§ 10. Інформаційно-технологічні атаки і способи захисту кіберпростору: новітні тактики гібридних війн

Захищеність кіберпростору як складова інформаційної безпеки. На сучасному етапі розвитку суспільства інформаційна безпека держави перебуває у фокусі уваги, стає одним із пріоритетів державної політики, адже ведення інформаційних війн передбачає необхідність протидіяти їм. Аналізуючи Доктрину інформаційної безпеки України, що затверджена указом Президента України від 25 лютого 2017 року, можна виокремити ***кілька напрямів забезпечення інформаційної безпеки***: утвердження свободи слова в країні; формування якісних урядових комунікацій – комплексу заходів, що передбачають діалог уповноважених представників Кабінету Міністрів України з цільовою аудиторією з метою роз'яснення урядової позиції та/або політики з певних проблемних питань [28]; об'єктивне інформування світової спільноти про Україну і формування її позитивного іміджу через систему іномовлення; інформаційна реінтеграція тимчасово окупованих територій; боротьба з пропагандою (контрпропаганда); протистояння кібератакам.

Механізм реалізації Доктрини інформаційної безпеки полягає в розподілі обов'язків між різними державними суб'єктами. До державних органів, що відповідальні у межах своєї компетенції за виконання зазначених напрямів, належать Міністерство інформаційної політики України, Міністерство закордонних справ України, Міністерство культури України, Державне агентство України з питань кіно, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення. Координацію діяльності органів виконавчої влади щодо реалізації Доктрини та забезпечення національної безпеки в інформаційній сфері має здійснювати РНБО, яка також визначає ключові заходи, відповідно до положень документа [26]. Кабінет Міністрів України також забезпечує здійснення інформаційної

політики держави, фінансування програм, пов'язаних з інформаційною безпекою, спрямовує й координує роботу міністерств, інших органів виконавчої влади в цій сфері [26].

Створення безпечного кіберпростору є одним із напрямів інформаційної політики. В Окінавській хартії глобального інформаційного суспільства, прийнятій лідерами країн вісімки у японському м. Окінава у 2000 р., кіберпростір розглядається як частина глобального інформаційного простору, пов'язана з комп'ютерною інфраструктурою, насамперед з Інтернетом [22, с. 205].

Д. Дубов характеризує **кіберпростір** як середовище, створене організованою сукупністю інформаційних процесів на підставі об'єднаних загальними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем незалежно від форми власності [8, с. 70].

Кіберпростір держави перебуває під різноманітними **кіберзагрозами**, серед яких вплив на 1) стан електронних інформаційних ресурсів та на можливість доступу до інформації; 2) функціонування об'єктів критичної інфраструктури; 3) складові частини інформаційно-комунікаційної інфраструктури; 4) морально-психологічний стан суб'єктів кіберпростору.

Тож поняття **кібербезпека** позначає стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та / або телекомунікаційних мереж, за якого мінімізується можливість завдати їм шкоди (через неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації) [8, с. 72] і стосується не лише технічних питань і технологічного складника, а й людського чинника – ворожих інсайдерських дій чи людський помилок, а також проблем владних відносин на національному та міжнародному рівнях [8, с. 71].

Можливість країни впливати на кіберпростір у науковій літературі окреслили поняттям **кіберпотужність**, яка залежить від багатьох чинників (можливості інтернету та інформаційних

технологій, можливості інтернет-ринку та ІТ-індустрії та ін.) [8, с. 59-60]. Рідше у вітчизняних джерелах використовується термін **кіберсила** (CyberPower) – потужність на основі інформаційних ресурсів, що залежить від ресурсів, які характеризують кіберпростір [33, с. 3]. Кіберсила країни вимірюється через такі параметри: рівень залежності, атак та захисту в кіберпросторі [23, с. 385]. Подію, яка може порушити кібербезпеку (конфіденційність, цілісність та доступність інформації у кіберпросторі), називають **кіберінцидентом** [6, с. 179].

Нормативно-правове підґрунтя для створення національної системи кібербезпеки. Країною з найпотужнішою кіберсилою є Сполучені Штати Америки, тож важливо знати її досвід у сфері кібербезпеки, зокрема, в питаннях створення відповідної нормативно-правової бази. У 2003 році була опублікована Національна стратегія безпеки кіберпростору (National Strategy to Secure Cyberspace) США. Вона стала складовою частиною стратегії національної безпеки. NSSC визначає три стратегічні цілі: захист від кібератак критичних інфраструктур США; зменшення вразливості від кібератак в загальнонаціональному масштабі; мінімізація збитків та часу відновлення від кібератак.

Адміністрація президента Барака Обами створила дієвий інструмент стримування потенційних кіберзагроз для обороноздатності і економіки США. Першого квітня 2015 року був підписаний указ «Про арешт власності осіб, причетних до серйозних протиправних дій у кіберпросторі», який дає владі США право накладати санкції на компанії і фізичних осіб, причетних до кібератак, що порушують функціонування об’єктів критичної інфраструктури США та ключових комп’ютерних мереж і систем, а також застосовувати відповідні санкції до осіб і компаній, які за допомогою кібератак незаконно привласнили кошти або інші активи, включаючи комерційні секрети, персональні дані та фінансову інформацію американських компаній і організацій, або використовували їх, якщо їм було відомо, що вони викрадені в ході кібератаки третьою стороною. Саме прописані в ньому механізми й лягли в основу прийнятих у грудні 2016 року санкцій проти Росії.

Питання кібербезпеки стало одним із пріоритетних напрямів діяльності і нового президента – Дональда Трампа, який має намір приділяти увагу розвитку кіберкомандування збройних сил Америки (у кінці січня в американських ЗМІ було оприлюднено проект президентського указу «Про зміцнення кібербезпеки і можливостей США в кіберпросторі»). У ньому визначено такі напрями роботи:

1) комплексна перевірка американської інформаційної інфраструктури на предмет критичних вразливостей (відповідальне відомство Міноборони щодо систем, які забезпечують національну безпеку та Міністерством внутрішньої безпеки – щодо цивільної інфраструктури, серед іншого систем федерального уряду і приватного сектора, а координація зазначених завдань покладається на директора нацрозвідки, помічника президента з питань нацбезпеки, а також помічника президента з питань внутрішньої безпеки та боротьби з тероризмом);
2) оцінювання потенційних супротивників США в кіберпросторі;
3) оцінювання можливостей США в кіберпросторі (мають здійснювати Міністерство оборони, Міністерство внутрішньої безпеки і Агентство національної безпеки для розроблення системи рекомендацій і практичних кроків для зміцнення захисту американської критичної інфраструктури);
4) дослідження і розробка заохочувальних заходів для зміцнення кібербезпеки приватного сектора (відповідальне Міністерство торгівлі) [4].

У Стратегії національної безпеки України 2015 р. вперше сформульовано загрози кібербезпеці та безпеці інформаційних ресурсів, а також визначено пріоритети забезпечення кібербезпеки. У 2016 р. було прийнято Стратегію кібербезпеки України, спрямовану на реалізацію до 2020 р. положень Стратегії національної безпеки України. Стратегія закладає основу формування національної системи кібербезпеки.

До **пріоритетів України в сфері кібербезпеки** належать: розвиток інформаційної інфраструктури держави; розвиток мережі реагування на комп'ютерні надзвичайні події (CERT – Computer

Emergency Response Team – команда реагування на комп'ютерні надзвичайні події), розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів, забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони, розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки.

У Стратегії кібербезпеки України зазначено, що розвиток безпечного, стабільного і надійного кіберпростору має полягати, зокрема, у таких діях:

1) вироблення і оперативна адаптація державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягненні сумісності з відповідними стандартами ЄС та НАТО;
2) створення вітчизняної нормативно-правової та термінологічної баз у цій сфері, гармонізація нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО;
3) формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту;
4) розвиток технологій кіберзахисту засобів рухомого зв'язку, забезпечення апаратної, контентної безпеки, безпеки додатків та сервісів зв'язку;
5) підвищення цифрової грамотності громадян та культури безпекової поведінки в кіберпросторі, набуття комплексних знань, навичок і здібностей, необхідних для підтримки кібербезпеки, впровадження державних і громадських проектів підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;
6) розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, підтримка міжнародних ініціатив у сфері кібербезпеки, які відповідають національним інтересам України,

поглиблення співпраці України з ЄС та НАТО для посилення спроможностей України у сфері кібербезпеки, участь у заходах зі зміцнення довіри у кіберпросторі, які проводяться під егідою ОБСЄ.

П'ятого жовтня 2017 року було прийнято Закон України «Про основні засади забезпечення кібербезпеки України», який «визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки» [24].

Важливим є питання формування ефективної **національної системи кібербезпеки**. Вона «має забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та / або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури» [27].

Суб'єктами національної системи кібербезпеки, які становлять її основу, є Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи. Кожен з цих суб'єктів бере на себе частину зобов'язань, щоб забезпечувати кібербезпеку України, а координацію та контроль їх діяльності має здійснювати Рада національної безпеки і оборони України.

Також «мають бути створені умови для залучення підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інфраструктури, до забезпечення кібербезпеки України» [27].

Держава має сприяти і залученню наукових установ, навчальних закладів, організацій, громадських об'єднань і громадян до розробки та реалізації заходів із кібербезпеки і кіберзахисту.

Види кіберконфліктів та протистояння їм. Кіберзагрози охоплюють різноманітні впливи агресора, яким можуть бути окремі держави, групи та особи, на різні сфери життя держави: економічну, науково-технічну, сферу державного управління, оборонно-промисловий і транспортний комплекси, інфраструктуру електронних комунікацій, сектор безпеки і оборони України. Нині кіберзлочинність не обмежується збиранням, зберігання, використанням, знищенням, поширенням персональних даних, незаконними фінансовими операціями, крадіжками та шахрайствами в мережі Інтернет, а стає транснаціональною проблемою та «здатна завдати значної шкоди інтересам особи, суспільства і держави» [27].

Кібератака розглядається як сукупність дій противника або ворожої групи, яка намагається досягти певної негативної для об'єкта атаки цілі чи ефекту з використанням комп'ютерної техніки зокрема чи можливостей кіберпростору в цілому, найчастіше – з використанням спеціально розроблених для таких завдань засобів. Сукупність кібератак, що перевищують за своїм загальним негативним впливом певне порогове значення, можуть розглядатися як початок кібервійни [8, с. 75] (рис. 10.1).

Кібератаки можуть здійснюватися дилетантами, хакерами, інсайдерами з метою особистого збагачення чи вигоди, а також спонсоруватися державою з метою шпигунства чи в умовах ведення інформаційної війни (рис. 10.2).

М. Каветлі пропонує таку **типологію кіберконфліктів**:

1) кібервандалізм (включає зміни чи знищення змісту, наприклад, веб-сайту, вимкнення чи перевантаження сервера, є найпоширенішою формою кіберконфлікту, що має значний суспільний резонанс, однак наслідки таких інцидентів обмежені в часі та відносно незначні);
2) інтернет-злочини (діяльність переважно з метою отримання прямого фінансового зиску, може включати як злочини з комп'ютерної техніки, так і суто комп'ютерні злочини);

3) кібершпигунство (головною жертвою найчастіше стає корпоративний сектор. За окремими підрахунками, втрати компаній від такої діяльності становлять до 1 трлн доларів США на рік. Урядові мережі, в яких міститься конфіденційна інформація, стають жертвами атак доволі рідко, хоча останнім часом такі атаки частішають);
4) кібертероризм (потенційно масштаби збитків від кібертеракту оцінюються надзвичайно високо, однак дотепер не було жодного реального випадку кібертероризму);
5) кібервійна [цит. за 8, с. 78].

Прикладом застосування кіберзброї в міжнародному кіберпросторі є кібератаки 2007 року, які завдали шкоди веб-сайтам відомих естонських організацій, зокрема установ громадського сектору, банків і медіа-компаній. Інформаційні ресурси різних країн стають об'єктами кібератак. Так, у 2010 році внаслідок кібератаки на компанію Google була тимчасово зупинена китайська версія цього сайту [16, с. 796].

Щорічно в спільній доповіді розвідувальних служб США йдеться про глобальні загрози національній безпеці. Починаючи з 2014 року, кіберзагрози займають 1-2 місця серед потенційних загроз, а список супротивників США стабільно містить РФ, КНР, Іран і КНДР [4].

У жовтні 2016 року адміністрація США офіційно звинуватила Росію у пошкодженні серверів американських партій під час виборчих перегонів. А в грудні президент США Барак Обама підписав указ про введення санкцій проти ФСБ і ГРУ, трьох російських компаній, що займаються інтернет-технологіями, а також шести громадян РФ у зв'язку з їх імовірною причетністю до кібератак на державні і політичні інститути США. У січні 2017 року розвідувальне відомство США оприлюднило заяву, в якій йшлося про повномасштабну кіберзагрозу для уряду США з боку Росії. У доповіді директора Нацрозвідки Джеймса Клеппера американському уряду та вищим посадовим особам зазначалося, що втручання росіян у процес виборів у США не обмежувалося лише хакерськими атаками. Також були використані такі засоби, як класична

пропаганда, дезінформація, фейкові новини, а наказ на втручання віддав особисто президент РФ.

Щодо України, то, за даними Держспецзв'язку, тільки в 2014 р. фахівці команди реагування CERT-UA вжили заходів щодо реагування на 216 комп'ютерних інцидентів (кіберінцидентів), 124 з яких стосувалися державного сектору України.

До **основних кіберзагроз України** належать:

1) використання кібератак для досягнення політичних цілей (атаки на системи ЦВК під час двох виборчих кампаній, використання проти українських урядових і неурядових структур), зокрема за допомогою бот-мереж;
2) поява нових та модифікація наявних зразків шкідливого програмного забезпечення проти України (віруси BlackEnergy, Uroboros, EnergeticBear, CrouchingYeti, EpicTurla);
3) поширення шкідливого програмного забезпечення, спрямованого на формування бот-мереж; фальшивих антивірусів, вірусів для основних мобільних платформ (у т.ч. для збирання даних з пристроїв, спостереження, запису розмов і перехоплення повідомлень).

Загрози кібербезпеці актуалізуються через дію таких чинників:

1) невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам;
2) недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз;
3) безсистемність заходів кіберзахисту критичної інформаційної інфраструктури;
4) недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інформаційної інфраструктури та державних електронних інформаційних ресурсів;

5) недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру;
6) недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки [27].

В аналітичній доповіді до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2016 році» зазначається, що загалом кількість кібератак в Україні збільшилася. І важливо зазначити не просто загальне зростання, а збільшення кількості атак типу APT (Advanced Persistent Threat), тобто цільових кібератак проти комп'ютерної мережі держави в поєднанні з негласними розвідувальними або підривними акціями, основною метою яких є отримання, порушення цілісності або блокування інформації, важливої для держави. Протягом 2013-2015 років було зафіксовано цілу низку APT-атак (Snake, Uroboros, Sofacy/APT28, EpicTurla, BlackEnergy 2 та 3, Armageddon та інші) на українські об'єкти. Вони спрямовані переважно проти державних інституцій і мають яскраво виражену мету збору таємної інформації чи інформації з обмеженим доступом. Зважаючи на те, що саме РФ здійснює системну гібридну агресію проти України, можна говорити про те, що за значною кількістю таких атак стоїть саме російський інтерес. Навіть західні партнери однозначно стверджують факт ведення Російською Федерацією кібервійни проти України [1, с. 222].

Серед випадків кібератак, що сталися останнім часом, атаки із застосуванням шкідливого програмного забезпечення BlackEnergy наприкінці 2015 року на українські телеканали «СТБ», «5 канал», «Україна». «Їхні сервери, а саме головні завантажувальні записи були повністю змінені. Більшість файлів на диску просто заповнювались нулями, зовні ніяк не змінившись», тож «у результаті атаки постраждала велика кількість інформаційних матеріалів, і робота каналів була значно ускладнена» [11, с. 18]. Як бачимо, кібервійна суттєво впливає й на умови роботи журналіста.

Так, Міністерство юстиції Сполучених Штатів оголосило, що виведення з ладу Yahoo в 2014 році, внаслідок чого було розкрито

понад 500 мільйонів поштових скриньок, – це справа рук російської Федеральної служби безпеки (ФСБ), чиї агенти співпрацюють з кіберзлочинцями. Це було одне з найбільших пошкоджень електронної пошти в історії, націлений проти поштових акаунтів групи журналістів, дисидентів і американських урядових чиновників [29].

За словами експерта «Інтерньюз-Україна» Віталія Мороза, кібервійна з Росією диктує нові правила для журналістів і «якщо журналіст розуміє, як безпечно пересилати інформацію, він зменшує ризики для військових» [13].

У червні 2016 року Український кіберальянс – спільнота українських кіберактивістів, що протидіють російській агресії в Україні, – передав волонтерам міжнародної спільноти Inform Napalm величезний масив даних, добутих зі зламаних поштових листувань та хмарних сховищ російських журналістів і пропагандистів.

Було оприлюднене листування російських пропагандистів щодо теми MH17, про обстріли української території, спроби інформаційного впливу росіян, спрямованого не тільки проти України, але і США. Зокрема, було розкрито подробиці роботи журналіста і пропагандиста державного «Першого каналу» РФ Сергія Зеніна, а також інформацію про його співпрацю з «Russia Today» та спроби дискредитації Агентства національної безпеки США [14].

Серед інших випадків атак на Україну – кібератака на Прикарпаття обленерго, що сталася 23 грудня 2015 року. Розслідування цього злочину показало, що функційну частину Black Energy завантажили в систему ще за шість місяців до фактичної дати атаки. Хакери «перепрошили» всю систему віддаленого доступу й отримали повний контроль над управлінням, зокрема рубильниками, а працівники були не в змозі протидіяти. Водночас відбувалася телефонна «сервісовідмовна» атака (так звана TelephonicDenial-of-ServiceAttack): на кол-центри компанії посипалися тисячі дзвінків із фіктивних номерів, що повністю унеможливило комунікацію між користувачами та підприємством через цей канал [11, с. 17]. Унаслідок цього «225 тис. споживачів на години залишилися без світла. За оцінками українських та іноземних фахівців, ця атака безпосередньо пов’язана з діями Російської Федерації. Про це

свідчать масштаби її підготовки (перші заходи, спрямовані на реалізацію цієї атаки, було вжито ще в 2014 році), ціль (абсолютно нетипова для традиційних цілей хакерів, які цікавляться передусім банківськими установами), використані засоби (вірус, що був підготовлений саме для цієї атаки і не детектувався антивірусними засобами)» [1, с. 221-222].У січні 2016 року була спроба повторити атаку, але вона була невдалою.

16 січня 2016 р. виявлено ознаки хакерського проникнення до інформаційних систем аеропорту «Бориспіль» знову із застосуванням вірусу Black Energy, яке було успішно локалізоване.

12 травня 2017 року сталася масштабна кібератака, від якої постраждали, за словами директора Європолу Роба Вейнрайта, 200 тисяч користувачів у 150 країнах світу. Комп'ютерний вірус-вимагач блокував доступ до файлів на дисках комп'ютерів, вимагаючи грошей за відновлення доступу. Найбільше від нього постраждали Британія і Росія. В Англії під удар вірусу потрапили 48 відділень Національної служби охорони здоров'я, і ще 13 – в Шотландії [9].

Одним із наймасштабніших за наслідками було поширення вірусу NotPetya, який 27 червня 2017 р. атакував численні комп'ютерні системи українських державних і комерційних установ. «Загалом, за підрахунками спеціалістів Microsoft та ESET, кібератака зачепила щонайменше 65 країн. Проте встановлено, що першою й основною (якщо не єдиною) метою кібератаки була саме Україна. […] За попередніми підрахунками, у результаті атаки на території України станом на 7 липня 2017 р. було виведено з ладу до 10% приватних, урядових і корпоративних комп'ютерів» [12, с. 52-53].

Відповідно до Стратегії кібербезпеки України боротьба з кіберзлочинністю передбачає здійснення таких заходів:

1) створення ефективного і зручного контакт-центру для повідомлень про випадки кіберзлочинів та шахрайства у кіберпросторі, підвищення оперативності реагування на кіберзлочини правоохоронних органів, зокрема їх регіональних підрозділів;
2) удосконалення процесуальних механізмів щодо збирання доказів в електронній формі, що стосуються злочину,

удосконалення класифікації, методів, засобів і технологій ідентифікації та фіксації кіберзлочинів, проведення експертних досліджень;

3) запровадження блокування операторами та провайдерами телекомунікацій визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу) за рішенням суду;
4) упровадження схеми (протоколу) координації правоохоронних органів щодо боротьби з кіберзлочинністю;
5) підготовка суддів (слідчих суддів), слідчих та прокурорів для роботи з доказами, що стосуються злочину, отриманими в електронній формі, з урахуванням особливостей кіберзлочинів;
6) запровадження особливого порядку зняття інформації з каналів телекомунікацій у випадку розслідування кіберзлочинів.

Для протистояння кібератакам та їх знешкодженню, запобіганню інформаційним загрозам у 2007 році в Україні була створена CERT-UA (скор. від Computer Emergency Response Team of Ukraine – команда реагування на комп'ютерні надзвичайні події України) – спеціалізований структурний підрозділ Державного центру кіберзахисту та протидії кіберзагрозам (ДЦКЗ) Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку). Основна мета CERT-UA – забезпечити захист державних інформаційних ресурсів та інформаційних і телекомунікаційних систем від несанкціонованого доступу, неправомірного використання, а також порушень їх конфіденційності, цілісності та доступності. А беручи до уваги транскордонність кіберзагроз, передбачені також заходи, спрямовані на ліквідацію інцидентів інформаційної безпеки, які виникають в інформаційному кіберпросторі українського сегмента мережі Інтернет. Членство з 2009 року CERT-UA у FIRST (скор. від Forumfor Incident Responseand Security Teams – Форум команд реагування на інциденти інформаційної безпеки) дає змогу їй оперативно взаємодіяти з 307 командами реагування на комп'ютерні інциденти (CERT) з 67 країн світу [32].

Також у межах реалізації Стратегії кібербезпеки України в 2015 році сформовано Департамент кіберполіції як структурний підрозділ

Національної поліції України, що спеціалізується на попередженні, виявленні, припиненні та розкритті кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних інтернет-мереж і систем. Його здобутками, зокрема, є те, що в 2016 р. було виявлено та знешкоджено бот-мережу Mumblehard, керовану з території Російської Федерації, що займалася розсиланням спаму [1, с. 223].

Міжнародна співпраця для посилення кібербезпеки України. У 2008 році в рамках Спільної робочої групи України – НАТО з питань воєнної реформи за ініціативою Служби безпеки України було започатковано створення робочої підгрупи з питань кібернетичного захисту, що стало поштовхом для розробки концептуальних засад взаємодії між Україною та Північноатлантичним Альянсом у цій сфері, запровадження механізму консультацій та оперативного обміну інформацією в разі скоєння кібернетичних атак національного масштабу, розробки критеріїв оцінки кібернетичних загроз. У 2009 р. штаб-квартира НАТО затвердила стратегічний документ «Рамки співробітництва у питаннях кібернетичного захисту між НАТО та державами-партнерами», яким було закладено політико-правове підґрунтя для налагодження комплексної взаємодії та співробітництва із зацікавленими країнами-партнерами, зокрема й з Україною [17, с. 53].

На основі досягнутих домовленостей між Україною та НАТО було прийнято рішення про створення п'яти трастових фондів для України. Один із них спрямований на розвиток сучасних систем кіберзахисту відповідно до стандартів країн-членів НАТО, контрибуторами якого виступили Румунія, Естонія, Туреччина та Угорщина. Створення Трастового фонду Україна – НАТО з кібербезпеки полягає в можливості надавати Україні необхідну підтримку для розвитку оборонних технічних можливостей, зокрема створення лабораторій для розслідування інцидентів у кібернетичній сфері. Основним завданням діяльності Трастового фонду є створення сприятливих умов для підвищення технічних можливостей України у сфері забезпечення кібербезпеки протягом 24 місяців (постачання устаткування та обладнання, програмного забезпечення, технічної

допомоги, консультативних послуг, проведення навчальних тренінгів), при цьому загальний обсяг фінансування становить 815 тис. євро. У квітні 2015 р. Естонія виділила на діяльність трастового фонду НАТО для підтримки кібербезпеки в Україні 100 тис. євро, решту – інші країни Альянсу. Саме через систему цього Трастового фонду країни-члени НАТО надаватимуть підтримку Україні з метою розвитку її оборонних можливостей у галузі забезпечення кібернетичної безпеки [17, с. 53].

Попри певні успіхи міжнародної співпраці, пріоритетом зовнішньої політики України в аспекті кібербезпеки залишаються військово-технічне співробітництво з іноземними державами, поглиблення конструктивної співпраці з НАТО та ЄС з метою запозичення передового досвіду забезпечення кібербезпеки, результативності функціонування інституцій, які опікуються питаннями кіберзахисту, передусім з Трастовим фондом з кібербезпеки, Міжнародним центром кіберзахисту НАТО.

Завдання і запитання до параграфа

1. Випишіть з «Настанов з кібербезпеки від експертів», розроблених Бельгійським Відділенням Міжнародної Торгової Палати, Федерацією підприємств Бельгії, Ernst&Young, корпорацією Майкрософт, Бельгійським відділенням ISACA, асоціацією L-SEC та Бельгійським центром боротьби проти кіберзлочинності, основні принципи та необхідні заходи інформаційної безпеки.
2. Що таке кібербезпека і як це поняття співвідноситься з інформаційною безпекою?
3. Які є види кібератак і кіберконфліктів?
4. У чому полягає реалізація Стратегії кібербезпеки України?
5. Як кібервійна впливає на роботу журналіста?
6. Які завдання у сфері інформаційної безпеки виконують CERT-UA і Департамент кіберполіції?
7. Які міжнародні організації співпрацюють з Україною для посилення кібербезпеки?

Список використаної та рекомендованої літератури

1. Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2016 році» / Національний інститут стратегічних досліджень. – Київ : НІСД, 2016. – 688 с.
2. Богданов О. Перші кроки волонтерів інформаційних військ / О. Богданов, В. Мохор // Безпека інформації. – 2015. – Т. 21, № 1. – С. 100-103.
3. Бурячок В. Л. Стратегія оцінювання рівня захищеності держави від ризику стороннього кібернетичного впливу / В. Л. Бурячок, О. Г. Корченко, В. О. Хорошко, В. А. Кудінов // Захист інформації. – 2013. – Т. 15, № 1. – С. 5-14.
4. Виноградський О. Нова кіберстратегія США: плани і цілі [Електронний ресурс] / Олександр Виноградський // Defense Express. – Режим доступу : https://defence-ua.com/index.php/statti/2642-nova-kiberstratehiya-ssha-plany-i-tsili (дата звернення: 23.03.2018).
5. Впровадження європейської кібербезпеки: загальний огляд [Електронний ресурс] / ISACA ; пер. Київського відділення ISACA. – Режим доступу : http://www.isaca.org/Knowledge-Center/Research/Documents/European-Cybersecurity-Implementation-Overview_res_Ukr_1215.pdf (дата звернення: 18.03.2018).
6. Гнатюк В. Аналіз дефініцій поняття «інцидент» та його інтерпретація у кіберпросторі / В. Гнатюк // Безпека інформації. – 2013. – Т. 19, № 3. – С. 175-180. – Режим доступу : http://nbuv.gov.ua/UJRN/bezin_2013_19_3_7 (дата звернення: 28.04.2018).
7. Головка А. А. Захист кіберпростору як складова інформаційної безпеки України в умовах гібридної війни / А. А. Головка // Молодий вчений. – 2016. – № 4. – С. 333-336. – Режим доступу : http://nbuv.gov.ua/UJRN/molv_2016_4_83 (дата звернення: 02.05.2018).
8. Дубов Д. Геополітичне суперництво у кіберпросторі як чинник впливу на національну безпеку України : дис. … д-ра наук : спец. 21.01.01 – основи національної безпеки держави (політичні науки) / Д. Дубов ; Нац. ін-т стратегічних досліджень. – Київ, 2016. – 434 с.
9. Європол: загроза кібератаки посилюється [Електронний ресурс] // BBC. Україна : веб-сайт. – Режим доступу : http://www.bbc.com/ukrainian/news-39914971?ocid=socialflow_facebook (дата звернення: 20.04.2018).
10. Живило Є. О. Стратегія воєнної безпеки кіберпростору України / Є. О. Живило, О. О. Черноног, В. В. Машталір // Збірник наукових праць Військового інституту телекомунікацій та інформатизації. – 2016. – Вип. 1. – С. 41-52.
11. Заман А. Основи безпеки кібердіяльності / Асіф Заман // Куншт. – 2017. – № 6. – С. 15-18.
12. Інформаційна безпека та кібербезпека держави // Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2017 році» / Національний інститут стратегічних досліджень. – Київ : НІСД, 2017. – С. 47-56.

13. Кібервійна з Росією диктує нові правила для журналістів [Електронний ресурс] // Громадське радіо. – Режим доступу : https://hromadskeradio.org/programs/rankova-hvylya/kiberviyna-z-rosiyeyu-dyktuye-novi-pravyla-dlya-zhurnalistiv-mediaekspert (дата звернення: 01.04.2018).
14. Кібервійна: огляд найуспішніших публічних операцій Українського Кіберальянсу в 2016 році [Електронний ресурс]. – Режим доступу : https://informnapalm.org/ua/cyberwar-2016 (дата звернення: 10.05.2018).
15. Косогов О. М. Сучасна політика безпеки кіберпростору в умовах його мілітаризації / О. М. Косогов, А. О. Сірик // Сучасні інформаційні технології у сфері безпеки та оборони. – 2015. – № 3. – С. 181-186.
16. Лук'янчикова В. Ю. Кіберпростір: загрози для міжнародних відносин та глобальної безпеки / В. Ю. Лук'янчикова // Гілея. – 2013. – № 72. – С. 793-796.
17. Лук'янчук Р. В. Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети / Р. В. Лук'янчук // Вісник Національної академії державного управління при Президентові України. Серія: Державне управління. – 2015. – № 4. – С. 50-56.
18. Марков В. В. Про механізми скоєння злочинів у кіберпросторі та особливості їх кваліфікації / В. В. Марков // Південноукраїнський правничий часопис. – 2013. – № 1. – С. 112-115.
19. Матвєєва О. В. Кіберпростір як місце зіткнення суспільних інтересів / О. В. Матвєєва // Актуальні проблеми міжнародних відносин. – 2012. – Вип. 104(1). – С. 248-251.
20. Медведєва О. Кіберпростір як сфера діяльності розвідувальних служб / О. Медведєва // Актуальні проблеми міжнародних відносин. – 2011. – Вип. 98(2). – С. 116-117. – Режим доступу : http://nbuv.gov.ua/UJRN/apmv_2011_98(2)_47 (дата звернення: 14.03.2018).
21. Настанови з кібербезпеки від експертів [Електронний ресурс] / Бельгійське Відділення Міжнародної Торгової Палати, Федерація підприємств Бельгії та ін. ; пер. Київського відділення ISACA, Microsoft Україна. – Режим доступу : http://www.isaca.org.ua/index.php/press-center/news/191-translation-of-guidelines-on-cybersecurity (дата звернення: 30.03.2018).
22. Піддубна Л. В. Кіберпростір як соціокультурний фактор мережевого суспільства / Л. В. Піддубна // Гілея. – 2016. – Вип. 105. – С. 204-207.
23. Почепцов Г. Сучасні інформаційні війни / Г. Почепцов. – 2-ге вид., допов. – Київ : Вид. дім «Києво-Могилянська академія», 2016. – 504 с.
24. Про основні засади забезпечення кібербезпеки України : Закон України / Верховна Рада України // Відомості Верховної Ради. – 2017.– № 45.– С. 42-57.
25. Рибка С. В. Кіберпростір, управління інфраструктурою, кібербезпека / С. В. Рибка, Є. В. Кільчицький, О. М. Післегін // Стратегічна панорама. – 2015. – № 1. – С. 126-134.
26. Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експертів [Електронний ресурс] / Н. Тарасенко // Центр досліджень соціальних комунікацій НБУВ : веб-сайт. – Режим доступу : http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2759:doktrina-informatsijnoji-

bezpeki-yak-zasib-protidiji-informatsijnim-zagrozam&catid=8& Itemid=350 (дата звернення: 25.04.2018).
27. Доктрина національної безпеки України. Затверджено Указом Президента України № 47/2017 від 25 лютого 2017 року // Офіційне інтернет-представництво Президента України : веб-сайт. – Режим доступу : http://www. president.gov.ua/documents/472017-21374 (дата звернення: 14.04.2018).
28. Указ Президента України №96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс] // Офіційне інтернет-представництво Президента України : веб-сайт. – Режим доступу : http://www.president.gov.ua/documents/962016-19836 (дата звернення: 16.03.2018).
29. Україна – полігон для хакерів: Як Росія пише нові правила кібервійни [Електронний ресурс]. – Режим доступу : https://ua.112.ua/statji/ukraina--polihon-dlia-khakeriv-yak-rosiia-pyshe-novi-pravyla-kiberviiny-379318.html (дата звернення: 05.05.2018).
30. Фахівці США в Києві шукають «російський слід» Black Energy : [Електронний ресурс]. – Режим доступу : https://www.ukrinform.ua/rubric-technology/1954993-fahivci-ssa-v-kievi-sukaut-rosijskij-slid-black-energy.html (дата звернення: 03.04.2018).
31. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності / В. М. Фурашев // Інформація і право. – 2012. – № 2. – С. 162-169.
32. Computer Emergency Response Teamof Ukraine [Електронний ресурс] : веб-сайт. – Режим доступу : http://cert.gov.ua (дата звернення: 27.03.2018).
33. Joseph S. Nye, Jr. CyberPower / Joseph S. Nye, Jr. ; Belfer Centerfor Scienceand International Affairs, Harvard Kennedy School. – Cambridge, MA, 2010. – 24 c.

Автор параграфа:
канд. філол. н., ст. викладач каф. журналістики
НПУ імені М. П. Драгоманова
Юлія Полтавець

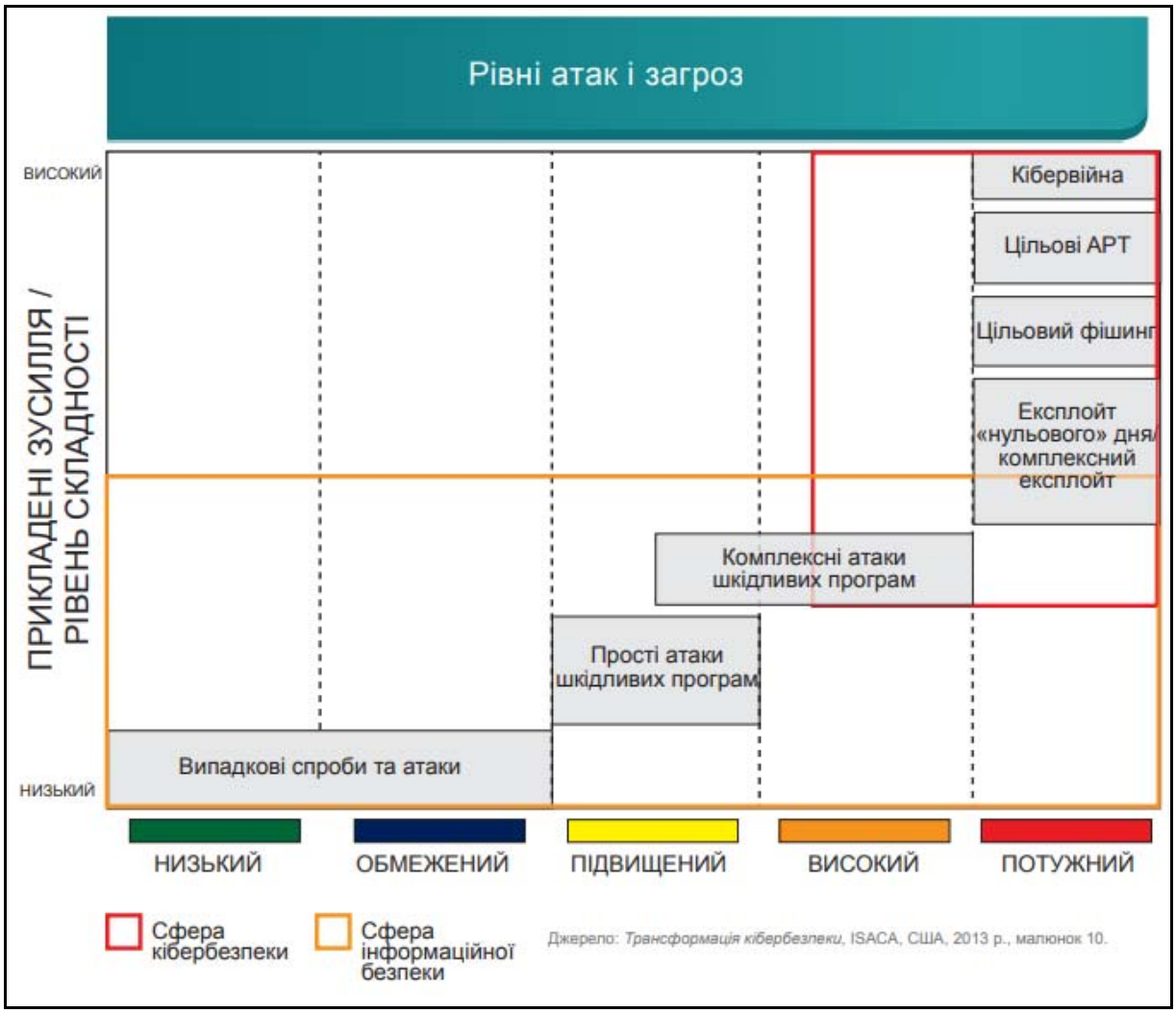
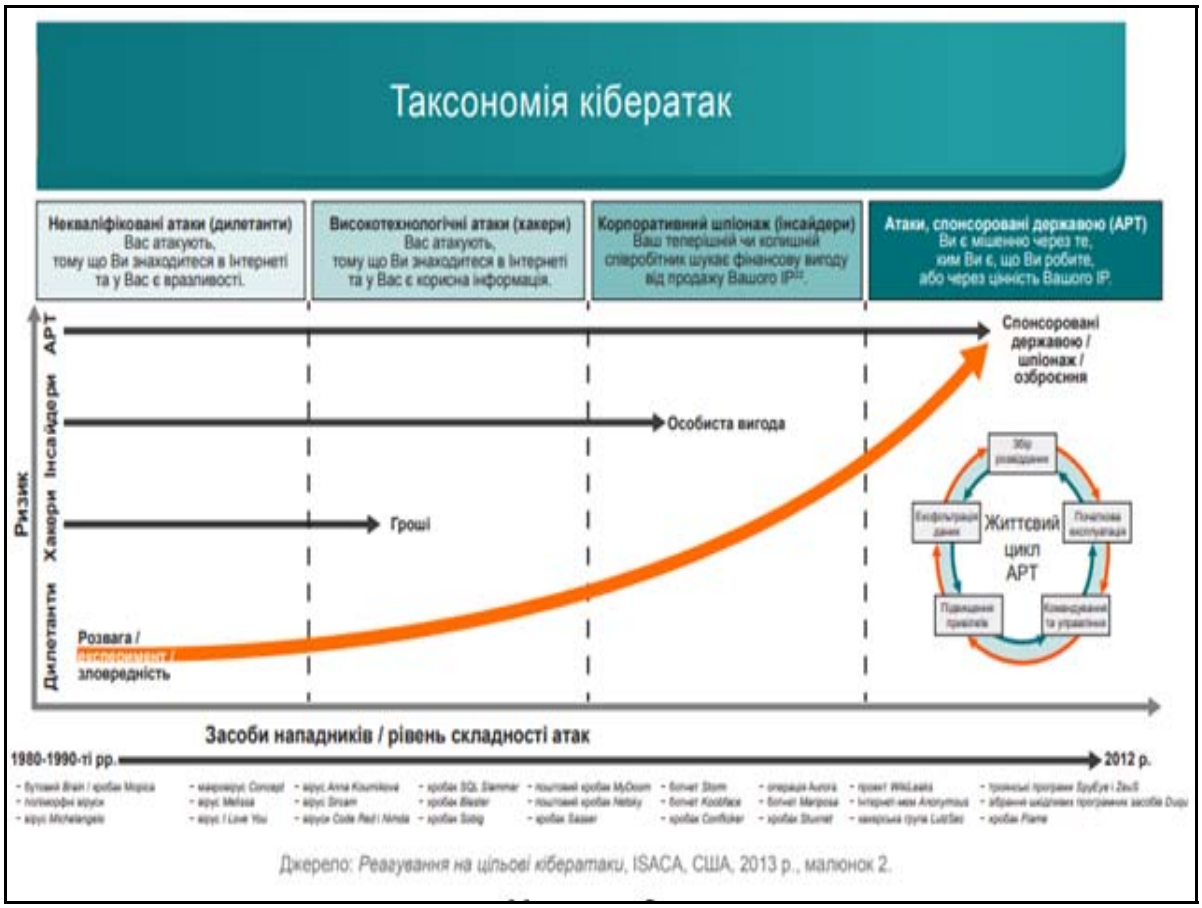


Рисунок 10.1. ***Оцінювання рівня загроз кібербезпеці залежно від кількості й характеристик кібератак***



Джерело: *Реагування на цільові кібератаки*, ISACA, США, 2013 р., малюнок 2.

Рисунок 10.2. ***Залежність ризиків від мети кібератак і характеристик агресора***

ГІБРИДНА ВІЙНА І ЖУРНАЛІСТИКА

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ
імені М. П. ДРАГОМАНОВА

ГІБРИДНА ВІЙНА І ЖУРНАЛІСТИКА

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Навчальний посібник

Київ
Вид-во НПУ імені М. П. Драгоманова
2018

УДК 070:355.01-025.26(07)
Г 46

Рекомендовано Вченою радою
Національного педагогічного університету імені М. П. Драгоманова
(протокол № 14 від 26 червня 2018)

За загальною редакцією
доктора філософських наук, професора кафедри журналістики
НПУ ім. М. П. Драгоманова, академіка НА вищої освіти України
В. О. Жадька

Рецензенти: ***Іван Васильович Крупський***, доктор історичних наук, професор, завідувач кафедри теорії і практики журналістики Львівського національного університету імені І. Франка;
Ірина Миколаївна Жиленкова, доктор історичних наук, професор кафедри історії та етнополітики Національного педагогічного університету імені М. П. Драгоманова.

Авторський колектив:
В. О. Жадько, О. І. Клименко, П. П. Куляс, О. Т. Марків, Ю. С. Полтавець, О. І. Харитоненко, О. В. Харчук, С. В. Шевчук.

Ілюстрація на обкладинці:
Ф. В. Сергеєв

Г 46 **Гібридна війна і журналістика. Проблеми інформаційної безпеки** : навчальний посібник / за заг. ред. В. О. Жадька ; ред.-упор. : О. І. Харитоненко, Ю. С. Полтавець. – Київ : Вид-во НПУ імені М. П. Драгоманова, 2018. – 356 с.

ISBN 978-966-931-181-8

Підготовлений викладачами кафедри журналістики НПУ імені М. П. Драгоманова посібник присвячено питанням інформаційної безпеки, діяльності журналіста в умовах гібридної війни, проблемам медіаосвіти. У книзі чотири розділи, що висвітлюють суть та складові сучасних гібридних протистоянь, їхній інформаційний, інформаційно-психологічний, семантичний, технологічний та силовий аспекти. Видання доповнене термінологічним словником. Посібник призначений для студентів спеціальності «Журналістика», а також для всіх, хто прагне навчитися критично оцінювати й аналізувати медіаповідомлення та інформацію загалом.

ISBN 978-966-931-181-8

УДК 070:355.01-025.26(07)

© Авторський колектив, 2018
© Сергеєв Ф. В., обкладинка, 2018
© Вид-во НПУ імені М. П. Драгоманова, 2018

ЗМІСТ

РОЗДІЛ 4
МЕДІАОСВІТА ЯК ФУНДАМЕНТАЛЬНА СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Навчальне видання

ГІБРИДНА ВІЙНА І ЖУРНАЛІСТИКА

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Навчальний посібник

За загальною редакцією
доктора філософських наук, професора кафедри журналістики
НПУ ім. М. П. Драгоманова, академіка НА вищої освіти України
В. О. Жадька

Авторський колектив:
Жадько Віктор Олексійович, док. філос. н., проф., зав. каф. журналістики НПУ імені М. П. Драгоманова (§ 2 «Інформаційні війни в історії та сучасності: характерні ознаки новітніх протистоянь»)
Клименко Олександр Іванович, ас. каф. журналістики (§ 3 «Технології маніпулювання і методики пошуку, відбору, верифікації даних у журналістиці»)
Куляс Павло Петрович, канд. іст. н., доц. каф. журналістики (вступ «Гібридні війни в сучасному світі. Що про них повинен знати журналіст і редактор?»)
Марків Олександра Тимофіївна, канд. педагог. н., доц. каф. журналістики (§ 9 «Інформаційні й психологічні операції: поняття, види, способи використання в умовах гібридної війни»; § 12 «Роль медіаграмотності в професійному та особистісному становленні людини інформаційної епохи»; § 13 «Формування в майбутніх журналістів культури роботи з інформацією в умовах гібридної війни»)
Полтавець Юлія Сергіївна, канд. філол. н., ст. викл. каф. журналістики (§ 4 «Фактчекінг у роботі сучасного журналіста – дієвий спосіб протистояння інформаційним загрозам»; §10 «Інформаційно-технологічні атаки і способи захисту кіберпростору: новітні тактики гібридних війн»)
Харитоненко Олена Іванівна, канд. філол. н., доцент каф. журналістики (§ 1 «Визначення, види, актуальні напрямки дослідження інформаційних війн» – у співавторстві; розділ 2 «Смислові війни в межах гібридних протистоянь»)
Харчук Олена Василівна, канд. філол. н., доцент каф. журналістики (§ 1 «Визначення, види, актуальні напрямки дослідження інформаційних війн» – у співавторстві)
Шевчук Світлана Вікторівна, ас. каф. журналістики (§ 11 «Особливості роботи журналіста в зонах військових конфліктів»; § 14 «Світові та вітчизняні тенденції розвитку медіаосвіти»)

Технічний редактор – *Т. С. Меркулова*
Макетування – *Т. М. Ветраченко*
Обкладинка – *Ф. В. Сергеєв*

ВИДАВНИЦТВО
НАЦІОНАЛЬНОГО ПЕДАГОГІЧНОГО УНІВЕРСИТЕТУ
ІМЕНІ М. П. ДРАГОМАНОВА

Підписано до друку *26 червня* 2018 р.
Формат 60x84/16. Папір офісний. Гарнітура Times New Roman.
Ум. др. арк. 22,25. Об.-вид. арк. 17,75.
Наклад 300 прим. Зам. № 397
Віддруковано з оригіналів

Видавництво Національного педагогічного університету
імені М. П. Драгоманова. 01601, м. Київ-30, вул. Пирогова, 9.
Свідоцтво про реєстрацію ДК № 1101 від 29.10.2002 (044) 234-75-87
Віддруковано в друкарні Національного педагогічного університету
імені М. П. Драгоманова (044) 239-30-26