КІБЕРБЕЗПЕКА ЯК ЗАХИСТ ВІД ІНФОРМАЦІЙНОЇ ВІЙНИ

Худавердова А. О.
Харківський національний університет Повітряних Сил імені Івана Кожедуба

На сьогодні накопичені значні напрацювання в галузі інформаційної безпеки. Проблематикою етимології поняття кібер, кіберпростору, «гібридної війни», національної безпеки, інформаційних атак у державних і недержавних структурах займалися такі провідні українські та світові вчені, як І. Кочан, Є. Магда, Р. Грищук, В. Горбулін, В. Пядишев, О. Рибальський, М. Делягін, В. Кутирьов, Г. Мірської, І. Міхеєв, В. Хорос, В. Антипенко, В. Крутов, В. Ліпкан, У. Еко.

Науково-технічна революція початку XXI сторіччя спричинила в усьому світі глибокі системні перетворення. Завдяки поєднанню досягнень у сфері новітніх інформаційно-комунікаційних технологій (ІКТ) із надбаннями, що постали на базі стрімкого розвитку інформаційно-телекомунікаційних систем (ІТС), сформувалися принципово нові глобальні субстанції – інформаційне суспільство, а також інформаційний та кібернетичний простори, які мають нині практично необмежений потенціал і відіграють провідну роль в економічному та соціальному розвитку кожної країни світу.

У зв'язку з поширення ІКТ та ІТС суспільство отримало як чисельні переваги так і певні проблеми, які зумовили вразливість інформаційної сфери щодо стороннього кібернетичного впливу. Відсутність такої системи може призвести до втрати політичної незалежності будь-якої держави світу, бо йтиметься про фактичний програш нею змагання невійськовими засобами та підпорядкування її національних інтересів інтересам протиборчої сторони. Постала необхідність невідкладного створення надійної системи кібернетичної безпеки.

Кібербезпеку можна визначити як стан захищеності кіберпростору держави в цілому або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і національним інтересам.

Досягається такий стан завдяки сукупності активних захисних і розвідувальних дій, що у процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугруповань розгортаються навколо ІР, ІКТ і ІТС.

Головні проблеми забезпечення кібербезпеки постають з таких причин:

• відсутності чіткого усвідомлення ролі та значення кібербезпекової складової в системі забезпечення національної безпеки держави;

• дефіциту щодо методичного забезпечення та кадрового наповнення відповідних структурних підрозділів;

• відсутності належної координації діяльності відповідних відомств, а отже, і неузгодженості дій зі створення окремих елементів системи кібербезпеки;

• дефініційної, термінологічної та нормативно-правової неврегульованості у сфері кібербезпеки;

• залежності держави від програмних і технічних продуктів іноземного виробництва.

Згідно із Законом № 2163 основними суб'єктами національної системи кібербезпеки України є Держспецзв'язку та захисту інформації, Нацполіція, СБУ, Міноборони та Генштаб ЗСУ, розвідувальні органи, НБУ. Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є: міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; ЗСУ, інші військові формування, утворені відповідно до закону; НБУ; підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури; суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

Протягом останніх років Україна, як і більшість інших країн світу, робить впевнені кроки в напрямку розбудови інформаційного суспільства, забезпечення кібербезпеки та боротьби з кіберзлочинністю. Нормативно-правову базу в цих сферах діяльності становлять Конвенція Ради Європи про кіберзлочинність, ратифікована Законом України від 07.09.2005 року № 2824-IV, а також відповідні закони України та Укази Президента України, присвячені цій проблемі, положення Кримінального кодексу України, окремі постанови Кабінету Міністрів та рішення РНБО України.

Важливий практичний крок у реалізації наявної нормативно-правової бази було зроблено створенням 2007 року Центру реагування на комп'ютерні інциденти, що ввійшов доскладу Державної служби спеціального зв'язку та захисту інформації України. На виконання

статті 35 Конвенції про кіберзлочинність у червні 2009 року при Службі безпеки (СБ) України на базі спеціального підрозділу для боротьби з кіберзагрозами запрацював Національний контактний пункт формату 24/7 із реагування та обміну терміновою інформацією про вчинені кіберзлочини. Окрім того, Указом Президента України «Про виклики та загрози національній безпеці України у 2011 році» від 10 грудня 2010 року № 1119/2010 ухвалено рішення про початок створення Єдиної загальнодержавної системи протидії кіберзлочинності. Іншим Указом Президента України «Про внесення змін до деяких законів України про структуру і порядок обліку кадрів Служби безпеки України» від 25 січня 2012 року № 34 у структурі СБ України створено 5 Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки. З огляду на динаміку поширення комп'ютерних інцидентів теренами України в липні 2010 року у структурі МВС України на базі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми, утворено новий структурний підрозділ – Департамент боротьби з кіберзлочинністю та торгівлею людьми.

Світ змінює своє ставлення до проблем кібербезпеки. В України дедалі більше зростає усвідомлення того, що найнебезпечнішими є кібернетичні та інформаційні загрози, що виходять від агресивно-налаштованих країн та їх спецслужб.

Гібридна агресія Російської Федерації щодо України є різнорівневим поєднанням різноманітних комбінацій форм та методів негативного впливу, серед яких домінуючим напрямком є інформаційний та кібернетичний. Одним із найважливіших аспектів негативного інформаційного впливу, що намагаються здійснювати російські спецслужби, є спрямованість на руйнування української державності починаючи з базового рівня – історичної пам'яті та самоусвідомлення нації як такої.

Для досягнення цієї мети російські спецслужби використовують підконтрольні їм ЗМІ, інтернет-ресурси, групи у соцмережах, блогери, тролі та навіть поштові сервіси. Через цю розгалужену мережу не тільки збирається розвідувальна інформація про українських громадян, але й проводяться деструктивні пропагандистські інформаційні операції.

Низка потужних та складних кібератак на комп'ютерні мережі енергетичного, банківського, транспортного секторів, галузі зв'язку, які відбулись з початку 2014 року, вкотре засвідчили, що агресор і надалі використовуватиме кібератаки як інструмент геополітичного впливу. Протидія цьому потребує не тільки зусиль на національному рівні, але й відпрацювання дієвих механізмів міжнародного співробітництва.

З 2014 року одними з перших руйнівної кібератаки зазнали комп'ютерні мережі Центральної виборчої комісії, за тиждень до виборів у травні 2014 року відбулось руйнування технологічної інфраструктури.

У грудні 2016 року внаслідок потужних кібератак на державні органи і транспортні підприємства України Державним казначейством тимчасово призупинено казначейське обслуговування клієнтів. Було заблоковано доступ до веб-порталу Міністерства фінансів, а також порушено роботу деяких об'єктів енергетики та транспорту.

27 червня 2017 року атака з використанням шкідливого програмного засобу "Petya/NotPetya", який використовував маловідомі вразливості системного ПЗ Windows, призвела до тимчасового блокування роботи обчислювальних систем окремих об'єктів критичної інфраструктури України.

У квітні 2018 року виявлено та локалізовано кібератаку на об'єкти оборонно-промислового комплексу держави, спрямовану дискредитацію України на міжнародній арені та поширення в інформаційному просторі недостовірної інформації щодо низки об'єктів критичної інфраструктури, зокрема ненадійності української сторони у співпраці в науковій та інженерній сферах.

Україна поступово нагромаджує важливий досвід у захисті власної ІТ-інфраструктури від кіберзагроз сучасності та протидії проявам кібертероризму. Утім протистояти фізичному руйнуванню технічних засобів, дезорганізації роботи інформаційних систем і мереж, порушенню функціонування об'єктів нападу, а також протиправній діяльності соціальних інженерів в умовах інтенсифікації кібервтручань кожного дня стає все важче. Одна з головних причин цих негараздів полягає в «незадовільному кадровому забезпеченні відомств відповідними фахівцями у сфері інформаційної безпеки», як наголошується в аналітичній доповіді Національного інституту стратегічних досліджень при Президентові України «Кібербезпека: світові тенденції та виклики для України».

Найбільшу загрозу вітчизняним установам і відомствам становить відчутна нестача професіоналів з інформаційної та кібербезпеки, здатних:

1) відшукувати, збирати або добувати інформацію про ІТ-системи й мережі протиборчих сторін, а також про технології та засоби їхнього впливу на власну інфосферу;

2) виявляти ознаки стороннього кібервпливу і моделювати можливі ситуації такого впливу, прогнозуючи відповідні наслідки;

3) протидіяти несанкціонованому проникненню протиборчих сторін у власні ІТ-системи й мережі, забезпечуючи стійкість їхньої

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;