**ПРИКЛАД ОФОРМЛЕННЯ**

*Шулімова Дар’я Денисівна*

*студентка групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна*

**ОСНОВНІ РИЗИКИ БЕЗПЕКИ МОБІЛЬНИХ ПРИСТРОЇВ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ**

Смартфони все частіше використовуються для роботи. За їх допомогою користувачі передають бізнес-інформацію через незахищені канали зв'язку. Все більше співробітників переглядають декілька поштових скриньок (організації та власних) з одного слабозахищеного мобільного пристрою. У зв'язку з цим все більше кіберзлочинців переходять на онлайн-шахрайство, включаючи вимагання та шантаж. Отримавши навіть віддалений (а не прямий, за допомогою крадіжки) доступ до мобільного пристрою, зловмисник зможе дізнатися не тільки особисті, а й банківські або корпоративні доступи. Крім цього, існують інші загрози для мобільних пристроїв, здатні відкрити хакерам доступ до смартфону.

Як зловмисники змушують користувачів переходити по зараженому посиланню.

Для атак зловмисники використовують фішинг та методи соціальної інженерії, які змушують співробітників натискати на заражені посилання. Їх надсилають електронною поштою або у повідомленнях месенджерів.



Рис.1. Цілі, за якими зловмисники здійснюють атаки

 Перелік посилань:

1. Смартфони та корпоративна інформація: основні ризики та як їм запобігти URL: <https://softline.ua/ua/news/smartfony-ta-korporatyvna-informatsiia-osnovni-ryzyky-ta-iak-im-zapobihty.html> (дата звернення: 26.09.2023).
2. MOBILE SECURITY URL: <https://www.digitalsecurity.film/mobile> (дата звернення: 02.10.2023).