD: Security and Privacy Considerations, IT Professional, 14(5), pp. 53-55. https://doi.org/10.1109/ MITP. 2012.93.

[12]. Wang, Y., Wei, J., & Vangury, K. (2014). Bring Your Own Device Security Issues and Challenges, 11th Consumer Communications and Networking Conf (CCNC), 2014 IEEE, pp. 80-85. https://doi.org/10.1109/ CCNC.2014.6866552.

[13]. Vishal, G., Deepak, S., & Lovekesh, D. (2013). An Approach to Implement Bring Your Own Device (BYOD) Securely, International Journal of Engineering Innovations and Research, 2(2), pp. 154-156.

[14]. Souppaya, M., & Kent, K.A. (2012). Guidelines for Managing and Securing Mobile Devices in the Enterprise: Recommendations of the National Institute of Standards and Technology. US Department of Commerce, National Institute of Standards and Technology. https://csrc.nist.rip/library/alt-SP800-124r1.pdf.

[15]. Ketel, M., & Shumate, T. (2015). Bring Your Own Device: Security Technologies, SoutheastCon, pp. 1-7. https://doi.org/10.1109/SECON.2015.7132981.

[16]. 2023 Data Breach Investigations Report. URL: https://www.verizon.com/business/resources/reports/dbir/.

[17]. Kukharska, N., & Lagun, A. (2023). Human recourses management as a component of organization information security. Electronic Professional Scientific Edition "Cybersecurity: Education, Science, Technique", (20), pp. 35-44.

УДК 004.056.5

Kukharska N., Lagun A. Ensuring the information security of the organization when implementing the BYOD concept

Abstract. *The BYOD concept involves the use of personal electronic devices (laptops, tablets, smartphones) by employees of the organization for official purposes. The idea of such a concept appeared in the mid-2000s, but only recently it gained popularity. The reason for this is the growing dependence of business processes on services located on the Internet, advances in mobile device production, expanding devices' capabilities and increasing productivity, as well as the development of network technologies and cloud storage. Like any concept, BYOD has its advantages and disadvantages. The positive aspects of this approach to the organization of the work process include, in particular, convenience for the user and the possibility of remote work, which allows organizations to use the working time of employees more efficiently, increase the efficiency of solving various tasks and thus achieve an increase in labor productivity. The main problem associated with the implementation of the BYOD concept is ensuring the security of the organization's information system. The more freedom employees using personal devices have to interact with an organization's network, the more potential damage they can cause to it. The article examines information security threats associated with the use of BYOD and gives recommendations on reducing their negative impact on the organization. In particular, it is suggested to use NAC to manage network access; install MDM to manage the security of mobile devices; implement DLP to protect against information leaks; use reliable passwords with regular updates to prevent unauthorized access; install organization-approved anti-virus software on employee-owned devices; perform data encryption; set restrictions on downloading and installing programs; implement a comprehensive IT policy.*

Keywords: *information security, the Bring Your Own Device (BYOD) concept, information protection, Network Access Control (NAC), Mobile Device Management (MDM), Data Leak Prevention (DLP).*

Кухарська Наталія Павлівна, кандидат фізико-математичних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного університету "Львівська політехніка".

Nataliia Kukharska, candidate of physical and mathematical sciences, associate professor, senior lecturer of the department of security of information technologies of the Lviv Polytechnic National University.

Лагун Андрій Едуардович, кандидат технічних наук, доцент, завідуючий кафедрою інформаційних систем і технологій Національного університету "Львівська політехніка".

Andrii Lagun, candidate of technical sciences, associate professor, head of the department of information systems and technologies of the Lviv Polytechnic National University.

Отримано *17 січня 2024 року,* затверджено редколегією *1 квітня 2024 року*