УДК 338.95

Куцик П.О.
kutsykpetro@gmail.com, ORCID ID: 0000-0001-5795-9704
д.е.н., проф., ректор Львівського торговельно-економічного університету, м. Львів

Туліка Н.М.
nazariitulika@gmail.com, ORCID ID: 0009-0007-9339-8220
здобувач, Львівський торговельно-економічний університет, м. Львів

ВИКОРИСТАННЯ РОСІЙСЬКОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА КІБЕРВИКЛИКИ: ВПЛИВ НА ЕКОНОМІКУ УКРАЇНИ ТА ПЕРСПЕКТИВИ ДЛЯ ВІТЧИЗНЯНОЇ ІТ-ГАЛУЗІ

Анотація. *У сучасних умовах ведення війни в кіберпросторі набуває не меншого значення, ніж бойові дії на фізичному полі бою. У статті проведено ґрунтовний аналіз проблеми використання російського програмного забезпечення (ПЗ) в Україні в умовах збройного конфлікту, економічних санкцій та посилення глобальних кіберзагроз. Досліджено масштаби проникнення російських цифрових рішень у державний та приватний сектори економіки України, а також наслідки їхнього використання для національної безпеки та фінансової стабільності. Розглянуто основні економічні втрати від експлуатації російського ПЗ, зокрема пряме фінансування економіки країни-агресора, ризики витоку конфіденційної інформації, репутаційні збитки для компаній, а також перешкоди для міжнародного співробітництва у сфері інформаційних технологій. Особливу увагу приділено аналізу кіберзагроз, що виникають унаслідок використання російських програмних рішень, включаючи конкретні випадки масштабних кібератак на державні установи та великі корпорації. Досліджено проблему вендорлоку, що перешкоджає переходу на альтернативні програмні продукти, а також ключові бар'єри, які ускладнюють імпортозаміщення в сфері ПЗ. Запропоновано комплекс заходів для вирішення проблеми: посилення державного регулювання, запровадження законодавчих обмежень, стимулювання розробки українських цифрових продуктів, створення програм підтримки бізнесу для переходу на безпечні альтернативи, підвищення рівня кіберстійкості інфраструктури та розширення міжнародної співпраці у сфері цифрової безпеки. Результати дослідження підтверджують, що повна відмова від російського ПЗ є необхідною умовою для забезпечення кібербезпеки, економічної незалежності та розвитку національної ІТ-індустрії. Використання власних або міжнародно сертифікованих програмних рішень сприятиме посиленню цифрового суверенітету України, зниженню ризиків інформаційного саботажу та втрати даних, а також стимулюватиме розвиток інноваційного середовища у сфері інформаційних технологій.*

Ключові слова: російське програмне забезпечення, кібербезпека, кібератаки, національна безпека, цифровий суверенітет, вендорлок, імпортозаміщення, економічні втрати, санкції, державне регулювання, ІТ-індустрія України, фінансова стабільність, репутаційні ризики, міжнародна співпраця, цифрова незалежність, технологічний розвиток, інформаційний захист.

Kutsyk Petro
kutsykpetro@gmail.com, ORCID ID: 0000-0001-5795-9704
Doctor of Economics, Professor, Rector, Lviv University of Trade and Economics, Lviv

Tulika Nazarii
nazariitulika@gmail.com, ORCID ID: 0009-0007-9339-8220
Postgraduate, Lviv University of Trade and Economics, Lviv

THE USE OF RUSSIAN SOFTWARE AND CYBER CHALLENGES: IMPACT ON UKRAINE'S ECONOMY AND PROSPECTS FOR THE DOMESTIC IT SECTOR

Abstract. *In modern conditions, waging war in cyberspace is becoming no less important than combat operations on the physical battlefield. This article provides a comprehensive analysis of the problem of using Russian software in Ukraine in the context of armed conflict, economic sanctions, and escalating global cyber threats. The study examines the scale of penetration of Russian digital solutions into Ukraine's public and private sectors, as well as the consequences of their use for national security and financial stability. The key economic losses associated with the exploitation of Russian software are analyzed, including direct financing of the aggressor state's economy, risks of confidential data leaks, reputational damage for companies, and obstacles to international cooperation in the field of information technology. Particular attention is paid to the analysis of cyber threats arising from the use of Russian software solutions, including specific cases of large-scale cyberattacks on government institutions and major corporations. The problem of vendor lock-in, which hinders the transition to alternative software products, is explored, along with the main barriers that complicate import substitution in the software sector. A comprehensive set of measures is proposed to address this issue, including strengthening state regulations, introducing legislative restrictions, promoting the development of Ukrainian digital products, creating support programs for businesses transitioning to secure alternatives, enhancing the cybersecurity resilience of infrastructure, and expanding international cooperation in the field of digital security. The study's findings confirm that the complete abandonment of Russian software is a necessary condition for ensuring cybersecurity, economic independence, and the development of Ukraine's IT industry. The adoption of domestically developed or internationally certified software solutions will contribute to strengthening Ukraine's digital sovereignty, reducing risks of information sabotage and data loss, and fostering the development of an innovative environment in the field of information technologies.*

Keywords: Russian software, cybersecurity, cyberattacks, national security, digital sovereignty, vendor lock-in, import substitution, economic losses, sanctions, state regulation, Ukraine's IT industry, financial stability, reputational risks, international cooperation, digital independence, technological development, information protection.

JEL Classification: M20
DOI: https://doi.org/10.32782/2522-1256-2025-44-14

Постановка проблеми. У сучасних умовах ведення війни в кіберпросторі набуває не меншого значення, ніж бойові дії на фізичному полі бою. Використання російського програмного забезпечення (ПЗ) на території України створює критичні ризики для національної безпеки, економіки та цифрового суверенітету держави. Попри санкції, введені з 2017 року, та рекомендації щодо відмови від ПЗ країни-агресора, велика кількість державних установ і приватних підприємств продовжує експлуатувати російські програмні рішення, що ставить під загрозу кіберстійкість країни. Основні загрози, що виникають унаслідок використання російського ПЗ, включають наступне:

• Кібершпигунство та саботаж – можливість отримання доступу до конфіденційної інформації українських державних і бізнесових структур через закладені уразливості або

приховані бекдори в російських програмах.

• Економічні втрати – фінансова підтримка російської ІТ-індустрії та, відповідно, державного бюджету країни-агресора, що прямо або опосередковано сприяє фінансуванню військових дій.

• Критична залежність від російських рішень – складнощі у заміні російського ПЗ через відсутність структурованої державної політики щодо імпортозаміщення, проблеми вендорлоку (ситуацію, коли постачальник послуг монополізував підтримку системи і зробив її залежною від себе) та низьку обізнаність користувачів про альтернативи.

• Ризики міжнародної співпраці – використання російських цифрових продуктів може стати перешкодою для міжнародного співробітництва України, оскільки багато західних компаній та урядів дотримуються санкційної політики щодо російського ПЗ.

Таким чином, постає нагальна необхідність комплексного аналізу ситуації з використанням російських програмних продуктів, визначення масштабів загроз, а також формування ефективних механізмів імпортозаміщення та посилення кібербезпеки в Україні.

Аналіз останніх досліджень та публікацій. Проблема використання російського ПЗ та пов'язаних із цим ризиків активно досліджується як міжнародними, так і українськими експертами у сфері кібербезпеки, економіки та державного управління.

У працях західних дослідників (Wolff, 2021; Brookings Institute, 2023) розглядаються загрози, пов'язані з використанням російських цифрових рішень у контексті глобальної кібербезпеки. Зокрема, доведено, що такі програми, як антивіруси "Kaspersky Lab", можуть бути інструментами для кібершпигунства та ведення прихованих атак. У 2024 році уряд США повністю заборонив продаж цього програмного забезпечення через його потенційну загрозу національній безпеці.

В українському контексті проблема досліджувалася у звітах Львівського ІТ Кластера (2024), Асоціації ІТ Ukraine (2023–2024), Transparency International Ukraine (2024). У цих матеріалах наголошується на масштабах використання російського ПЗ серед українських підприємств, проблемах заміщення та економічних втратах, спричинених залежністю від рішень країни-агресора.

Зокрема, дослідження CFO Club Ukraine (2024) виявило, що понад 75% українських компаній продовжують використовувати 1С та його модифікації, незважаючи на заборони. Також було зазначено, що близько 1,160 млрд грн було витрачено державними підприємствами України на закупівлю російських програмних рішень навіть після початку повномасштабної війни.

Аналіз останніх публікацій також свідчить про зростання загроз у сфері кібербезпеки. У звіті Ради національної безпеки і оборони України (2024) зафіксовано понад 10 000 кібератак на державні ресурси України лише у 2023 році. Частина з них була здійснена через уразливості в ПЗ, що мало російське походження.

Проте, незважаючи на широкий спектр досліджень, залишається недостатньо опрацьованою тема конкретних механізмів імпортозаміщення російських цифрових продуктів та оцінки економічного ефекту від їхнього повного витіснення з ринку України. Саме ці аспекти є ключовими для подальшого дослідження.

Постановка завдання. З огляду на актуальність проблеми та результати попередніх досліджень основна мета статті – визначення масштабів загроз, що виникають унаслідок використання російського ПЗ в Україні, аналіз економічних втрат та вироблення стратегічних підходів до імпортозаміщення російських цифрових рішень. Для досягнення цієї мети поставлено такі завдання:

• Оцінити масштаби використання російського програмного забезпечення в Україні, зокрема у державному секторі та серед комерційних підприємств.

• Проаналізувати кіберзагрози, що виникають через використання російських цифрових продуктів, на основі реальних кейсів кібератак на державні та приватні компанії.

• Визначити економічні втрати України від експлуатації російського ПЗ, включаючи втрачений потенціал для українських ІТ-компаній.

• Проаналізувати проблеми переходу на безпечні альтернативи, зокрема бар'єри вендорлоку, брак фінансування та низьку обізнаність користувачів.

• Визначити перспективи для вітчизняної ІТ-галузі у контексті повної заборони та витіснення російських програмних продуктів.

• Сформувати рекомендації щодо поступового витіснення російського ПЗ з ринку України, включаючи пропозиції щодо державного

регулювання, стимулювання розробки вітчизняних альтернатив та міжнародного співробітництва у сфері кібербезпеки.

Результати дослідження дозволять оцінити реальний вплив російського ПЗ на економіку та кібербезпеку України, а також визначити ефективні механізми для його повного усунення та розвитку вітчизняних цифрових рішень.

Виклад основного матеріалу дослідження. Сучасна цифрова епоха та гібридна війна роблять кібербезпеку критичним чинником національної безпеки й економічної стабільності [10; 11]. Попри багаторічну військову агресію росії, в Україні досі масово використовується програмне забезпечення (ПЗ) російського походження. У листопаді 2024 року Комітет Верховної Ради з питань нацбезпеки навіть створив робочу групу для доопрацювання законопроєктів щодо повної заборони ПЗ країни-агресора. Асоціація IT Ukraine запустила проєкт «Ворожий софт» (2023), метою якого є вилучення з обігу всіх російських програмних продуктів [1].

Світова тенденція також чітко демонструє відмову від російського ПЗ через потенційні загрози. Ще у 2017 році США заборонили використання продуктів "Kaspersky" у федеральних установах, а уряд Німеччини у 2022 р. рекомендував відмовитися від цього антивірусу через ризики шпигунства. У 2024 році американська влада пішла далі, запровадивши повну заборону на продаж ПЗ "Kaspersky" в країні. Європейські країни також поступово позбавляються залежності від російських IT-рішень, особливо в державному секторі та критичній інфраструктурі [2]. Міжнародні кіберінциденти також підтверджують небезпеку: наприклад, атака вірусу NotPetya у 2017 році, пов'язана з російськими хакерами, спричинила глобальні збитки на рівні $10 млрд [3]. Таким чином, питання кібервикликів та відмови від ворожого ПЗ є вкрай актуальним для захисту як держави, так і бізнесу, зростає актуальність аналізу впливу використання російського програмного забезпечення на економіку України та визначення перспектив для вітчизняної IT-сфери в умовах цих викликів.

Масштаби використання російського ПЗ в Україні. Історично склалося, що український ринок корпоративного софту був тісно пов'язаний із російськими продуктами. Російське програмне забезпечення залишається поширеним як у державному, так і в приватному секторі України. За даними дослідження CFO Club Ukraine на замовлення USAID, близько 75% українських компаній продовжують користуватися російською системою 1С [1]. Йдеться про понад 500 тисяч підприємств малого, середнього і великого бізнесу. Попри те, що у 2017 році рішенням РНБО було запроваджено санкції проти 1С і заборонено його продаж в Україні, фактичне використання цієї платформи не припинилося [4]. Ба більше, російський софт проникає під виглядом «клонів»: після санкцій з'явилися продукти на кшталт BAS, BAF, «UA-Бюджет», «Комплексні бюджетні системи» тощо, формально перереєстровані в Європі, але по суті побудовані на ядрі 1С. Деякі користувачі помилково вважають такі продукти іноземними чи українськими, але фактично це те саме російське ПЗ. Одним із прикладів маскування є популярний конструктор сайтів Tilda, який широко використовується українським малим бізнесом; ця платформа має російське походження і сервери в РФ. Усього експерти "IT Ukraine" ідентифікували понад 100 програмних продуктів російського походження, що й досі перебувають в обігу в Україні [1]. Така залежність несе подвійний негативний ефект: з одного боку, кошти за ліцензії фактично фінансують економіку агресора, з іншого, – існує пряма загроза несанкціонованого доступу до чутливих даних. Держслужба спецзв'язку наголошує, що, використовуючи російське ПЗ, українські організації фактично надають спецслужбам РФ доступ до своїх інформаційних ресурсів.

Економічні втрати від використання російського ПЗ. Одним із суттєвих наслідків використання російського ПЗ є фінансова підтримка економіки країни-агресора за рахунок українських коштів. За даними проєкту «Ворожий софт», лише державні підприємства України з 2017 року витратили на закупівлю російського програмного забезпечення щонайменше 1,160 млрд грн (приблизно $43 млн). Ця цифра постійно зростає: у 2024 році через систему публічних закупівель Prozorro було зафіксовано витрати близько 200 млн грн на російські програмні продукти [1]. Враховуючи, що ці дані охоплюють лише державний сектор, реальні обсяги фінансових потоків у приватному бізнесі є значно більшими – експерти оцінюють, що вони можуть бути в десятки разів вищими.

Таким чином, українська економіка зазнає непрямих втрат, оскільки значні кошти замість

підтримки вітчизняних розробників спрямовуються російським компаніям. Фактично ці гроші стають внеском у бюджети та податки РФ, фінансують російських співробітників, а отже – опосередковано підтримують військову машину противника.

Окрім прямих фінансових втрат, існують також втрати можливостей. Гроші, витрачені на іноземний (російський) продукт, могли б залишитися в національній економіці. Використання українських або західних програмних рішень означало б, що ці кошти працюють на економіку України: створюють робочі місця для ІТ-фахівців, наповнюють бюджет податковими надходженнями, стимулюють розвиток локальних компаній. За оцінками експертів, перенаправлення попиту на безпечні українські аналоги має мультиплікативний ефект: по-перше, це підсилює національну ІТ-екосистему, а по-друге, – чіткий сигнал про звільнення частки ринку стимулює інвесторів вкладати в українські проєкти [1]. Іншими словами, витіснення російського ПЗ створює ніші для нових українських продуктів і залучає додаткові інвестиції в галузь.

Наслідком продовження статус-кво є також потенційні втрати від кібератак, спричинених наявністю уразливого російського ПЗ. Масштабні кібератаки можуть мати відчутний економічний ефект. По-перше, зростають прямі витрати бізнесу на ліквідацію наслідків кіберінцидентів. 2023 року кількість зареєстрованих кібератак в Україні зросла на 62,5%, і компанії, що використовують ПЗ російського походження (наприклад, системи «1С» чи BAS), можуть бути більш вразливими до таких атак. Кожен серйозний інцидент може зупинити бізнес-процеси: простій виробництва чи сервісу означає втрачений прибуток, штрафи за невиконання контрактів і втрату клієнтів, які уникають співпраці з скомпрометованими фірмами [5]. По-друге, приховані втрати мають довгостроковий характер. За оцінками експертів, подальша експлуатація російських облікових систем і іншого ПЗ може спричинити збитки, що значно перевищують інвестиції, необхідні для переходу на західні чи українські аналоги. Іншими словами, витрати на впровадження безпечного програмного забезпечення менші, ніж потенційні збитки від кіберінцидентів та простоїв [5]. По-третє, невідповідність російського софту міжнародним стандартам накладає додаткові обмеження. Зокрема, багато продуктів із РФ не відповідають вимогам GDPR та інших регуляцій ЄС, що ускладнює роботу українських експортерів на європейському ринку. Компанії, які не замінять такі системи, можуть отримати штрафи та втратити контракти в ЄС [5]. Це прямо впливає на експортну виручку і репутацію українського бізнесу.

Репутаційні ризики теж вагомі. Україна закликає міжнародних партнерів бойкотувати російські товари і запроваджувати санкції, але водночас всередині країни продовжує використовуватися програмне забезпечення агресора [1]. Така невідповідність підриває позицію України на міжнародній арені. Оприлюднення фактів використання проросійського ПЗ негативно впливає на довіру клієнтів і партнерів, ставлячи під сумнів кібергігієну та відповідальність компанії. У підсумку підприємство може втратити ринки збуту і вимушене витрачати ресурси на відновлення ділової репутації.

Санкційна політика. Порівняння з міжнародною санкційною політикою демонструє, що Україна рухається в руслі світових тенденцій, хоча і з певним запізненням. У нашій країні санкційна політика щодо російського ПЗ активно формується після 2014 року. Рішенням РНБО у 2017 р. було заборонено використання програмних продуктів агресора в органах державної влади (включно зі згаданою «1С»). Проте у приватному секторі ці системи продовжували домінувати до останнього часу. Лише після початку повномасштабної війни проблема набула розголосу: у квітні 2023 р. введено нові 10-річні санкції проти ряду російських ІТ-компаній указом Президента України №227/2023 (на додаток до санкцій 2017 р.) [7]. Ці кроки наближають українську практику до підходів союзників і покликані усунути правові прогалини, що дозволяли російським продуктам залишатися на ринку (зокрема, через ребрендинг чи обходження санкцій). Важливо, що держава усвідомлює: кіберзагрози від ворожого ПЗ – це не тільки технічна проблема окремих фірм, а й фактор економічної безпеки країни.

Урядова роль у вирішенні даної проблеми є визначальною. Окрім санкцій, держава може стимулювати бізнес до імпортозаміщення в ІТ-сфері. Вже зараз створено інструменти підтримки переходу на безпечне ПЗ: зокрема, діє державний каталог “Replace Russian Software with Ukrainian Solutions”, де зібрані українські аналоги популярних російських програм. Центральні органи влади можуть

здійснювати закупівлі через ДП «УСС» – централізовану організацію, що перевіряє постачальників і походження програмних продуктів [8]. Такі заходи мінімізують ризик випадкового придбання небезпечного софту. Крім того, уряд заохочує приватні компанії відмовлятися від ворожих рішень – інформаційними кампаніями, консультаціями, а надалі, ймовірно, економічними стимулами. Важливим є і врахування досвіду міжнародних партнерів: впровадження стандартів кібербезпеки, обов'язкових аудитів ПЗ у критичних галузях, обмін інформацією про виявлені бекдори. Таким чином, синергія державної політики й усвідомленості бізнесу здатна значно скоротити кіберризики та підвищити стійкість економічного сектору.

Проблеми переходу на безпечні альтернативи. Незважаючи на очевидні ризики, багато українських компаній не поспішають відмовлятися від звичного російського софту. Існує низка причин та бар'єрів при переході на альтернативні рішення, серед яких ключові такі:

• Низька обізнаність та міфи про відсутність аналогів. Поширена упередженість: «перейти немає на що, немає рівноцінної заміни». Насправді ж майже для кожного російського продукту існує принаймні кілька альтернативних рішень – як іноземних, так і українських. Наприклад, для 1С нараховуються десятки систем-аналогів. Проте багато підприємців просто не знають про них. Додатково ситуацію ускладнює маскування російського ПЗ під європейське: як зазначалося, деякі сервіси (наприклад, Altegio для сфери послуг) зареєстровані у Польщі чи Нідерландах і неочевидно пов'язані з РФ, тому користувачі можуть навіть не здогадуватися про їх справжнє походження. Без цілеспрямованого інформування бізнесу багато хто продовжує працювати з «ворожим» ПЗ просто через незнання.

• Побоювання високих витрат на перехід. Інший міф – «це дуже дорого, нам не по кишені змінювати систему». Дійсно, великий бізнес, що роками інвестував у кастомізацію 1С під свої потреби, остерігається втратити вкладені кошти. Проте для **малого і середнього бізнесу** цей бар'єр значно нижчий: часто там використовують лише базові функції для бухгалтерії чи звітності, тож перехід на готові «коробкові» рішення може бути відносно недорогим. Як приклад, перехід із російського конструктора сайтів Tilda на українську платформу Weblium не потребує десятків тисяч доларів інвестицій. Отже, питання вартості є перебільшеним для більшості МСБ. Для великих корпорацій, безумовно, ціна міграції вища, але її слід порівнювати з потенційною шкодою від кіберінцидентів.

• **Технічна складність і інерція.** Великі компанії часто глибоко інтегрували російські продукти у свої бізнес-процеси – наприклад, ERP-система 1С може бути «серцем» обліку, до якого підключено безліч модулів, складів, фабрик тощо. У таких випадках перехід ускладнений: компанії вкладали багато не стільки в ліцензії 1С, скільки в допрацювання та налаштування систем під себе. Змінити ПЗ означає переробити цілий пласт бізнес-процесів, що лякає масштабом. Нерідко відповідальні ІТ-підрозділи чи підрядники протидіють змінам через «вендорлок» – ситуацію, коли постачальник послуг монополізував підтримку системи і зробив її залежною від себе. Така залежність стримує конкуренцію і гальмує впровадження нових технологій у державних органах і бізнесі. За оцінками, близько половини державних інформаційних систем України тією чи іншою мірою залежать від монопольних постачальників або навіть окремих людей, що їх контролюють. Це породжує організаційну інерцію: без зовнішнього стимулу системи можуть не оновлюватися роками.

• **Низький рівень кібергігієни та усвідомлення ризиків.** Багато підприємств приділяють увагу кібербезпеці лише після того, як вже стали жертвами атаки, або коли в галузі трапляються гучні випадки. На жаль, проактивна безпека поки що не є нормою. Це призводить до толерування «дірок» у системах: як відзначають експерти, компанії часто не усвідомлюють, що мають незахищений «тил» у вигляді того ж 1С, через який зловмисник при бажанні може отримати доступ до їхніх даних. Показовою є реакція бізнесу на відомі інциденти: лише після кібератак на великі підприємства (наприклад, випадки з «Київстаром» чи злами державних реєстрів) починається пожвавлення інтересу до перевірки власних систем. Отже, поки не настало розуміння, що профілактика дешевша за ліквідацію наслідків, компанії схильні відкладати перехід на безпечний софт.

Вирішення зазначених проблем потребує комплексного підходу: підвищення поінформованості (роз'яснювальна робота про наявність вітчизняних та міжнародних аналогів), економічних стимулів та підтримки для міграції, а також адміністративних важелів (від

санкцій до нормативних вимог кібербезпеки). Вже зараз профільні асоціації співпрацюють із галузевими об'єднаннями бізнесу, пропонуючи дорожні карти переходу для різних секторів та конкретні рекомендації, на яке ПЗ перейти і як. Такий проактивний підхід має поступово зменшити опір змінам та розвіяти міфи про «незамінність» російського софту.

Кіберзагрози та інциденти, пов'язані з російським ПЗ. Використання російського програмного забезпечення створює підвищені кіберризики для України. По-перше, як зазначалося, програми на кшталт 1С можуть мати приховані уразливості або бекдори, що дозволяють отримати несанкціонований доступ до систем. Сервери таких сервісів часто розміщені за межами контролю України (інколи й на території РФ), що означає відсутність гарантій безпеки для даних користувачів [4]. На тлі того, що Україна є однією з найбільш кібератакованих країн світу, подібні лазівки активно шукаються і використовуються противником. Конкретні випадки кібератак підтверджують реальність загроз. Зокрема, в грудні 2024 року було здійснено масштабну кібератаку на державні реєстри Міністерства юстиції України, яку назвали найбільшою за останній час [1]. Хакерське угруповання XakNet (асоційоване з РФ) заявило, що зламало ІТ-інфраструктуру ДП «Національні інформаційні системи» і завантажило понад 1 млрд рядків даних із реєстрів, після чого видалило їх разом із резервними копіями. У результаті була паралізована робота ключових онлайн-сервісів держави – збої торкнулися сервісів «Дія» (перереєстрація авто, витяги ЄДР тощо) та інших електронних послуг. За даними експертів, однією з причин успішності цієї атаки могла стати наявність «вразливого місця» у вигляді російського ПЗ на кшталт 1С, яке використовувалося в інфраструктурі реєстрів. Чимало деталей такого інциденту не розкриваються публічно, однак факт залишається фактом: російські програми дійсно стають каналом для атак. В Асоціації ІТ Ukraine підтверджують, що їм відомо про кібердари, які здійснюються саме через уразливості 1С. Тобто, залишаючи «дірку» у вигляді ворожого софту, організації наражаються на пряму небезпеку.

Кіберзлочинці атакують не лише державні, а й приватні структури. Показовим прикладом є атака на найбільшого телеком-оператора «Київстар» у грудні 2023 року. Група російських хакерів (ймовірно Sandworm, пов'язана з ГРУ РФ) протягом кількох місяців приховано перебувала в мережах компанії, а 12 грудня 2023 року здійснила руйнівну атаку, фактично знищивши ядро ІТ-інфраструктури оператора. Були стерті тисячі віртуальних серверів і комп'ютерів, через що 24 мільйони абонентів втратили зв'язок та сервіси на кілька днів [9]. Ця атака показала, що навіть приватний бізнес із високими інвестиціями в захист залишається вразливим. Хоч «Київстар» і не використовував, за наявною інформацією, російського ПЗ, сам факт такої атаки привернув увагу багатьох компаній до питання кіберстійкості та стану їхніх систем. Після цих подій питання безпеки даних і ризиків використання стороннього (особливо російського) софту стало більш актуальним для широкого кола підприємств.

Ще один різновид загроз – корупційні ризики та саботаж через «вендорлок». Монополізація підтримки державних систем окремими підрядниками призводить до застою технологій і нехтування безпекою. Наприклад, в одному з кейсів Пенсійного фонду виявилося, що єдиний ІТ-підрядник отримав понад 400 млн грн за 4 роки без тендерів – ці кошти витрачено лише на підтримку застарілих реєстрів [1]. Відсутність конкуренції та контролю означає, що системи роками не оновлювалися і могли містити невиправлені вразливості. У такому середовищі будь-який впроваджений елемент російського ПЗ або навіть просто стара версія програмного забезпечення стає слабкою ланкою, яку зловмисник може використати. Таким чином, російський софт у поєднанні з монопольним становищем підрядників створює подвійний ризик: імовірність прихованих «бекдорів» з боку розробника і відсутність належних оновлень чи аудиту з боку замовника. Це підриває кібербезпеку критичних систем держави.

Перспективи для вітчизняної ІТ-сфери. Водночас вирішення проблеми «ворожого» ПЗ відкриває значні перспективи для української ІТ-галузі. Повна заборона та витіснення російських програмних продуктів створить вакуум на ринку, який мають заповнити альтернативні рішення. Україна має досить розвинений ІТ-сектор, щоб запропонувати власні якісні продукти практично в усіх сегментах. Експерти наголошують, що альтернатива є фактично на все: було б дивно, якби в країні з сильною ІТ-галуззю не знайшлося вітчизняних аналогів для програм із бізнес-управ-

ління чи бухгалтерії. Вже зараз для кожної популярної російської програми можна нарахувати кілька (а для 1С – десятки) альтернатив [1]. Це добрий фундамент для імпортозаміщення у сфері софту. Очікуваний ефект від заміщення російського ПЗ на українське багатоаспектний:

• Економічне зростання та інновації. Вітчизняні ІТ-компанії отримають новий стимул для розвитку, адже звільняється значна частка ринку, раніше зайнята російськими продуктами. Збільшення попиту на українські рішення буде сигналом для інвесторів, що заохотить притік капіталу в галузь. Це може привести до появи нових стартапів, продуктів і технологій. Має запрацювати здорова ринкова конкуренція, яка спонукатиме постійне вдосконалення рішень. Як зауважують аналітики, технології не стоять на місці – звільнення ніші стимулюватиме появу нових гравців, застосування сучасних підходів (хмарні сервіси, штучний інтелект, оптимізація процесів тощо) та здешевлення продуктів.

• Створення робочих місць і розвиток експертизи. Перехід на українське ПЗ означає, що замість оплати ліцензій та послуг російських компаній кошти будуть спрямовані українським фахівцям. Це допоможе утримати таланти всередині країни, збільшити кількість ІТ-робочих місць і розширити експертизу у певних доменних напрямках (наприклад, у розробці ERP/облікового софту, систем електронного документообігу тощо). В довгостроковій перспективі накопичення знань і досвіду у цих сферах може посилити конкурентоспроможність українських продуктів на глобальному ринку.

• Підвищення кіберстійкості. Використання власного або перевіреного західного ПЗ з прозорим кодом та підтримкою знижує ризики прихованих вразливостей і залежності від недобросовісних постачальників. Українські компанії, розуміючи контекст, більш схильні враховувати вимоги кібербезпеки та рекомендації державних органів (Держспецзв'язку, РНБО) при розробці рішень. Крім того, зниження рівня «вендорлоку» через появу альтернативних постачальників підвищить гнучкість та безпеку систем: замовник зможе у разі потреби змінити підрядника, код чи технологію, що стимулює всіх гравців дотримуватися стандартів безпеки. Тобто імпортозаміщення ПЗ і розвиток конкуренції напряму сприятимуть більшій стійкості до кібератак.

• Політична та інформаційна вигода. Україна зможе демонструвати послідовність у своїй політиці: закликаючи світ відмовитися від російського, вона й сама не буде залежна від нього. Це підсилить позиції у перемовинах щодо санкцій та цифрової безпеки. До того ж, успішний кейс швидкого й ефективного заміщення ПЗ стане позитивним сигналом для суспільства і партнерів, показавши здатність країни до технологічної незалежності навіть під час війни.

Рекомендації. Для зниження ризиків слід реалізувати комплекс заходів. Першочергово – повна відмова від російського ПЗ у державних органах та на підприємствах критичної інфраструктури, з жорстким контролем виконання. В приватному секторі варто запровадити перехідні програми: компаніям необхідно дати чіткі рекомендації і часові рамки для міграції на безпечні рішення. Багато українських фірм уже успішно перейшли на західні ERP-системи (Microsoft Dynamics 365, SAP тощо) або вітчизняні аналоги. Хоча така міграція потребує інвестицій, вона розглядається як стратегічна – вкладення окуповується за рахунок зменшення кіберризиків та підвищення ефективності управління. Для нових впроваджень слід одразу обирати безпечні, сучасні та гнучкі платформи замість застарілого російського софту.

Другий напрям – політика імпортозаміщення і підтримка українських ІТ-компаній. Держава може стимулювати розробку вітчизняних програмних продуктів, які замінять російські. Йдеться про гранти, пільгове кредитування або податкові канікули для розробників стратегічного ПЗ (ERP, бухгалтерія, антивіруси, ОС тощо). Важливо налагодити співпрацю між бізнесом та місцевими розробниками: великі корпорації можуть стати першими клієнтами українських рішень, надавши їм необхідний поштовх. Наприклад, у 2023 році спостерігався сплеск попиту на українські ERP-системи для рітейлу після відмови від «1С», і великий рітейл перейшов на продукти вітчизняного виробництва. Альтернативи існують практично для всіх категорій софту, і їхній список постійно розширюється.

Третя складова – підвищення рівня кіберстійкості інфраструктури. Перенесення критичних даних до захищених хмарних сервісів глобальних провайдерів мінімізує ризики фізичного знищення серверів та передових кібератак. Одночасно слід впроваджувати регулярний моніторинг та аудит безпеки: компанії повинні перевіряти наявність сторонніх або підозрілих

програм у своїх системах. Рекомендовано використовувати відкритий код або міжнародно сертифіковані продукти там, де це можливо, аби забезпечити прозорість і перевіреність ПЗ.

Не менш важливі освіта та тренінги – підвищення обізнаності керівників і ІТ-персоналу щодо кіберзагроз, пов'язаних із використанням сумнівного програмного забезпечення. Кадровий потенціал необхідно посилювати фахівцями з кібербезпеки, які здатні впроваджувати найкращі практики захисту.

Нарешті, слід продовжувати розвивати нормативно-правову базу. Прийняття закону, що забороняє використання російського ПЗ в Україні, стане важливим кроком, який надасть чіткий сигнал бізнесу. Також варто передбачити механізми відповідальності за порушення (штрафи, відключення від мереж у разі ігнорування вимог безпеки тощо) та визначити перелік критичних галузей, де контроль має бути особливо строгим.

Висновки і перспективи подальших досліджень у даному напрямі. Використання російського програмного забезпечення в Україні несе неприйнятні ризики у воєнний час – від прямого фінансування держави-агресора до створення «воріт» для кібератак. Економічні втрати вимірюються не лише мільярдами гривень, сплаченими за ліцензії, але й потенційними збитками від паралічу ключових систем чи втрати даних. Масштаб проблеми великий: історично сформована залежність (75% підприємств на 1С) не зникне миттєво, але її подолання є вкрай важливим завданням.

Для мінімізації загроз потрібен комплекс заходів. По-перше, нормативне врегулювання і контроль – ухвалення законів про заборону російського ПЗ та механізми їх дотримання, особливо в державному секторі. По-друге, перехідний період із державною підтримкою: допомога підприємствам у міграції на безпечний софт, навчання персоналу, податкові стимули для тих, хто відмовляється від продуктів РФ. По-третє, інформаційна кампанія – розвінчання міфів про відсутність альтернатив, публічні каталоги українських і міжнародних рішень (на кшталт платформи «Ворожий софт»), обмін успішним досвідом переходу. І, безумовно, посилення кібербезпеки на всіх рівнях: аудит систем на наявність «ворожих» компонентів, оновлення застарілих програм, впровадження сучасних засобів захисту та підвищення культури кібергігієни.

Подолання залежності від російського ПЗ – це не лише питання національної безпеки, а й шанс для економічного розвитку. Українська ІТ-індустрія отримує унікальну можливість для прогресу, заповнюючи ніші, що звільняються: попит на вітчизняні програмні продукти зростає, причому не лише всередині країни, а й потенційно за кордоном. Вже нині технологічний сектор є важливою частиною економіки України, забезпечуючи близько 4,4% ВВП і понад третину експорту послуг [6]. Заміщення імпортного (російського) ПЗ локальними рішеннями посилить цю тенденцію, залишаючи кошти в національній економіці та створюючи нові робочі місця для ІТ-фахівців. Прогнозовано, що підвищення рівня кіберстійкості та цифрової незалежності позитивно вплине на інвестиційну привабливість України та її інтеграцію у світові ринки.

В умовах війни і повоєнної відбудови така цифрова незалежність стане запорукою стійкості держави та драйвером інноваційного зростання. Україна, маючи талант і експертизу, здатна перетворити нинішній кібервиклик на довгострокову перевагу, забезпечивши собі технологічний суверенітет і конкурентну ІТ-галузь.

ЛІТЕРАТУРА

1. Eleonora Burdina Чому Україна досі купує російський софт і що з цим робити. Інтерв'ю з керівницею Асоціації IT Ukraine Марією Шевчук. *DOU*. 25 лютого 2025. URL: https://dou.ua/lenta/interviews/why-ukraine-still-buys-russian-software

2. Alexandra Alper Biden bans US sales of Kaspersky software over Russia ties. *Reuters*. June 21, 2024. URL: https://www.reuters.com/technology/biden-ban-us-sales-kaspersky-software-over-ties-russia-source-says-2024-06-20

3. Wolff J. How the NotPetya attack is reshaping cyber insurance. *Brookings*. December 1, 2021. URL: https://www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance

4. Daryna Synytska During the full-scale war, Accounting programs related to Russia are still ordered in Ukraine. *Transparency International Ukraine*. May 29, 2023. URL: https://ti-ukraine.org/en/blogs/accounting-programs-related-to-russia-are-still-ordered-in-ukraine

5. Попінако Д. Економічні втрати бізнесу через використання російського ПЗ: хто платить? *SPEKA*. 25 листопада 2024. URL: https://speka.media/ekonomicni-vtrati-biznesu-cerez-vikoristannya-rosiiskogo-programnogo-zabezpecennya-xto-platit-cinu-9dng6e

6. Українська техгалузь на третій рік війни: результати IT Research Ukraine 2024. Стійкість

як нова реальність. *Lviv IT Cluster*. 27 листопада 2024. URL: https://itcluster.lviv.ua/ukrayinska-tehgaluz-na-tretij-rik-vijny-rezultaty-it-research-ukraine-2024-stijkist-yak-nova-realnist/

7. Movement to abandon Russian software getting off the ground: demand for analogs now a steady trend. *IT Ukraine Association*. 22.02.2024. URL: https://itukraine.org.ua/en/movement-to-abandon-russian-software-getting-off-the-ground-demand-for-analogs-now-a-steady-trend

8. Використання російського програмного забезпечення – величезна загроза для українських організацій усіх форм власності. *Урядовий кур'єр*. 4 липня 2023. URL: https://ukurier.gov.ua/uk/news/vikoristannya-rosijskogo-programnogo-zabezpechenny

9. Tom Balmforth Exclusive: Russian hackers were inside Ukraine telecoms giant for months. *Reuters*. January 5, 2024. URL: https://reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04

10. Куцик П., Лупак Р., Щупаківський Р., Качан О., Вірт М. Концептуальні засади узгодження галузевих структурних зрушень із потребами забезпечення конкурентоспроможності економіки в умовах цифрових трансформацій. *Фінансово-кредитна діяльність: проблеми теорії та практики*. 2024. Том 2(55). С. 346–361. DOI: https://doi.org/10.55643/fcaptp.2.55.2024.4284

11. Куцик П. О., Туліка Н. М., Процикевич А. І. Стан та перспективи розвитку IT-індустрії України. *Економіка та суспільство*. 2024. № 67. DOI: https://doi.org/10.32782/2524-0072/2024-67-108

REFERENCES

1. Eleonora Burdina Chomu Ukraina dosi kupuie rosijs'kyj soft i scho z tsym robyty. Interv'iu z kerivnytseiu Asotsiatsii IT Ukraine Mariieiu Shevchuk. *DOU*. 25 liutoho 2025, available at: https://dou.ua/lenta/interviews/why-ukraine-still-buys-russian-software

2. Alexandra Alper Biden bans US sales of Kaspersky software over Russia ties. *Reuters*. June 21, 2024, available at: https://www.reuters.com/technology/biden-ban-us-sales-kaspersky-software-over-ties-russia-source-says-2024-06-20

3. Wolff J. How the NotPetya attack is reshaping cyber insurance. *Brookings*. December 1, 2021, available at: https://www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance

4. Daryna Synytska During the full-scale war, Accounting programs related to Russia are still ordered in Ukraine. *Transparency International Ukraine*. May 29, 2023, available at: https://ti-ukraine.org/en/blogs/accounting-programs-related-to-russia-are-still-ordered-in-ukraine

5. Popinako D. Ekonomichni vtraty biznesu cherez vykorystannia rosijs'koho PZ: khto platyt'? *SPEKA*. 25 lystopada 2024, available at: https://speka.media/ekonomicni-vtrati-biznesu-cerez-vikoristannya-rosiiskogo-programnogo-zabezpecennya-xto-platit-cinu-9dng6e

6. Ukrains'ka tekhhaluz' na tretij rik vijny: rezul'taty IT Research Ukraine 2024. Stijkist' iak nova real'nist'. *Lviv IT Cluster*. 27 lystopada 2024, available at: https://itcluster.lviv.ua/ukrayinska-tehgaluz-na-tretij-rik-vijny-rezultaty-it-research-ukraine-2024-stijkist-yak-nova-realnist/

7. Movement to abandon Russian software getting off the ground: demand for analogs now a steady trend. *IT Ukraine Association*. 22.02.2024, available at: https://itukraine.org.ua/en/movement-to-abandon-russian-software-getting-off-the-ground-demand-for-analogs-now-a-steady-trend

8. Vykorystannia rosijs'koho prohramnoho zabezpechennia – velychezna zahroza dlia ukrains'kykh orhanizatsij usikh form vlasnosti. *Uriadovyj kur'ier*. 4 lypnia 2023, available at: https://ukurier.gov.ua/uk/news/vikoristannya-rosijskogo-programnogo-zabezpechenny

9. Tom Balmforth Exclusive: Russian hackers were inside Ukraine telecoms giant for months. *Reuters*. January 5, 2024, available at: https://reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04

10. Kutsyk P., Lupak R., Schupakivs'kyj R., Kachan O. and Virt M. (2024), Kontseptual'ni zasady uzghodzhennia haluzevykh strukturnykh zrushen' iz potrebamy zabezpechennia konkurentospromozhnosti ekonomiky v umovakh tsyfrovykh transformatsij. *Finansovo-kredytna diial'nist': problemy teorii ta praktyky*, Tom 2(55), s. 346-361. DOI: https://doi.org/10.55643/fcaptp.2.55.2024.4284

11. Kutsyk P. O., Tulika N. M. and Protsykevych A. I. (2024), Stan ta perspektyvy rozvytku IT-industrii Ukrainy. E*konomika ta suspil'stvo*, № 67. DOI: https://doi.org/10.32782/2524-0072/2024-67-108

Стаття надійшла до редакції
05 січня 2025 року