роботи, а також відновлення нормального функціонування після здійснення кібернападів.

Кібербезпека сьогодні набуває значення нової галузі і призначена забезпечити національну безпеку держави. Тому своєчасне планування й реалізація заходів забезпечення кібербезпеки та інформаційного протиборства на глобальному й регіональному рівнях стає одним із пріоритетних завдань держави. Україна не просто може, а вимушена перестати концентруватися виключно на оборонних заходах. Маючи один із найкращих у світі людських потенціалів, фахівців з ІТ, здатність працювати швидко та ефективно, високу мотивацію до протистояння зовнішній агресії, держава повинна робити ставку не лише на оборонні технології, а й на наступальні, в тому числі кіберозброєння.

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНСЬКОГО СУСПІЛЬСТВА: ГІБРИДНИЙ ФРОНТ

Чалапко В. В., аспірант кафедри філософії
Національний технічний університет «Харківський політехнічний інститут»

Виклики та загрози інформаційній безпеці українського суспільства набули нових форм у зв'язку з гібридними атаками, що здійснюються повсякчасно проти нашої держави. Україна за останні п'ять років стикнулась з новітніми методами ведення "гібридної війни" в основу яких покладено, в першу чергу, інформаційну складову.

З точки зору науковців, одним з основних засобів ведення "гібридної війни" є так звана інформаційна зброя, яка за своєю ефективністю та наслідками становить значну загрозу для будь-якої держави втягнуту у гібридне протистояння, для України зокрема. Інформаційна зброя – це інформація та інформаційні технології, які є засобом ведення інформаційних воєн і призначення яких полягає в зміні системних якостей об'єкта інформаційного впливу за допомогою прихованих установок на здійснення задуманих користувачем інформаційної зброї дій. Напрямки і приклади використання інформаційної зброї є такі:

− порушення, пошкодження або модифікація інформаційних ресурсів і знань людей про самих себе та про середовище яке їх оточує;

− здійснення впливу на суспільну думку та позицію політичної еліти;

− завдання шкоди протилежній стороні дипломатичними засобами;

− пропагандистські, психологічні та підривні акції у сфері культури й політики;

− дезінформація;

− чутки, які створені навмисно;

− упровадження у ЗМІ своїх прибічників для проведення підривних акцій;

− проникнення в комп'ютерні мережі та системи управління базами даних, зараження комп'ютерних систем вірусами, навмисне введення різного роду помилок у програмне забезпечення об'єкта;

− інформаційна підтримка дисидентських та опозиційних рухів.

Різновидом інформаційної зброї є так звана інформаційно-психологічна зброя, яка застосовується з метою руйнування тонких структур суспільства (мораль, традиції) та формування інформаційного колоніалізму активною стороною і може бути задіяна як самостійно, так і у комплексі з іншими видами сучасної зброї, що використовуються у "гібридних війнах". Даний вид зброї передбачає здійснення інформаційно-психологічного впливу на певні об'єкти та маніпуляції їхніми цінностями й поведінковими настановами, що зводяться до підмін знаків і значень та іміджевої маніпулятивної гри смисловими полями.

Необхідно зазначити, що інформаційна зброя особливо ефективно діє, проти тієї країни, яка знаходиться у кризовому стані, у суспільній свідомості якої панує ціннісна амбівалентність, соціально-політична невизначеність. Застосування інформаційної зброї стає особливо дієвим, коли у державі спостерігається протистояння між політичними силами, наявна криза моральної та правової свідомості, слабкою є патріотично налаштована еліта тощо.

Застосовуючи інформаційну зброю, суб'єкти агресії здійснюють постійні атаки спрямовані на інформаційно-комунікаційний простір нашої країни. За оцінками вітчизняних експертів з проблем інформаційної безпеки, що сформовані на основі аналізу іноземного впливу на інформаційний медіа і кіберпростір України, існують ознаки реальних загроз для нашої держави. Про це свідчать такі основні тенденції:

− цілеспрямоване формування окремими іноземними державами негативного міжнародного іміджу України;

− активізація критики вищого державного керівництва України;

− здійснення низкою зарубіжних країн потужного інформаційного тиску на Україну з метою спонукання українського керівництва до прийняття вигідних для цих країн рішень у внутрішньо та зовнішньополітичній сферах

− посилення інформаційних заходів з перешкоджання реалізації Україною її зовнішньополітичного курсу та спонукання її до участі в проектах, які в сучасних умовах не вигідні нашій державі;

− дискредитація нашої держави як конкурента у сфері міжнародного військово-технічного співробітництва;

− зростання для України загроз кібернетичних атак, що обумовлено появою нових, більш досконалих зразків кібернетичної зброї.

Безсумнівно, розуміння інформаційної безпеки має включати в себе не тільки захист інформаційних ресурсів суспільства, держави та людини, а й збереження ціннісних аспектів історичної пам'яті, культурних традицій, специфічного національно-етнічного способу життя українського народу. У цьому контексті мова йде про захист інформаційного суверенітету нашої країни, розуміння якого вбирає в себе правові, політичні, ціннісно-культурні, безпекові й інформаційні процеси в державі. Цілком логічно, що програми з інформаційної безпеки спрямовані в першу чергу на захист інформаційного суверенітету держави.

Спираючись на дослідження О. Дзьобаня, варто виокремити декілька основних груп загроз інформаційній безпеці України. Перша група пов'язана з бурхливим розвитком нового класу зброї − інформаційної, яка здатна ефективно впливати і на психіку, свідомість людей, і на інформаційно-технічну інфраструктуру суспільства й армії. Друга група інформаційно-технічних загроз для особистості, суспільства й держави − це новий клас соціальних злочинів, заснованих на використанні сучасної інформаційної технології (махінації з електронними грошима, комп'ютерне хуліганство тощо). Третя група інформаційно-технічних загроз − електронний контроль за життям, настроями, планами громадян, політичних організацій. Четверта група інформаційних загроз – використання нових інформаційних технологій у політичних цілях.

Необхідно зазначити, що існуючі загрози інформаційній безпеці України значно посилюються у зв'язку з низкою проблем функціонування інформаційного простору нашої держави, які набули іншого виміру під впливом "гібридних атак". Зокрема, до головних негативних чинників, які зумовлюють сучасний стан українського інформаційного простору фахівці відносять такі:

– відсутність чіткої скоординованої державної інформаційної політики за умов наявності й активного виконання кількох, на жаль, недостатньо скоординованих державних програм за такими напрямами, як інформатизація, формування і захист національного інформаційного ресурсу і простору тощо;

– інвестування інформаційних структур (як державних, так і приватних) за "залишковим принципом" унаслідок економічних причин;

– експансія в Україну зарубіжних виробників інформаційної продукції, що об'єктивно переважають національних за якістю продукції, економічними можливостями, а також застосовують агресивну ринкову стратегію;

− недостатній професійний рівень працівників інформаційної сфери, недоліки вітчизняної системи їхньої підготовки (особливо це стосується електронних ЗМІ та нових інформаційних, зокрема, глобальних систем);

− технічне відставання інформаційної інфраструктури і її повна залежність від постачання іноземної техніки, занепад вітчизняної телекомунікаційної промисловості.

Отже, реалії "гібридної війни" вимагають від держави та структур громадянського суспільства більш системних, скоординованих та стратегічно спрямованих дій щодо зміцнення внутрішніх підвалин інформаційної безпеки України.

Як справедливо зазначає У. Ільницька, Україна стала об'єктом інформаційно-психологічних впливів, операцій, війн, а її інформаційна безпека опинилась під загрозою. Можна констатувати, що:

1) український інформаційний простір є незахищеним від зовнішніх негативних пропагандистсько-маніпулятивних впливів і стає об'єктом інформаційної експансії;

2) у світовому медіапросторі відсутній український національний інформаційний продукт, що поширював би об'єктивну, неупереджену та актуальну інформацію про події в Україні. Як наслідок – світова громадськість відчуває брак інформації або отримує

її з інших джерел, які часом дезінформують, надають викривлену, спотворену, неповну інформацію. Водночас, проти України активно застосовується потужний медіа-ресурс, здійснюється експансія іноземних суб'єктів на ринку інформаційних послуг, активізуються негативні інформаційні впливи, які спрямовані на викривлення реальності, заниження міжнародного іміджу держави;

3) діяльність вітчизняних ЗМІ щодо систематичного, об'єктивного висвітлення фактів, подій та явищ є недостатньою та позбавлена стратегічного планування; інформаційно-комунікативна політика України у сфері національної безпеки потребує невідкладного перегляду та удосконалення.

Таким чином, інформаційна безпека українського суспільства потребує переформатування у зв'язку з новітніми, гібридними загрозами. Зокрема, мова йде про необхідність більш ретельного стратегічного планування у цій сфері та посилення якості системних дій, спрямованих не тільки на захист інформаційного суверенітету нашої держави, а й на проведення інформаційних наступальних (профілактичних) операцій. Для посилення інформаційної безпеки України, на наше переконання, варто активніше використовувати вітчизняні наукові розробки та закордонний досвід.

ДО ПИТАННЯ ПРО ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНЕ ПРОТИБОРСТВО В МЕДІА ПРОСТОРІ

Голодюк В.Я., слухач, Національний університет оборони України

У 2014 році Україна зазнала прямої агресії з боку Російської Федерації. Спочатку було анексовано Автономну Республіку Крим, згодом через пряме втручанню Росії та підтримку сепаратистських рухів виникла загроза втрати ще двох територіальних одиниць України – Донецької та Луганської областей. Водночас, ще задовго до загострення ситуації, що перетворилася у збройне протистояння, проти України розпочалась інформаційна війна. Форми, методи, технології та засоби її ведення, з одного боку, вважаються простими, навіть примітивними, з другого – ця війна була давно спланована, розроблена й досить успішно реалізована. Принаймні, українській владі, суспільству, громадському сектору та журналістам довелося докласти неймовірних зусиль, щоб протистояти пропагандистському тиску російських ЗМІ.

Розробка концепції протидії інформаційним впливам випливає безпосередньо з аналізу цих впливів. Під інформаційним впливом