АНОТАЦІЯ

Відповідно до мети дослідження робота присвячена аналізу Bring Your Own Device (BYOD), політики, що дозволяє працівникам використовувати свої особисті пристрої для робочих цілей. BYOD може запропонувати низку переваг для бізнесу, зокрема: підвищення продуктивності – працівники можуть бути більш продуктивними, коли вони можуть використовувати свої власні пристрої, з якими вони вже знайомі і якими їм комфортно користуватися; підвищення задоволеності працівників – працівники з більшою ймовірністю будуть задоволені своєю роботою, якщо їм дозволять користуватися власними пристроями. Однак, BYOD також несе в собі певні ризики, зокрема: безпека даних – пристрої BYOD частіше губляться або викрадаються, ніж корпоративні пристрої, що може призвести до витоку даних; зараження шкідливим програмним забезпеченням – пристрої BYOD з більшою ймовірністю можуть бути заражені шкідливим програмним додатками.

ABSTRACT

In line with the research objectives, the work is dedicated to the analysis of Bring Your Own Device (BYOD) policies, allowing employees to use their personal devices for work purposes. BYOD can offer several advantages for businesses, including increased productivity – employees can be more productive when they use their own devices, with which they are already familiar and comfortable; and enhanced employee satisfaction – employees are more likely to be satisfied with their work if they are allowed to use their own devices. However, BYOD also carries certain risks, including data security – BYOD devices are more prone to loss or theft, which may lead to data leaks; and susceptibility to malware infection – BYOD devices are more likely to be infected with malicious software.