

## **ТАРКІН ВАСИЛЬ ПАВЛОВИЧ**

*Національний університет «Одеська юридична академія»,  
аспірант кафедри політичних теорій*

### **ІНФОРМАЦІЙНО-ТЕХНІЧНА ВІЙНА У ГОНИТВІ ВАКЦИНАЦІЇ**

Створення безпечної й ефективної вакцини дарує надію на швидке завершення пандемії Covid-19. Ряд країн невпинно працювали над її отриманням.

У 2019 році з'явилася необхідність розробки вакцини проти Covid-19. Раніше на розробку вакцини йшло від трьох до п'яти років, а у випадку з вакциною проти поліомієліту, розроблену у 1957 році – вісім років. Вакцина від Covid-19 не могла стільки чекати, до того ж отримані раніше знання про коронавіруси, дали змогу зробити цей процес набагато швидшим (до одного року). Так, уже 17 березня 2020 року Американська компанія Pfizer заявила про спільну розробку вакцини із німецькою компанією BioNTech; 20 березня 2020 року Росія розпочала випробування «на лабораторних тваринах для оцінки ефективності і безпеки вакцини» [1]; 23 березня 2020 року Китай оголосив, що понад 108 добровольців отримали перші ін'єкції для тестування майбутньої вакцини [2]. Багатьох країн об'єднало бажання стримати і побороти вірус за допомогою ефективної вакцини – загалом над її розробкою працювало близько 35 компаній в усьому світі.

Пандемія Covid-19 і розробка вакцини проти недуги із перших днів супроводжувалися елементами як інформаційно-психологічної (перекручування, приховування інформації), так й інформаційно-технічної (кібератаки з метою отримання інформації) війни.

Інформаційно-технічна війна – будь-який тип інформаційного впливу із застосуванням інформаційної зброї, метою якого є порушення нормального функціонування інформаційної інфраструктури (дезорганізація роботи технічних засобів, долання системи захисту, обмеження доступу законних користувачів) з можливістю подальшого несанкціонованого збору, копіювання, блокування, видалення інформації. Синонімом даної дефініції може виступити «кібервійна» [3].

Ознаками інформаційно-технічної війни є: 1) економія ресурсів і фінансів – на відміну від розробок збройних технологій, інформаційні технології не вимагають значних фінансових ресурсів. Комп'ютер, доступ до Інтернету, експертиза інформаційних систем і доступ до важливих мереж можуть бути єдиним «озброєнням»; 2) проблема тактичного попередження і оцінки атак; 3) розмиті кордони – значення географічних меж нівелюється під впливом зростання ролі інформаційної інфраструктури, протиборство відбувається у віртуальному просторі. Тепер бої ведуться не лише на землі, морі чи повітрі, але й на віртуальному полі битви. Будь-хто може стати учасником війни, не

лише воюючи, але й передаючи інформацію, гроші чи технології через он-лайн інфраструктуру.

Кібервійна має у своєму арсеналі велику кількість методів – від вірусів і фішингових атак до шпигування. Розглянемо, які з них застосовувалися під час розробки вакцини проти коронавірусу. Початковою метою кіберзлочинців було отримання секретної інформації про *створення вакцини*.

Занепокоєння міжнародними атаками, спрямованих на медичні заклади розпочалося у травні 2020 року, коли ФБР США і Міністерство національної безпеки США офіційно звинуватили Китай у спробі використати комп'ютерне **шпигування** (вторгнення у чужі комп'ютерні системи з метою збору інформації) для крадіжки даних про вакцину проти Covid-19. Такі дії: 1) роблять спробу незаконного отримання інтелектуальної власності, пов'язаної із вакциною, її тестуванням, дослідженнями (очевидно, що інформація про вакцину стане менш цінною, коли вакцина отримає патент), яка має велику цінність – як результат і потенційний прибуток; 2) ставлять під загрозу виготовлення безпечних, ефективних варіантів вакцинації.

На адресу Ірану теж лунали звинувачення про спробу вкрати дослідження за допомогою **зламування** (техніка таємного отримання доступу до інформаційної системи) особистих адрес електронної пошти співробітників ВООЗ. Британські, американські і канадські спецслужби звинувачували Росію і Китай у спробах вкрати дослідження університетів і компаній, які працювали над створенням вакцини шляхом **встановлення шкідливого програмного забезпечення** такого як WellMess і WellMail [4].

Другим етапом інформаційно-технічної «вакцинаційної» війни стали кібератаки спрямовані на *порушення властивостей вакцини*. Війна за інформацію про вакцину Covid-19 проводилася переважно за допомогою цільових **фішингових атак**. У загальному, фішинг – спроба виманити особисту інформацію в користувача Інтернету. Зазвичай для фішингу застосовуються електронні листи, оголошення та фіктивні сайти, за дизайном дуже подібні до тих, які часто відвідує користувач [5]. Цільовий фішинг – різновид фішингової атаки, суть якої – видати себе за законного партнера або учасника із метою отримання або відновлення конфіденційних даних від окремих осіб чи організацій. Для прикладу, різним компаніям, причетним до розповсюдження вакцини у США, Європі, Азії було розіслано серію шкідливих, «фішингових» електронних листів, одне з яких було начебто від керівника HaierBiomedical – великої китайської компанії. У листі вказувалося, що він хоче замовити вакцину і його навіть включили у проект контракту. Очевидно, що кіберзлочинці хотіли отримати інформацію про те, як буде зберігатися і транспортуватися вакцина із якою метою – вкрати технологію чи завадити розповсюдженню вакцини – достеменно невідомо. Було проведено серію кібератак, спрямованих на холододовий ланцюг вакцини (технологія безперервного дотримання належних температурних умов), який дозволяє її транспортування при безпечних

температурах. За даними International Business Machines кібератака розпочалася у вересні 2020 року і полягала у цільовому фішингові компаній, залучених до рефрижераторного транспортування вакцини [6]. Кіберзлочинці, вочевидь були добре знайомі із критичними компонентами холодних ланцюгів. Наприклад, вакцина Pfizer і BioNTech повинна зберігатися за температури від  $-70^{\circ}\text{C}$  до  $-80^{\circ}\text{C}$  до 15 днів і навіть незначне коливання температур або її танення і повторне заморожування може призвести до недієвості, тому можна припустити, що шляхом знищення холодного ланцюга кіберзлочинці сподівалися зробити вакцину неефективною.

Третім етапом стало *незаконне отримання і розміщення даних про вакцину* від Pfizer і BioNTech проти COVID-19 через зламування мереж Європейського агентства лікарських засобів, до завдань якого належить прийняття рішення про допуск вакцини проти коронавірусу на ринок.

Паралельно велася боротьба і за допомогою методів інформаційно-психологічної війни з метою викликати страх, несприйняття і отримання переваги у розробці вакцини. Окрім, посилення «теорії змов»: поява вакцини супроводжується тим фактом, що провідні організації охорони здоров'я, такі як Фонд Білла Гейтса чи ВООЗ будуть причетні до її виробництва чи розповсюдження, тож конспірологічний матеріал твердо доповнився тезами, що окремі особи не лише створили вірус, але й планують на ньому добре заробити.

Сучасна науково-технічна революція породила нові форми конфліктів: інтенсивні, небезпечні, масштабні. Інформаційна цивілізація здійснила трансформацію поняття «агресія», яке набуло форм і особливостей «агресії інформаційної». У числі її складових – інформаційно-технічна війна. Під час пандемії Covid-19 інформаційно-технічні атаки проявилися, по-перше, у комп'ютерному шпигуванні; по-друге, у техніці таємного отримання доступу до інформаційної системи, яким є шпигування; по-третє, шляхом встановлення шкідливого програмного забезпечення; по-четверте, за допомогою методу цільового фішингу.

### ***Список використаної літератури:***

1. В России начались испытания вакцины от коронавируса на животных. [Електронний ресурс]. – Режим доступу: <https://lenta.ru/news/2020/03/20/vaccine/> – Назва з екрана. – Дата публікації: 20.03.2020. – Дата звернення: 15.02.2021.
2. В Ухані вакцину проти коронавірусу ввели трьом групам добровольців. – [Електронний ресурс]. – Режим доступу: <https://tsn.ua/svit/v-uhani-vakcinu-proti-koronavirusu-vveli-trom-grupam-dobrovolciv-1512594.html>. – Назва з екрана. – Дата публікації: 23.03.2020. – Дата звернення: 15.02.2021.
3. Міщенко І. В., Басалюк Н. В., Таркін В. П. Інформаційні війни й кібертероризм: поняття, особливості / І. В. Міщенко, Н. В. Басалюк, В. П. Таркін // Молодий вчений. – 2017. – № 10. – С. 698–703.
4. UK and allies expose Russian attacks on coronavirus vaccine development. – [Електронний ресурс]. – Режим доступу: <https://www.ncsc.gov.uk/news/>

- uk-and-allies-expose-russian-attacks-on-coronavirus-vaccine-development – Назва з екрана. – Дата публікації: 16.07.2020. – Дата звернення: 16.02.2021.
5. Обачність. Пильність. Захист. Ввічливість. Сміливість: посібник із цифрового громадянства та безпеки. – [Електронний ресурс]. – Режим доступу: <https://nus.org.ua/wp-content/uploads/2018/08/PRESS.pdf> – Назва з екрана.
6. Lena Korot, IBM alerte sur les cybermenaces pesant sur le transport des vaccins contre le Covid-19. – [Електронний ресурс]. – Режим доступу: <https://www.usine-digitale.fr/article/ibm-alerte-sur-les-cybermenaces-pesant-sur-le-transport-des-vaccins-contre-le-covid-19.N1036244> – Назва з екрана. – Дата публікації: 03.09.2020. – Дата звернення: 16.02.2021.

**Ключові слова:** інформаційна війна, інформаційно-технічна війна, фішинг, інформаційна зброя, кібервійна.

**Ключевые слова:** информационная война, информационно-техническая война, информационное оружие, фишинг, кибервойна.

**Key words:** information warfare, information and technical warfare, phishing, information weapons, cyberwar.

### **ФІЛІНА АЛІНА ЮРІЇВНА**

*Національний університет «Одеська юридична академія»,  
аспірант кафедри політичних теорій*

## **СОЦІАЛЬНЕ ПАРТНЕРСТВО ЯК МОДЕЛЬ ВІДНОСИН ДЕРЖАВИ ТА ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА**

Соціальне партнерство є необхідною умовою розвитку громадянського суспільства як сукупності незалежних, рівноправних громадян, які взаємодіють, спілкуються, добровільно самоорганізуються на підставі спільних приватних інтересів у громади і об'єднання та захищені необхідними законами від прямого втручання і обмежень з боку держави. На думку дослідників, ключовим аспектом соціального партнерства в широкому сенсі є відносини громадянського суспільства із державою.

Модельний закон про соціальне партнерство, прийнятий на 27 пленарному засіданні Міжпарламентської асамблеї держав-учасників СНД визначає соціальне партнерство як взаємодію органів державної влади, об'єднань роботодавців і профспілок у визначенні і впровадженні в життя узгодженої соціально – економічної політики, політики в галузі трудових відносин, а також двосторонні відносини між роботодавцями і профспілками, спрямовані на забезпечення узгодження їх інтересів в порядку, що визначається законодавством [4].

Інститут соціального партнерства складається із сукупності соціальних суб'єктів. Традиційно до суб'єктів соціального партнерства відносять найманих працівників, роботодавців і державу. Їх функції як