УДК 004.056.53(045)
DOI: 10.31673/2409-7292.2025.020383

Вербиненко В.О., Зибін С.В.

ПРОБЛЕМИ КІБЕРБЕЗПЕКИ В ОРГАНІЗАЦІЯХ З ДИСТАНЦІЙНОЮ ФОРМОЮ ПРАЦІ

Стрімке поширення віддаленої роботи у світі створює нові виклики для забезпечення ефективної та безпечної цифрової взаємодії в організаціях. Метою даного дослідження є комплексний аналіз сучасних підходів, інструментів та організаційно-правових засобів, що використовуються для організації захищеної цифрової взаємодії в умовах віддаленої праці. Для досягнення поставленої мети застосовано метод аналізу літературних джерел, який дозволив систематизувати інформацію про технологічні рішення, управлінські практики та нормативні вимоги, пов'язані з віддаленою роботою.

Проаналізовано основні ключові аспекти: цифрові платформи та сервіси для комунікації й спільної роботи, управління користувацькими пристроями та концепцію Bring Your Own Device (BYOD), а також правове регулювання сфери кібербезпеки та приватності. За результатами дослідження встановлено, що використання уніфікованих платформ для управління корпоративними сервісами зменшує фрагментацію цифрового середовища та ризики витоку даних; надання співробітникам захищених корпоративних пристроїв або запровадження чітких політик BYOD мінімізує основні кіберзагрози; дотримання міжнародних стандартів і національного законодавства у сфері захисту інформації забезпечує правову відповідність діяльності розподіленого колективу. Комплексний підхід, який поєднує сучасні технологічні інструменти, ефективне управління та виконання правових норм, дозволяє підвищити рівень інформаційної безпеки та ефективності дистанційної роботи, мінімізуючи потенційні ризики.

Ключові слова: кібербезпека, безпека хмарних технологій, віддалена робота, BYOD, правове регулювання.

Вступ

Поширення дистанційної (або віддаленої) форми праці стало визначальним наслідком глобальних змін, спричинених пандемією COVID-19 та подальшими геополітичними трансформаціями. Підприємства у всьому світі були змушені адаптувати свої бізнес-процеси до нових умов, впроваджуючи цифрові рішення, які дозволяють співробітникам ефективно працювати поза межами офісу. Цей тренд набув особливої актуальності в Україні після 2022 року, коли мільйони громадян опинилися за кордоном, але продовжили професійну діяльність в українському економічному просторі. Як наслідок, підтримка цифрової взаємодії у віддаленому режимі стала не лише операційним, а й стратегічним завданням для організацій.

Зростання кількості дистанційних робочих місць, зумовлене глобальними викликами, трансформувало підхід компаній до власних операційних процесів [1].

Сучасні організації, що діють у повністю віддаленому форматі, характеризуються відсутністю власної фізичної інфраструктури, зокрема офісних приміщень або локальних серверів. Із розвитком цифрових технологій, зокрема хмарних обчислень, комунікаційних платформ і сервісів дистанційного управління, подібна організаційна модель не лише стала технічно можливою, але й перетворилася на необхідну умову функціонування для багатьох підприємств, особливо зважаючи на збільшення вимог до гнучкості графіку зі сторони працівників та зменшенню кількості професій, які залежать від стабільного місця роботи [2].

Водночас впровадження віддаленої роботи створює численні виклики у сфері кібербезпеки, зокрема через збільшення периметру атаки, використання неконтрольованих мереж, нестабільну цифрову гігієну працівників та необхідність швидкої адаптації до нових режимів доступу. У відповідь на це компанії змушені переглядати підходи до захисту інформаційної інфраструктури, впроваджуючи як технічні, так і організаційно-правові механізми. Водночас самі працівники нерідко сприймають інструменти контролю як інвазію в особистий простір, що знижує ефективність впроваджених рішень.

Мета та завдання дослідження

Дана стаття є оглядовим дослідженням, метою якого є комплексний аналіз підходів, інструментів та організаційно-правових засобів для забезпечення захищеної цифрової

взаємодії при дистанційній праці. Для досягнення цієї мети використано метод аналізу літературних джерел, що дозволяє вивчити й узагальнити досвід попередніх досліджень і практик. У статті розглядаються три ключові аспекти, від яких залежить успішна робота розподілених команд: по-перше, сучасні програмні платформи та цифрові сервіси для комунікації, спільної роботи й захисту даних (хмарні середовища, системи автентифікації, VPN, концепції Zero Trust тощо) [3]; по-друге, управління користувацькими пристроями, включно з політикою BYOD, тобто використанням персональних пристроїв працівників, та засобами їх централізованого адміністрування (MDM, Zero-Touch Deployment тощо); по-третє, правове регулювання сфери кібербезпеки й захисту інформації у різних юрисдикціях (дотримання стандартів GDPR, CCPA та відповідних національних законодавчих вимог). Застосування такого підходу дозволяє сформувати цілісне уявлення про наявні рішення та проблеми, а також визначити напрями для їх подальшого розвитку.

Для досягнення поставленої мети, необхідно зосередитись на трьох ключових складових. Першою складовою є аналіз програмного забезпечення та цифрових сервісів, що використовуються компаніями для забезпечення комунікації, спільної роботи та захисту даних.

Другою складовою є використання пристроїв для віддаленої роботи – зокрема, корпоративних ноутбуків з попередньо встановленими політиками безпеки або особистих пристроїв працівників (концепція BYOD). Надання захищених, централізовано керованих пристроїв, а також застосування засобів Mobile Device Management (MDM) і Zero-Touch Deployment є важливою умовою безпечного доступу до корпоративної інфраструктури [4].

Третім критичним аспектом є врахування особливостей правового регулювання у різних юрисдикціях, де перебувають працівники. Зокрема, мова йде про дотримання вимог Загального регламенту захисту даних ЄС (GDPR), законів США (CCPA) та аналогічних норм інших країн. Дотримання правових вимог є не менш важливим, ніж технічні рішення, оскільки порушення законодавства щодо обробки персональних даних може спричинити юридичні наслідки та втрату репутації [5, 6].

Результати дослідження

Цифрові платформи та сервіси

Сучасні підприємства, що працюють у віддаленому форматі, дедалі більше покладаються на хмарні інструменти для забезпечення продуктивності. Це включає сервіси для створення та редагування документів, обміну повідомленнями, проведення відеоконференцій, управління проєктами та розкладом. У більш технологічно розвинених організаціях використовуються також внутрішні CRM-системи, бази даних і виділені сервери.

Використання уніфікованих рішень, таких як Google Workspace або Microsoft 365, дозволяє досягти високого рівня інтеграції, спрощує адміністрування, централізує контроль доступу та допомагає реалізовувати комплексні політики інформаційної безпеки на рівні всієї організації. Такі рішення знижують ризики через меншу кількість точок входу для атак. Ефективною практикою в подібних системах є впровадження багатофакторної автентифікації (MFA) для всіх користувачів і розподілення прав доступу за допомогою адміністративних інструментів.

Натомість розподілені інфраструктури, що використовують інструменти від різних постачальників, потребують значно більшої складності в управлінні, а також створюють ризики несумісності політик шифрування, автентифікації та контролю доступу. Це може призвести до фрагментації безпекових механізмів і збільшення вразливостей у системі. Крім того, часто виникає явище створення тіньових даних – ситуації, коли співробітники використовують сторонні сервіси без дозволу IT-відділу, що створює "сліпі зони" в інформаційній безпеці та підвищує ризик витоку даних [7].

Варто зазначити, що загроза від поширення тіньових даних може виникнути навіть при використанні комплексних уніфікованих рішень. Ризики, пов’язані з подібними загрозами в

організаціях з віддаленим типом працевлаштування, можна зменшити шляхом регулярних навчальних заходів, спрямованих на підвищення обізнаності персоналу щодо небезпек використання сторонніх інструментів, зокрема несанкціонованих месенджерів чи онлайн-редакторів.

Незалежно від обраної архітектури, людський фактор залишається критичною вразливістю в сфері кібербезпеки. За даними IBM Cost of a Data Breach Report 2024 [8], фішинг є другим за поширеністю вектором атак і став причиною 15% витоків даних. Одним з найтриваліших за часом усунення інцидентів залишаються порушення, пов'язані з викраденими або скомпрометованими обліковими даними – в середньому потрібно 292 дні, щоб їх виявити та вжити необхідних заходів з нівелювання загрози.

У звіті IBM [8] також згадуються тіньові дані. У 2024 році 35% інцидентів порушення безпеки були пов'язані саме з таким типом інформації. Ці витоки виявилися також на 16% дорожчими у ліквідації. Крім того, зберігання даних у кількох середовищах (гібридні стратегії) виявилося особливо вразливим: 40% витоків сталися саме в таких умовах, і їм притаманний подовжений час виявлення та реагування.

Для порівняння, витоки даних в межах одного типу середовища відбувалися рідше – у публічній хмарі (25%), на локальних серверах (20%) або в приватній хмарі (15%). Ці показники свідчать про необхідність зменшення кількості середовищ для зберігання даних та централізації політик доступу.

Окремою ланкою тут варто зазначити хмарну інфраструктуру, таку як сервери, бази даних чи сховища архівних файлів або логів. Все це може бути вкрай необхідним в діяльності компанії. Наприклад, компанія може мати власний сайт або підтримувати власний онлайн-сервіс. Якщо компанія публічна і працює на фондовому ринку США, згідно з вимогами одного з американських законів, а саме Сарбейнса-Окслі (SOX) [9], для таких компаній фінансова документація, включно з відповідними журналами логів, повинна зберігатися щонайменше сім років. Багато хмарних сервісів не надають можливості зберігати дані так довго, тому необхідно заздалегідь продумати механізм експорту журналів до спеціалізованого сховища або системи резервного зберігання, яка забезпечує відповідність нормативним вимогам.

Оскільки подібні ресурси є особливо критичними для діяльності компанії, доступ до них має бути суворо регламентованим і технічно контрольованим. Вони мають періодично проходити аудит на вразливості, а заходи для покращення безпеки таких ресурсів мають постійно оновлюватися та підтримуватись.

Таким чином, підприємствам, що працюють у віддаленому середовищі, рекомендується впроваджувати уніфіковані платформи управління цифровими сервісами, зменшувати кількість окремих середовищ для зберігання даних, а також встановлювати чітку політику доступу та моніторингу активів.

Хоча дослідження від 2023 року показують, що режим віддаленої роботи може позитивно впливати на рівень обізнаності у сфері кібербезпеки [10], регулярні тренінги не стали менш важливими для персоналу, завдяки тому що вони сприяють зниженню впливу людського фактора.

У контексті загроз, які мають безпосередній вплив на компанії у віддаленому режимі роботи, наукові джерела виокремлюють такі основні напрями:

1. Ризик компрометації облікових даних через фішинг, атаки на MFA або повторне використання паролів [11];
2. Складність забезпечення постійного моніторингу та реагування на інциденти у розподілених системах [12];
3. Використання несанкціонованих додатків і створення тіньових даних, які уникають контролю з боку IT-відділів [13];
4. Соціальна інженерія, що легко реалізується в умовах ізольованої комунікації, характерної для дистанційної роботи [14].

© Вербиненко В.О., Зибін С.В. (2025). Проблеми кібербезпеки в організаціях з дистанційною формою праці. Сучасний захист інформації, 2(62), 22–30.
https://doi.org/10.31673/2409-7292.2025.020383

Користувацькі пристрої

У компаніях з віддаленим режимом роботи працівники виконують поставлені задачі, використовуючи як надану, так і особисту техніку, підключаючись до корпоративних сервісів, таких як месенджери або програми для створення чи редагування файлів через домашні мережі. Усе це збільшило навантаження на адміністрування пристроїв та послуг, значно розширивши цифрову інфраструктуру компаній і, відповідно, – потенційний периметр атаки.

Кожен працівник і кожен пристрій, з якого він працює, перетворився на окрему точку входу в інфраструктуру організації. Інвестуючи в ноутбуки працівників, бізнес очікує не просто можливості для них виконувати робочі обов'язки, а й кращої захищеності інформації. Додатковими засобами кібербезпеки на робочих пристроях слугують VPN-доступи, агенти для моніторингу систем, антивірусні рішення та менеджери паролів.

Для забезпечення керованості та безпеки пристроїв джерела рекомендують впроваджувати стандартизовані засоби управління, які поєднують налаштування, політики й моніторинг [10]. Найкращою практикою визнано використання попередньо налаштованих корпоративних пристроїв із багатофакторною автентифікацією, шифруванням дисків і вбудованим засобом віддаленого контролю. Такі пристрої мінімізують потребу в ручному втручанні з боку користувача та одразу готові до безпечної роботи.

Концепція, за якою працівник виконує задачі, використовуючи особистий пристрій, отримала назву Bring Your Own Device. Вона дозволяє співробітникам працювати з власних ноутбуків або смартфонів. Це сприяє зручності, проте створює значні ризики: особисті пристрої рідко повністю відповідають вимогам корпоративної безпеки. Наприклад, 21% компаній мали проблеми з кібербезпекою через підключення працівників до сумнівних Wi-Fi мереж [5].

З огляду на джерела, можемо виділити ключові технічні загрози пов'язані з пристроями для компаній із віддаленим режимом роботи:

Компрометація пристроїв, що використовуються поза корпоративним захистом [15].

Незахищені домашні мережі Wi-Fi, які не відповідають сучасним стандартам безпеки (наприклад, WPA3), використовують слабкі паролі або застарілі налаштування. Домашні роутери часто стають точкою входу для атак, що далі поширюються на підключені пристрої [16].

Небезпечні дозволи мобільних застосунків. Дослідження вказують, що багато додатків запитують надмірні дозволи, наприклад, доступ до мікрофона, контактів або геолокації, що може становити загрозу витоку конфіденційної інформації [17].

Відсутність регулярних оновлень і патчів, що відкриває пристрої до відомих вразливостей [18]. Попри регулярні звіти OWASP або CISA на дану тематику, в академічному середовищі ця проблема не має достатньо публікацій, які б її розглядали.

Фізична втрата пристрою, що не має шифрування або функцій віддаленого стирання даних, створює значний ризик несанкціонованого доступу до робочої інформації.

Відомі інциденти компрометації підтверджують ці ризики. Наприклад, у 2022-2023 роках компанії LastPass та Okta повідомили про витоки даних, що починалися саме з персональних пристроїв співробітників, які були зламані через фішингові повідомлення або вразливості у домашній інфраструктурі.

При концепції BYOD на особистий пристрій співробітника компанії встановлюється необхідне для кібербезпеки програмне забезпечення, таке як згадані раніше агенти для моніторингу систем та антивіруси. Часто також встановлюється програма для віддаленого доступу адміністратора і утиліти, які дозволяють розгортати інше програмне забезпечення. Набуває поширення також практика контейнеризації – розділення особистих і робочих даних, наприклад, через окремі профілі або віртуальні робочі столи (VDI).

Однак перехід на режим віддаленої роботи для менеджменту став причиною впровадження різноманітних систем контролю за робочими процесами колег, зокрема шляхом

встановлення систем моніторингу. Такі програми відстежують активність користувача, реєструють рухи миші, кількість натискань клавіш, а іноді навіть фіксують скріншоти з екранів.

Подібні інструменти часто сприймаються як інвазивні [19], особливо якщо вони накладаються на інші програми кібербезпеки, які можуть втручатися у взаємодію з пристроєм. У результаті працівники можуть ототожнювати засоби безпеки із засобами контролю, що створює недовіру до ІТ-відділу та фахівців з безпеки. Це, своєю чергою, може бути причиною відходу працівників від прийнятої політики безпеки, відмови реєструвати нові пристрої і встановлювати на них необхідні програми для підтримки кібернетичної безпеки, а отже – виникнення більшої кількості тіньових даних.

Етичний вимір BYOD-підходу вивчається у науковій літературі як частина ширшого дискурсу про приватність та етичність. BYOD змінює межі між особистим і професійним простором. Виникає етична дилема: наскільки компанія має право втручатися в особисті пристрої, навіть якщо на них встановлені корпоративні застосунки. Відсутність прозорості у правилах використання таких технологій породжує недовіру, що може вплинути на моральний стан команди. Таким чином, політика BYOD повинна бути не лише технічно надійною, а й етично обґрунтованою [20].

Оптимальним рішенням є надання працівникам попередньо налаштованих корпоративних пристроїв, готових до роботи з моменту увімкнення. Мова не про просту видачу техніки, а про попередньо налаштовані пристрої з уже встановленими політиками безпеки та програмним забезпеченням, необхідним для роботи. У такий спосіб відбувається розмежування віртуального особистого і робочого простору, що дає необхідний рівень приватності при забезпеченні всіх заходів кібернетичної безпеки на пристроях.

Сучасні практики менеджменту пристроїв наголошують на використанні так званого «розгортання без дотику» (zero-touch deployment) [4]. Це означає, що працівнику не потрібно самостійно встановлювати необхідне програмне забезпечення – пристрій вже налаштований у відповідності до вимог компанії.

Наприклад, компанія Apple пропонує рішення Apple Business Manager (ABM), яке дозволяє заздалегідь зареєструвати пристрої в системі MDM (Mobile Device Management). Завдяки цьому, як тільки працівник отримує пристрій і входить у систему, йому автоматично надаються всі потрібні додатки, конфігурації та політики безпеки.

Для користувачів Windows подібну функціональність забезпечує Windows Autopilot, який входить до складу Microsoft Endpoint Manager. Це рішення дозволяє автоматично приєднувати пристрої до системи Intune – мобільної платформи для управління пристроями Microsoft. Завдяки цьому пристрої також отримують готові корпоративні профілі, налаштування та політики безпеки без необхідності ручного втручання.

Це гарантує, що пристрої отримують необхідні профілі без ручного налаштування з боку працівника, мінімізуючи людський фактор.

Наявність системи MDM (Mobile Device Management) дозволяє централізовано:

- застосовувати політики щодо паролів, шифрування, оновлень;
- здійснювати моніторинг стану пристроїв;
- стирати дані у разі втрати або компрометації.

Це дає змогу ІТ-відділу підтримувати стандартизоване середовище безпеки незалежно від локації працівника [4]. Перешкодою до застосування подібних технологій є їх поки що слабке поширення у різних регіонах світу і необхідність постачальників техніки та тісної співпраці безпосередньо з виробниками пристроїв.

Юридичні аспекти

Через те, що географічні межі в умовах дистанційної роботи розмиті, організація може бути зареєстрована в одній країні, але її співробітники працюватимуть із персональними даними громадян інших держав. У таких випадках компанія повинна забезпечити

відповідність своїх політик безпеки усім чинним нормам – від загальних правил захисту персональних даних до галузевих стандартів і локальних законів, що стосуються кібербезпеки.

Наприклад, будь-яка обробка особистих даних резидентів Європейського Союзу автоматично підпадає під дію Загального регламенту захисту даних (GDPR). Цей регламент висуває суворі вимоги до обробки персональної інформації, зокрема передбачає використання технічних і організаційних засобів захисту – таких як шифрування даних «у стані спокою» та «в дорозі», контроль доступу до інформації та процедури інформування про витоки [21].

Дослідження, присвячені поширенню віддаленого режиму роботи, показують, що відповідність вимогам GDPR має свої унікальні виклики: від забезпечення достатнього рівня безпеки домашніх мереж працівників до контролю за міжнародною передачею даних, коли співробітники переміщують файли між країнами.

Компанії повинні оновити свої політики безпеки, чітко вказавши, як саме дані мають зберігатися, передаватися та використовуватись віддаленими працівниками відповідно до законодавства. У США, наприклад, особливо важливо дотримуватися таких актів, як Закон про конфіденційність споживачів Каліфорнії (CCPA), а також інших федеральних та штатних законів, які регулюють поводження з персональними даними.

Крім ЄС і США, інші країни також мають аналогічні законодавчі вимоги: закон про кібербезпеку Сінгапуру, Закон про загальний захист даних Бразилії (LGPD) тощо. Всі ці акти можуть впливати на те, як компанія контролює безпеку віддалених систем, моніторинг і аудит [22].

Ще одним важливим аспектом є правила локалізації даних, які зобов'язують зберігати певні види інформації (наприклад, фінансові або медичні записи) в межах певної країни або передавати їх лише з дотриманням спеціальних заходів безпеки.

На практиці побудова юридично узгодженої системи кібербезпеки для віддаленої роботи потребує участі юристів, які зможуть проаналізувати законодавство кожної юрисдикції, де працюють співробітники, і допомогти адаптувати політики компанії. Одним із підходів є створення загальної політики безпеки з найвищим рівнем захисту, який відповідає вимогам усіх країн, або ж додавання до політики спеціальних розділів для окремих регіонів.

Таким чином, надійна система кібербезпеки для віддаленої роботи – це не лише питання технологій, а й відповідності юридичним стандартам. Щоб уникнути штрафів, санкцій або втрати довіри з боку клієнтів, компанії повинні постійно стежити за змінами у міжнародному та національному законодавстві і адаптувати свої внутрішні політики відповідно до нових вимог.

Компанії з віддаленим форматом праці стикаються з низкою юридичних загроз, серед яких:

1. Суперечності у локальних вимогах до зберігання даних, які можуть накладати обов'язок зберігати дані фізично на території конкретної держави [23];

2. Юридична невизначеність щодо відповідальності компанії за дії працівника, який працює з даними з-за кордону, у разі витоку або порушення [24];

3. Використання програм моніторингу продуктивності працівників, що може суперечити нормам права на приватність у деяких юрисдикціях [25].

В Україні захист персональних даних під час дистанційної роботи має низку специфічних викликів, зумовлених як нормативною базою, так і поточною безпековою ситуацією. Незважаючи на декларовану відповідність європейським стандартам, механізми контролю за обробкою даних залишаються недостатньо ефективними, особливо в умовах цифровізації державних сервісів і зростання ролі віддаленої праці [26].

Повномасштабна війна посилила потребу у цифровій безпеці: організації впроваджували шифрування, переносили сервери за кордон, адаптували політики до нових ризиків. Водночас посилилася міжнародна співпраця у сфері кіберзахисту, що стало важливою складовою підвищення стійкості цифрової інфраструктури [26].

© Вербиненко В.О., Зибін С.В. (2025). Проблеми кібербезпеки в організаціях з дистанційною формою праці. Сучасний захист інформації, 2(62), 22–30.
https://doi.org/10.31673/2409-7292.2025.020383

Дискусія та обговорення

Проведений огляд виявив ряд питань, що залишаються дискусійними або неоднозначно трактуються різними авторами. Одне з таких питань – вплив віддаленого формату роботи на культуру кібербезпеки в організації. Деякі дослідження вказують на позитивний ефект дистанційної роботи: зокрема, підвищення обізнаності співробітників щодо кіберзагроз та відповідальних поведінкових практик. Можливо, працюючи поза офісом, персонал приділяє більше уваги захисту власних пристроїв і даних, усвідомлюючи вразливість розподіленого середовища. Водночас інші джерела наголошують, що людський фактор залишається одним із найслабших місць системи безпеки. Тому, незважаючи на певне зростання обізнаності, регулярні навчання та тренінги з кібербезпеки для персоналу не втрачають своєї актуальності. Навпаки, у віддаленому режимі такі заходи набувають особливого значення, оскільки допомагають мінімізувати ризики, пов'язані з помилками або недбалістю користувачів.

Ще однією складною темою є вибір між використанням персональних пристроїв працівників (концепція BYOD) та забезпеченням усіх співробітників корпоративною технікою. Літературні джерела пропонують різні підходи до цієї проблеми. З одного боку, модель BYOD підвищує гнучкість і мобільність роботи та може скоротити витрати компанії на обладнання, проте одночасно створює додаткові кіберризики. Особисті пристрої не завжди відповідають корпоративним стандартам безпеки, можуть містити уразливе або застаріле програмне забезпечення і частіше підключаються до незахищених мереж. З іншого боку, надання всім співробітникам уніфікованих захищених ноутбуків із наперед налаштованими політиками безпеки дозволяє значно знизити ймовірність компрометації даних, але потребує суттєвих ресурсів. Крім того, повний контроль компанії над робочими пристроями порушує межі особистого простору працівників, що створює етичні питання. Таким чином, при виборі стратегії щодо користувацьких пристроїв виникає дилема між зручністю і безпекою. Для успішної реалізації BYOD організації мусять впроваджувати суворі політики управління пристроями, засоби шифрування та моніторингу, а також забезпечити прозорість і дотримання етичних норм стосовно приватності співробітників.

Неоднозначності присутні і в площині правового регулювання. Розмитість географічних меж дистанційної роботи призводить до того, що компанії повинні дотримуватися одночасно декількох юрисдикцій. Виникає напруженість між потребою контролювати продуктивність віддалених працівників і обов'язком забезпечувати їхнє право на приватність. Сучасні програмні засоби дозволяють детально відстежувати дії персоналу онлайн, проте в деяких країнах надмірний електронний нагляд може розцінюватися як порушення законодавства про захист персональних даних. Наприклад, використання інструментів моніторингу робочого часу чи запису екрану співробітника потенційно суперечить вимогам GDPR у Європейському Союзі. Така ситуація ставить перед глобальними організаціями непросте завдання: знайти баланс між ефективним управлінням командою та виконанням правових норм різних держав. Одним із підходів є розробка чітких внутрішніх політик, які б обмежували обсяг контролю та водночас відповідає законодавчим вимогам усіх юрисдикцій, де працюють співробітники. Проте універсальних рішень наразі бракує, що вказує на необхідність подальших досліджень у цьому напрямі.

Зважаючи на динамічність розвитку технологій і моделей організації праці, виявлені проблеми потребують глибшого наукового опрацювання. Перспективним напрямком подальших досліджень є оцінка довгострокової ефективності комплексних систем кібербезпеки у повністю віддалених компаніях: наскільки впровадження таких систем (зокрема, концепції Zero Trust чи централізованих платформ управління) впливає на зниження кількості інцидентів та підвищення довіри клієнтів. Вартим уваги є й питання людського фактору в умовах цифрової ізольованості – потрібні соціально-психологічні дослідження того, як підтримувати належний рівень дисципліни й мотивації працівників дотримуватися політик безпеки без прямого контролю. Окремо слід дослідити шляхи гармонізації міжнародних і

національних вимог: міждисциплінарні студії за участю фахівців з права, інформаційної безпеки та менеджменту можуть виробити рекомендації щодо уніфікації підходів до кібербезпеки у дистанційному режимі, які враховують як технічні, так і правові чинники.

Висновки

У межах огляду літературних джерел було всебічно проаналізовано сучасні рішення та підходи до забезпечення ефективної і захищеної роботи розподілених команд, зокрема у сфері впровадження цифрових платформ, управління віддаленими пристроями та дотримання нормативно-правових вимог. Це дозволило сформувати цілісне уявлення щодо найкращих практик та типових проблем, з якими стикаються організації в умовах дистанційної діяльності.

Результати аналізу підтверджують, що успішна реалізація дистанційної роботи потребує інтегрованого поєднання технологічних, організаційних і правових заходів. Використання сучасних цифрових інструментів, упровадження обґрунтованих політик управління пристроями та інформаційною безпекою (включно з контролем BYOD), а також неухильне дотримання вимог законодавства (як міжнародних, так і локальних) є ключовими умовами мінімізації ризиків і забезпечення продуктивності у віддаленому режимі. Автори здійснили узагальнення й синтез наявних знань про різні аспекти кібербезпеки при застосуванні дистанційної праці. Були Сформульовані висновки та виявлені тенденції можуть стати основою для розробки практичних рекомендацій бізнесу та подальших досліджень у даній галузі, спрямованих на підвищення рівня кіберстійкості організацій в умовах глобальної цифровізації та поширення гнучких форматів роботи.

Перелік посилань

1. Radha P., Sayyed N., Fathima Y. The new normal: navigating cyber security challenges in remote work policies. NPRC journal of multidisciplinary research. 2024. Vol. 1, no. 8. P. 106–118. URL: https://doi.org/10.3126/nprcjmr.v1i8.73042 (date of access: 30.04.2025).

2. Office I. L., Messenger J. C. Telework in the 21st century: an evolutionary perspective. International Labour Organisation (ILO), 2019.

3. Sabin J. The future of security in a remote-work environment. Network security. 2021. Vol. 2021, no. 10. P. 15–17. URL: https://doi.org/10.1016/s1353-4858(21)00118-5 (date of access: 30.04.2025).

4. Rhodes C., Bettany A. Automating windows deployment with zero touch. Windows installation and update troubleshooting. Berkeley, CA, 2016. P. 119–137. URL: https://doi.org/10.1007/978-1-4842-1827-3_5 (date of access: 30.04.2025).

5. AlShalaan M. R., Fati S. M. Enhancing organizational data security on employee-connected devices using BYOD policy. Information. 2023. Vol. 14, no. 5. P. 275. URL: https://doi.org/10.3390/info14050275 (date of access: 30.04.2025).

6. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

7. Jarrahi M. H., Reynolds R., Eshraghi A. Personal knowledge management and enactment of personal knowledge infrastructures as shadow IT. Information and learning sciences. 2020. Ahead-of-print, ahead-of-print. URL: https://doi.org/10.1108/ils-11-2019-0120 (date of access: 08.05.2025).

8. Bonderud D. Cost of a data breach 2024: Financial industry | IBM. IBM - United States. URL: https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry (date of access: 07.05.2025).

9. Public Company Accounting Reform and Investor Protection Act of 2002, 15 U.S.C. § 7201 et seq. (2002). https://www.govinfo.gov/content/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf.

10. Nwankpa J. K., Datta P. M. Remote vigilance: the roles of cyber awareness and cybersecurity policies among remote workers. Computers & security. 2023. P. 103266. URL: https://doi.org/10.1016/j.cose.2023.103266 (date of access: 30.04.2025).

11. Das S., Dingman A., Camp L. Why Johnny doesn't use two factor: A two-phase usability study of the FIDO U2F security key. 2018. P. 160–179. URL: https://doi.org/10.1007/978-3-662-58387-6_9.

12. Repetto M. Adaptive monitoring, detection, and response for agile digital service chains. Computers & Security. 2023. Vol. 132. P. 103343. URL: https://doi.org/10.1016/j.cose.2023.103343 (date of access: 08.05.2025).

13. Haag S., Eckhardt A., Schwarz A. The Acceptance of Justifications among Shadow IT Users and Nonusers – An Empirical Analysis. Information & Management. 2019. Vol. 56, no. 5. P. 731–741. URL: https://doi.org/10.1016/j.im.2018.11.006 (date of access: 08.05.2025).

© Вербиненко В.О., Зибін С.В. (2025). Проблеми кібербезпеки в організаціях з дистанційною формою праці. Сучасний захист інформації, 2(62), 22–30.
https://doi.org/10.31673/2409-7292.2025.020383

14. Waelchli S., Walter Y. Reducing the risk of social engineering attacks using SOAR measures in a real world environment: A case study. Computers & Security. 2024. P. 104137. URL: https://doi.org/10.1016/j.cose.2024.104137 (date of access: 09.05.2025).

15. Ratchford M., Wang P., Sbeit R. O. BYOD Security Risks and Mitigations. Advances in Intelligent Systems and Computing. Cham, 2017. P. 193–197. URL: https://doi.org/10.1007/978-3-319-54978-1_27 (date of access: 09.05.2025).

16. Lim Y. Z., Rahman H. B. A., Sikdar B. False sense of security on protected wi-fi networks. Cryptography and security. URL: https://arxiv.org/abs/2501.13363.

17. Al Jutail M., Al-Akhras M., Albesher A. Associated risks in mobile applications permissions. Journal of Information Security. 2019. Vol. 10, no. 02. P. 69–90. URL: https://doi.org/10.4236/jis.2019.102004 (date of access: 09.05.2025).

18. Outdated software | OWASP foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/www-project-top-10-infrastructure-security-risks/docs/2024/ISR01_2024-Outdated_Software (date of access: 09.05.2025).

19. Adascalitei D., Riso S. Effects of employee monitoring on remote work. An empirical study from Germany and Spain using AMPWork survey data (2021-2022). Sinappsi. 2024. Vol. XIV. P. 93–112.

20. Bring your own device (BYOD): organizational control and justice perspectives / H. Lam et al. Employee Responsibilities and Rights Journal. 2024. URL: https://doi.org/10.1007/s10672-024-09498-1 (date of access: 09.05.2025).

21. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

22. J. G. Balancing employee privacy and cyber security in remote work: ethical and legal challenges. URL: https://www.researchgate.net/publication/389711296_BALANCING_EMPLOYEE_PRIVACY_AND_CYBER_SECURITY_IN_REMOTE_WORK_ETHICAL_AND_LEGAL_CHALLENGES.

23. Swire P., Kennedy-Mayo D. The risks to cybersecurity from data localization – organizational effects. Arizona law journal of emerging technologies. 2025. Vol. 8, no. 1. URL: https://doi.org/10.2458/azlawjet.7523 (date of access: 09.05.2025).

24. Golubock D. Remote workers, ever-present risk: employer liability for data breaches in the era of hybrid workplaces. Journal of law, technology, & the internet. 2024. Vol. 15, no. 2. URL: https://scholarlycommons.law.case.edu/jolti/vol15/iss2/4 (date of access: 09.05.2025).

25. Nwosu O. Monitoring productivity vis-a-vis employee privacy: legal and ethical considerations: thesis. 2022. 32 p. URL: https://doi.org/10.2139/ssrn.4095627 (date of access: 09.05.2025).

26. Simutina Y. Remote work in Ukraine: problems and prospects of improving its legal regulation. Yearly journal of scientific articles “Pravova derzhava”. 2023. No. 34. P. 431–444. URL: https://doi.org/10.33663/1563-3349-2023-34-431-444 (date of access: 09.05.2025).

Надійшла 07.04.2025