УДК 342.951

ШЕВЧЕНКО В.П., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/ 0000-0001-5095-1160.

ІМПОРТОЗАМІЩЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЯК ВАЖЛИВА СКЛАДОВА ПОСИЛЕННЯ КІБЕРБЕЗПЕКИ ДЕРЖАВИ

Анотація. *Досліджено загрози поширення діяльності китайської корпорації Huawei на американському та європейському цифровому ринках. Деталізовано перспективи глобального впровадження технологій нового покоління 5G. Проаналізовано законодавство окремих держав світу щодо запровадження імпортозаміщення програмного забезпечення та технологічної продукції, особливо для потреб державного сектору. Визначено загальносвітові тенденції посилення кібербезпеки за напрямом ліквідації технологічної залежності від іноземних виробників інформаційно-комунікаційних технологій. Узагальнено засади вітчизняної державної політики у сфері імпортозаміщення програмного забезпечення та технологічного розвитку. Окреслено шляхи удосконалення вітчизняного ІТ-ринку та визначено його внесок у справу забезпечення кібербезпеки.*

Ключові слова: *кібербезпека, кібератака, інформаційно-комунікаційні технології, софт, імпортозалежність, програмне забезпечення, критична інфраструктура, технології 5G, ІТ-аутсорсинг.*

Summary. *The threats of Chinese Huawei's activity in the American and European digital markets have been studied. Prospects for the global implementation of new generation 5G technologies are detailed. The legislation of some countries on the introduction of import substitution programs for software and technological products, especially for the needs of the public sector, is analyzed. Global trends in strengthening cyber security in the direction of eliminating technological dependence on foreign manufacturers of information and communication technologies have been identified. The principles of domestic state policy in the field of software import substitution and technological development are generalized. The directions of improvement of the domestic IT-market and its contribution to cyber security are outlined.*

Keywords: *cybersecurity, cyberattack, information and communication technologies, software, import dependence, software, critical infrastructure, 5G technology, IT-outsourcing.*

Аннотация. *Исследованы угрозы распространения деятельности китайской корпорации Huawei на американском и европейском цифровых рынках. Детализированы перспективы глобального внедрения технологий нового поколения 5G. Проанализировано законодательство отдельных государств мира в отношении внедрения импортозамещения программного обеспечения и технологической продукции, особенно для нужд государственного сектора. Определены общемировые тенденции усиления кибербезопасности по направлению ликвидации технологической зависимости от иностранных производителей информационно-коммуникационных технологий. Обобщены основы отечественной государственной политики в сфере импортозамещения программного обеспечения и технологического развития. Очерчены направления усовершенствования отечественного ИТ-рынка и определен его вклад в дело обеспечения кибербезопасности.*

Ключевые слова: *кибербезопасность, кибератака, информационно-коммуникационные технологии, софт, импортозамещение, программное обеспечение, критическая инфраструктура, технологии 5G, ИТ-аутсорсинг.*

Постановка проблеми. Цифрова трансформація, яка є одним із пріоритетів розвитку України, створює нові виклики у сфері кібербезпеки. Державні інформаційні ресурси та об'єкти критичної інформаційної інфраструктури, які призначені для забезпечення задоволення життєво важливих потреб громадянина, особи, суспільства і держави, є недостатньо захищеними від кібератак. На цьому фоні, останнім часом спостерігається висока технологічна залежність України від іноземних виробників продукції ІКТ та програмного забезпечення управління нею, відсутність сучасних національних стандартів щодо вимог з безпеки ланцюга поставок відповідного обладнання, розроблення програмного забезпечення та інформаційно-комунікаційних систем, систем сертифікації або оцінки відповідності з безпеки такої продукції підвищують ступінь уразливості об'єктів військової, політичної, фінансово-економічної та промислової інфраструктури держави від шкідливих і не задекларованих функцій у такому обладнанні та значно звужують вітчизняні спроможності протидії кіберзагрозам. Також значна частина підприємств, установ та організацій усіх форм власності не забезпечують надійний кіберзахист електронних інформаційних ресурсів, якими вони розпоряджаються, що призводить до порушень прав користувачів цифрових послуг та дискредитує процеси цифрової трансформації в державі.

У сучасному світі безперервно збільшується кількість кібератак, спрямованих на викрадення персональних та інших конфіденційних даних громадян та організацій із використанням методів соціальної інженерії. Зростає рівень ризику застосування фішингових атак, ботнетів, шкідливого програмного забезпечення, у тому числі програм-вимагачів, як з боку фінансово мотивованих кіберзлочинних груп, так і з боку хакерських угруповань, підконтрольних, у першу чергу, країні-агресору та іншим країнам. Збільшення інформації у базах даних та інформаційних системах та посилення відповідальності за витоки персональних даних громадян у провідних країнах створило глобальний ринок для розвитку програм-вимагачів, які вимагають кошти за розблокування доступу до інформації або нерозміщення викраденої інформації в мережі Інтернет. Усе частіше спрямовані кібератаки не здійснюються безпосередньо на уряди країн та організації. Кібератак зазнають розробники та постачальники програмних і апаратних засобів з метою зараження популярних додатків, внесення змін у вихідні коди та процеси оновлень. У подальшому це використовується для проникнення до значної кількості їх клієнтів та завдання масштабної шкоди. Популярні веб-сайти, соціальні мережі збирають велику кількість різноманітних персональних даних користувачів. Витоки інформації з баз даних, які їм належать, створюють загрозу використання цих даних з метою атаки на інші ресурси та інформаційні системи.

Зазначене провокує прискорення розробки та впровадження на державному рівні програмних документів, які б визначали умови та порядок здійснення імпортозаміщення у вітчизняній галузі ІТ-технологій. Проте основна проблема – відсутність чіткої стратегії розвитку високотехнологічних галузей на державному рівні, що визначає пріоритети держави у даній сфері. Окрім того, законодавство України також потребує вдосконалення на основі вивчення кращих світових та європейських практик у цій площині. За таких умов актуальним та доцільним є розгляд проблемних питань імпортозаміщення програмного забезпечення у сфері інформаційних технологій з метою визначення дієвих кроків, практична реалізація яких сприятиме посиленню стану кібербезпеки держави.

Результати аналізу наукових публікацій. Сучасний стан, особливості та тенденції розвитку вітчизняного ринку високих технологій досліджували у наукових працях: Р. Винничук [1], О. Журавльов [2], І. Кораблінова [3], І. Новаківський [4], М. Чайковська [5] та інші. Окремі питання правового забезпечення безпеки у кіберпросторі вивчали такі

фахівці, як: О. Баранов [6], М. Гребенюк [7], І. Доронін [8], В. Шеломенцев [9] тощо. Проте висвітлення передового іноземного досвіду та сучасних зарубіжних законодавчих практик у сфері подолання технологічної залежності від імпортної продукції ІКТ та програмного забезпечення, пошуку ефективних й оптимальних моделей уникнення імпортної залежності, особливо в умовах масштабного впровадження системи рухомого (мобільного) зв'язку п'ятого покоління – 5G, як важливої складової забезпечення кібербезпеки держави, жоден із вказаних авторів не здійснював, що посилює актуальність обраної теми цієї наукової публікації.

Метою статті є визначення заходів, які вживаються державами світу для уникнення та подолання імпортозалежності програмного забезпечення та цифрових технологій щодо посилення спроможностей у сфері кібербезпеки, особливо в умовах світової пандемії COVID-19.

Виклад основного матеріалу. Якщо раніше держави світу конкурували за право володіти природними ресурсами та землями, то в сучасному геополітичному просторі усі країни прагнуть отримати доступ та домінувати у сфері передових цифрових технологій, оскільки революційна технологічна перевага – це гарантія прориву у всіх інших сферах, від освіти до безпеки і оборони, від охорони здоров'я до запуску космічних об'єктів. На фоні глобального поширення пандемії COVID-19, світовий цифровий ринок зіткнувся із необхідністю перебудовувати технологічні та бізнес-процеси у відповідності до нових санітарних норм й стандартів. При цьому, у пріоритеті залишаються рішення, які сприятимуть швидкому, безпечному та ефективному процесу організації дистанційної роботи.

Важливим комбінованим показником, який характеризує досягнення країн світу з позиції розвитку інформаційно-комунікаційних технологій (далі – ІКТ) є "Індекс інформаційно-комунікаційних технологій" (ICT Development Index), який було запроваджено ще у 2007 році. У 2017 році перше місце у цьому рейтингу посідала Ісландія, 5-е місце Великобританія, 15-е місце Франція, 16-е США. За прогнозами експертів, до 2025 року глобальна ІТ-індустрія буде біполярною: американські та деякі європейські гіганти протистоятимуть компаніям з КНР, Південно-Східної Азії, Індії та РФ. Китай мріє про світове лідерство у сфері цифрових технологій, у зв'язку з чим активно залучає інвестиції у власне виробництво процесорів, власних операційних систем, мікрочипів, розробляє та запускає власні месенджери та є державою закритою від зовнішнього технологічного впливу. На сьогодні, одним із прикладів такого суперництва є запуск бездротових мереж формату 5G. Беззаперечно, новий стандарт не просто покращить роботу стільникового зв'язку, але й відкриває безпрецедентні можливості для розвитку Інтернету речей. Це дозволить оперативно управляти інфраструктурою, енергетикою, здійснити прорив у сфері штучного інтелекту, безпілотного транспорту та машинного навчання. Очікується, що до 2025 року кількість користувачів 5G досягне 1,2 млрд. осіб, при цьому третина з них буде знаходитися саме у Китаї. Китайська компанія "Huawei" найбільш просунулася на ринку високих технологій у цьому сегменті, виступає основним постачальником обладнання для забезпечення роботи нового стандарту навколо світу. Жодна інша компанія у світі не може продемонструвати такі колосальні успіхи. Тобто промислова політика Пекіну виводить КНР на роль світового лідера у сфері високих технологій, що провокує занепокоєння з боку інших великих держав світу (США, РФ, Великобританія).

У США політикум неодноразово повідомляв, що діяльність "Huawei" представляє суттєву загрозу усьому світу. Навіть у 2018 році президент США Д. Трамп підписав указ, яким заборонив використання урядовими відомствами продукції цієї компанії. У

подальшому адміністрація Д. Трампа неодноразово виступала за недопущення “Huawei” до запуску 5G через побоювання щодо використання цією китайською компанією у своїх продуктах бекдорів (“уразливостей”), які можуть сприяти відстеженню трафіка, який проходить по мережам. Тобто, на випадок глобальної кібервійни компанія зможе відключити своє обладнання, таким чином, заблокувавши роботу усієї критичної інфраструктури. Навіть у травні 2019 року китайська компанія “Huawei” була внесена Міністерством торгівлі США у чорний список. Американським підприємствам було заборонено здійснювати реалізацію бізнес-проектів з китайським IT-гігантом, а щоб продавати йому продукцію вимагалися особливі ліцензії. Тобто вже понад два роки компанія Huawei бойкотується в США та перебуває у “чорному списку” завдяки звинуваченням у можливій співпраці зі спецслужбами КНР. Запроваджені Вашингтоном санкції фактично спрямовані на обмеження доступу цієї компанії до напівпровідників, які є конче необхідними для виробництва телекомунікаційного обладнання та відповідного програмного забезпечення, включаючи мережі 5G. У рамках посилення інституційних спроможностей забезпечення кібербезпеки на початку 2019 року керівники трьох американських спецслужб ЦРУ, АНБ і ФБР офіційно заявили, що смартфони “Huawei” та “ZTE” можуть стежити за користувачами. У зв’язку із оприлюдненням цієї інформації, розвідувальна служба Нової Зеландії відхилила запит постачальника телекомунікацій щодо використання обладнання “Huawei” 5G, а Австралія заборонила “Huawei” постачати обладнання для платформи 5G. Обидві країни назвали підставами для таких заходів наявні загрози національній безпеці.

Проте у сучасному світі є держави, які більш-менш лояльно ставляться до імпортозаміщення у сфері телекомунікацій та цифрових технологій. Так, політична влада Франції не запровадила повної заборони на використання обладнання китайської компанії Huawei з метою розгортання мереж 5G. Наприклад, на переконання британської розвідки, існують серйозні ризики використання китайського обладнання та програмного забезпечення, особливо на військових об’єктах, атомних електростанціях та в інших стратегічних галузях, хоча британські спеціалісти здатні проконтролювати Huawei та запобігти встановленню шпигунського обладнання. Проте фінальне рішення, яке було схвалено на засіданні британської ради безпеки, надало цій китайській компанії доступ у розмірі квоти 35 % усього ринку телекомунікацій. Хоча компанію “Huawei” не допускатимуть до таких ключових об’єктів британської національної інфраструктури, а також на особливі військові та ядерні об’єкти. Будь-яке обладнання компанії має бути сумісними з розробками інших учасників проекту, такими як шведський “Ericsson” або фінський “Nokia”. У 2019 році 5G розпочав функціонувати у Великобританії, проте покриття мережі залишається досить низьким.

На переконання провідних експертів світу, техніка виробництва компанії “Huawei” нібито має “чорні двері”, які дають китайським спецслужбам доступ до зашифрованих даних пристроїв, хоча Пекін це заперечує. Таким чином, низка держав, зокрема: США, Канада, Австралія, Великобританія та Японія, наклали значні обмеження на сфери впливу компанії “Huawei” через побоювання, що використання продукції компаній зробить їхні мережі вразливими для проникнення та шпигунства ззовні. У Пекіні вбачають у такому вибірковому ставленні в ЄС до “Huawei” прояв недобросовісної конкуренції, оскільки після запровадження масштабних санкцій проти цієї китайської корпорації з боку США, багато країн Євросоюзу почали з побоюванням сприймати діяльність китайців в Європі.

Викладене дає підстави констатувати, що у 2020 році технологічний суверенітет став питанням номер один у глобальному порядку денному на фоні різкого

технологічного протистояння між США та КНР, а європейські держави вкладають €10 млрд. у розробку власної інфраструктури Хмарних технологій та програмного забезпечення. Хоча деякі держави світу активно розвивають та впроваджують політику імпортозаміщення іноземного програмного забезпечення та технологічного оснащення на вітчизняний софт, особливо для потреб державного сектору, оскільки задоволення внутрішнього попиту безальтернативно роками відбувалося виключно за рахунок імпортних поставок. При цьому, імпортозаміщення у сфері ІТ зростає переважно на фоні запроваджених регуляторних та стимулюючих заходів з боку держави.

Так, у РФ сфера інформаційних технологій вважається однією із найбільш залежних від імпорту та уразливих, оскільки відбувається масштабне користування комп'ютерами та сервісами, які вироблені виключно на імпортних компонентах, системному та прикладному програмному забезпеченні переважно іноземного походження. Уряд РФ заборонив державним органам та установам купувати зарубіжне програмне забезпечення при наявності вітчизняних аналогів. У зв'язку з цим держава-агресор планувала до кінця 2021 року в ІТ-інфраструктурі для усіх федеральних та регіональних органів влади запровадити на 80 % вітчизняне програмне забезпечення. Причинами для цього стали ініціативи уряду РФ ще у 2015 році, спрямовані на поступову заборону закупівлі зарубіжного програмного забезпечення для органів влади та адаптацію плану поступового переходу органів державного управління та державних корпорацій на вітчизняний софт. Оскільки софт розроблено компанією, яка відноситься до юрисдикції іншої країни світу, то завжди є вірогідність того, що масив даних, який проходить через відповідне програмне забезпечення можуть потенційно перейти у розпорядження "третіх осіб", що для державних компаній є неприйнятим. У грудні 2020 році була встановлена вимога у розмірі 50 % комп'ютерної техніки та програмного забезпечення вітчизняного виробництва, які мають працювати у державному секторі, а з 2023 року цей показник має зрости до 70 %.

Російське походження програмного забезпечення та софту підтверджується його включенням до Єдиного реєстру радіоелектронної продукції РФ. Очікується, що у перспективі політика, направлена на розвиток вітчизняного виробництва ІТ-продукції сприятиме нарощуванню темпів у цій площині, а державні підприємства мають придбати технологічну продукцію саме внесену до цього реєстру. Оскільки основна проблема інформатизації обумовлена низьким рівнем впровадження вітчизняних розробок програмного забезпечення, це певним чином впливає на загальний рівень цифровізації. Тому держава-агресор активно впроваджує політику імпортозаміщення інформаційних технологій на власне ПЗ як цілеспрямований системний курс з метою створення перспективних вітчизняних цифрових рішень до 2025 року. На переконання політичного керівництва РФ, перехід органів державної влади та державних компаній на вітчизняні програмні продукти відкриває нові можливості, зміцнює економіку та створює фундамент для створення цифрового майбутнього.

Розробка та впровадження засад державної політики імпортозаміщення програмного забезпечення також актуальна і для Казахстану. Метою її реалізації є стимулювання вітчизняної ІТ-галузі шляхом надання доступу до фінансових інструментів, які відповідають специфічним умовам її розвитку [10]. В сучасних умовах сфера інформаційно-комунікаційних технологій залишається однією із найбільш динамічно розвинутих галузей казахської економіки. У 2021 році заплановано внесення змін до законодавчої бази цієї країни у сфері закупівлі та розробки програм імпортозаміщення та відповідного фінансування за такими напрямками: заміна раніше придбаного зарубіжного програмного забезпечення та вітчизняне; проведення аналізу усіх програмних продуктів,

іноземного походження, що використовуються в органах державної влади та управління. Також у 2020 році було розроблено та схвалено спрощений механізм списання іноземного програмного забезпечення. На його виконання було вирішено провести аналіз усіх програмних продуктів, які використовуються в державних компаніях, та визначити детальний план поетапної їх заміни з урахуванням показників економічного ефекту. Отже, Казахстан робить поступальні кроки у напрямку зниження технологічної залежності від іноземного програмного забезпечення.

Для України питання імпортозаміщення програмного забезпечення також є одним із пріоритетних. Указом Президента України від 30 вересня 2019 року [11] з метою забезпечення національних інтересів України щодо сталого розвитку економіки, громадянського суспільства і держави визначено Цілі сталого розвитку України на період до 2030 року. Одним із пріоритетів визначено створення стійкої інфраструктури, сприяння всеохоплюючій і сталій індустріалізації та інноваціям. За таких умов, держава має поступово запроваджувати ефективні інституціональні механізми для розвитку високотехнологічних галузей, створювати сучасну інформаційно-комунікаційну інфраструктуру, стимулювати розвиток новітніх перспективних та випереджальних технологій та забезпечити суттєве зменшення імпортної залежності вітчизняного високотехнологічного сектору.

11 листопада 2020 року Уряд України ухвалив Розпорядження, яким затвердив план заходів щодо впровадження в Україні системи рухомого (мобільного) зв'язку п'ятого покоління 5G [12]. Документ встановлює перелік необхідних заходів для забезпечення впровадження в Україні системи 5G та забезпечує їх проведення. Основними функціональними особливостями мереж 5G є вдосконалений мобільний широкосмуговий доступ до Інтернету та наднадійні комунікації з низькою затримкою, на основі яких будується все різноманіття послуг і можливостей нових мереж 5G.

До таких послуг і можливостей належать: висока швидкість передачі даних, промислова автоматизація, зв'язок при надзвичайних ситуаціях тощо. Технологія 5G дозволяє використовувати мережу Інтернет, швидкість якого перевищує 4G у 10-20 разів, а в деяких випадках швидкість 5G може бути більшою навіть у 100 разів. У провідних технологічних компаніях світу – в США, Японії, Південній Кореї та КНР – сподіваються, що технологія 5G значно прискорить розвиток інших технологій, таких як "розумне місто", безпілотні автомобілі тощо.

Для України велике значення має розвиток ринку IT-аутсорсингу. Україна є лідером серед країн – аутсорсерів в Європі. Проте вітчизняна IT-галузь України – це не тільки аутсорсинг. Вітчизняні технологічні стартапи створюють продукти міжнародного рівня, які визнають у всьому світі. Наприклад, український стартап "Reface" потрапив в список рекомендованих від "Google". Проте такі випадки поодинокі. На переконання вітчизняних експертів, 90 % наших IT-спеціалістів працюють саме на засадах аутсорсингу, а не як розробники власних IT-продуктів. Розвитку IT-технологій в нашій країні сприятиме здійснення комплексу заходів, спрямованих на використання у всіх сферах діяльності не лише ліцензійного програмного забезпечення, але і переважно вітчизняного, що, у свою чергу, потребує активізації зусиль у напрямку розробки власних напрацювань та їх запровадження, перш за все, в органах державної влади та на державних стратегічних підприємствах.

Проте останнім часом, пріоритети вітчизняної політики щодо розвитку ІКТ в Україні певним чином стали незрозумілими для наших стратегічних партнерів, особливо США. Так 15 жовтня 2020 року стався резонансний випадок. Проблема полягає у тому, що Держспецзв'язку України підписав меморандум про співпрацю з китайською

компанією “Huawei”, ігноруючи побоювання та відкриту позицію політичного керівництва США щодо глобальної загрозливої діяльності цієї корпорації. На своє виправдання Держспецзв’язку офіційно повідомив, що цей меморандум сприятиме розбудові відповідної платформи з метою впровадження ефективних механізмів державно-приватного партнерства з будь-якими компаніями, які представлені на вітчизняному ринку, у тому числі й компанією “Huawei”. Таким чином, Державна служба спеціального зв’язку порушила законодавство України, підписавши меморандум про співпрацю з компанією “Huawei” без координації та узгодження із зовнішньополітичним відомством України. Укладання вказаного меморандуму стало наслідком негативної реакції з боку міжнародних партнерів, з якими наша країна працює над зміцненням кібербезпеки, що у свою чергу, викликало обурення представників світової спільноти, спричинило потужний удар по іміджу України на міжнародній арені.

Висновки.

Останні світові тенденції демонструють посилення конкуренції між країнами за збереження існуючого ІТ-бізнесу та залучення нових іноземних та локальних інвесторів в цифрову економіку. Держави шукають оптимальні шляхи збереження та підвищення своєї конкурентоздатності на світовому ринку. На цьому фоні у сучасному світі відбувається геополітичне протистояння у кіберпросторі між великими гравцями (США, КНР, РФ) у боротьбі за світове домінування та лідерство. На цьому фоні ситуація, що склалася у вітчизняній ІТ-сфері є досить непростою. На жаль, вітчизняні програмні продукти нездатні замінити зарубіжні аналоги, хоча поступальні кроки у цьому напрямку активно здійснюються. Чимало держав світу законодавчо обмежують використання імпортного програмного забезпечення, особливо у державному секторі, стимулюючи активізацію власних ІТ-розробок та продуктів у цьому сегменті.

Українська ІТ-індустрія все ще перебуває на стадії зародження та розвитку і має потенціал необмеженого зростання в майбутньому. Вітчизняний ІТ-ринок характеризується позитивною тенденцією до зростання показників його прибутковості: у 2019 році вона дорівнювала за обсягами $5 млрд. Хоча сфера інформаційних технологій вважається однією із найбільш залежних від імпорту, оскільки в сучасних умовах досить часто використовуються комп’ютери та сервіси, вироблені виключно за рахунок імпортних компонентів, системного та прикладного програмного забезпечення іноземного походження. Враховуючи викладене, для України в сучасних умовах актуальним залишається визначення концептів державної політики імпортозаміщення, особливо в умовах поширення масштабів пандемії та зростання ролі та значення цифрових технологій для держави, суспільства та пересічених громадян.

Тому доцільним є прискорення розробки та формування правових основ щодо визначення пріоритетних засад імпортозаміщення програмного та технологічного забезпечення власними аналогами на фоні загального розвитку цифрової економіки та зростання частки високотехнологічних продуктів та послуг власного виробництва, що передбачає, зокрема, прискорення прийняття законопроекту “Про стимулювання розвитку цифрової економіки в Україні” від 02.11.20 р. № 4303 [13]. Цей законопроект спрямований на формування важелів щодо стимулювання розвитку цифрової економіки в Україні шляхом створення сприятливих передумов для ведення інноваційного бізнесу, залучення інвестицій, розбудови вітчизняної цифрової інфраструктури. Очікується, що у випадку схвалення цього законопроекту українська ІТ-індустрія до 2025 року становитиме 10 % загального ВВП країни, яка генеруватиме у сукупності $11,8 млрд. Очевидно, що при зростанні вітчизняної ІТ-індустрії та кількості зайнятих у цій сфері фахівців, податкові надходження до державного бюджету також активно зростатимуть,

відбудеться посилення забезпечення кібербезпеки, відбудеться модельний перехід на абсолютне задоволення потреб державного сектору власними технологічними продуктами та відповідним програмним забезпеченням з метою уникнення імпортної залежності.

Використана література

1. Винничук Р.О., Склярук Т.В. Особливості розвитку ІТ-ринку в Україні: стан та тенденції. *Вісник Національного університету "Львівська політехніка". Серія: "Логістика"*. 2015. № 833. С. 3-8. URL: http://nbuv.gov.ua/UJRN/VNULPL_2015_833_3

2. Журавльов О.В., Сімачов О.А. Статистичне дослідження ринку ІТ-послуг в Україні. *Статистика України*. 2018. № 4. С. 25-33.

3. Кораблінова І.А., Кульбацька Н.М. Актуальні проблеми дослідження ІТ-ринку України. *Ефективна економіка.* 2017. № 12. URL: http://www.economy.nayka.com.ua/?op=1&z=5997

4. Новаківський І.І. Розвиток вітчизняної ІТ-галузі як основа формування конкуретноздатної національної економіки. *Соціально-економічні проблеми сучасного періоду України*. 2015. Вип. 3. С. 14-18. URL: http://nbuv.gov.ua/UJRN/sepspu_2015_3_5

5. Чайковська М.П. Стратегії розвитку ІТ-ринку України в умовах фінансової кризи. *Вісник соціально-економічних досліджень*: зб. наук. праць. Вип. № 35. Одеса: ОДЕУ, 2009. С. 132-138.

6. Баранов О.А. Про тлумачення та визначення поняття "кібербезпека". *Інформація і право.* № 2(42)/2014. С. 54-62.

7. Гребенюк М.В. Деякі питання організаційно-правового забезпечення кібербезпеки: огляд кращих практик зарубіжного досвіду. *Підприємництво, господарство і право*. 2019. № 2. С. 203-207.

8. Доронін І.М. Правове регулювання забезпечення кібербезпеки у реалізації окремих функцій держави. *Інформація і право.* № 1(20)/2017. С. 104-111.

9. Шеломенцев В.П. Основні проблеми побудови системи кібернетичної безпеки України. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2014. № 2. С. 183-186. URL: http://nbuv.gov.ua/UJRN/boz_2014_2_44

10. Отчет по развитию отрасли информационно-коммуникационных технологий в Республике Казахстан в 2019 году. URL: https://zerde.gov.kz/upload/Отчет%20ИКТ%20отрасли%202019.pdf

11. Про Цілі сталого розвитку України на період до 2030 року: Указ Президента України від 30.09.19 р. № 722/2019. URL: https://zakon.rada.gov.ua/laws/show/722/2019#Text

12. Про затвердження плану заходів щодо впровадження в Україні системи рухомого (мобільного) зв'язку п'ятого покоління: Розпорядження Кабінету Міністрів України від 11.11.20 р. № 1409. URL: https://zakon.rada.gov.ua/laws/show/1409-2020-р#Text

13. Про стимулювання розвитку сфери інформаційних технологій в Україні: проект закону України від 18.11.20 р. № 4303-2. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70474

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~