УДК 32.019.51

Олена Бондаренко

***Бондаренко Олена**, доцент, кандидат психологічних наук, доцент кафедри міжнародних відносин і туризму*
Хмельницький національний університет (Україна, Хмельницький)
elenaivbond@gmail.com

***Bondarenko Olena**, Ph.D., Assoc. Prof. at the Department of international information and regional geography*
Khmelnytsky National University (Ukraine, Khmelnytskyi)
elenaivbond@gmail.com

Аналіз загроз безпеці розвитку країн крізь призму кіберзлочинності

Анотація. У статті зроблений аналіз загроз безпеці розвитку країн крізь призму кіберзлочинності. Для вирішення поставленої мети були використані наступні методи дослідження: інформаційно-пошуковий, статистичний, порівняльний, системний аналіз, регресійне моделювання. У статті проаналізовані статистичні дані дванадцяти показників, які розкривають загрози безпеці розвитку країн, проаналізована їх динаміка. Було встановлено, що ззлочинність в інформаційній сфері чинить суттєві перешкоди для розвитку країн. Серед найбільш небезпечних напрямків кіберзлочинності для розвитку країн є атаки на інфраструктуру, руйнування роботи підприємств, державних установ, кібершпигунство, а також прямі економічні збитки через різного роду шахрайства, здирництва, компрометацію даних. Встановлено, що у 2017 р. найбільше постраждав глобальний сектор фінансових послуг. Сьогодні провідними шкідливими загрозами стали кіберздирництво та банківські троянські програми. Протягом 2015-2016 рр. на сектор послуг доводилося 38% глобальних здирницьких вірусів, виробництво посіло друге місце з 17%. Серед різних галузей, що зазнали кіберздирництва, освіта мала найбільшу частку серед підприємств, які несли втрати через вимагання викупу. Роздрібна торгівля мала лише 16% всіх нападів з викупом. Кібератаки постійно здійснюються і на державні органи влади. Більшою мірою ці атаки переслідують не мету стягнення коштів, а порушення нормальної роботи установи, дестабілізацію в наданні послуг. У роботі зроблений прогноз рівня уразливостей та ризиків ІТ безпеці у світі. За реалістичним сценарієм прогнозування максимальний рівень уразливостей та ризиків ІТ безпеці у світі у 2019 р. складатиме 11,75 тис. випадків, що відповідає зменшенню на 20,1% порівняно з 2017 р. Аналіз показав, що розвиток світової спільноти на даний час неможливий без розвитку ІКТ та мережевих технологій, однак з таким розвитком зростає і рівень загроз від злочинності в інформаційній сфері.

Ключові слова: кібербезпека; кіберздирництва; злочинність в інформаційній сфері; напади з викупом; економічні збитки.

Постановка наукової проблеми та її значення. У сучасному світі спостерігається інтенсивний процес розвитку, поширення і впровадження різних інформаційно-комунікаційних технологій в усі сфери діяльності людини, суспільства і держави. Рівень розвитку національної інформаційної інфраструктури впливає на

оборонний і політичний потенціал держав і є одним з ключових чинників зростання і підвищення конкурентоспроможності на світовій арені. Проникнення ІКТ в усі сфери життєдіяльності виявило значний вплив на всю систему сучасних міжнародних відносин. Багато країн світу потребують прискорення розвитку важливих індикаторів в сфері кібербезпеки, підвищенні ефективності кіберпростору. Вирішення проблеми вимагає впровадження комплексу організаційно-технічних заходів і процедур в системі світового кіберпростору з урахуванням негативних чинників вразливості механізмів безпеки. Забезпечення міжнародної безпеки у світовому кіберпросторі вимагає не тільки зусиль окремих країн світу, але і розробку і здійснення максимально ефективних міжнародних інструментів. Тому всі економічні і політичні ресурси з протидії загрозам повинні розглядатися спільними зусиллями міжнародного співтовариства. Таким чином, забезпечення кібербезпеки стає глобальною проблемою людства. Тому визначення тенденцій глобальних загроз у міжнародному інформаційному просторі є актуальним для розробки і здійснення превентивних заходів проти кібератак і кіберзлочинів. **Мета** дослідження: аналіз сучасного стану загроз безпеці розвитку країн крізь призму злочинності в інформаційній сфері. **Методологічна база дослідження**: інформаційно-пошуковий метод, статистичний, порівняльний, системний аналізи, регресійне моделювання.

Особливості ІКТ та актуальні тенденції їх розвитку з політологічної точки зору досліджують такі автори як М. Кастельс, К. Кукьер і В. Майер-Шедбергер. Аналізу процесів глобальної інформатизації у контексті права присвячені роботи Бачило І.Л., Наумова В. Б., Серго А. Г., М. Фрумкіна, Д. Курбаль, Д. Менте, Л. Лессига, С. Раушера, Л. Грінберга, С. Гудмана, К. Суху. Проблематика міжнародного управління Інтернетом у дослідженнях і дипломатичній риториці більшості держав сьогодні пов'язана із забезпеченням інформаційної безпеки. Серед робіт, присвячених міжнародним політичним аспектам управління Інтернетом слід зазначити монографію І. Курбаль і Е. Гелбстайна, збірники статей під редакцією Д. Макліна і В. Кляйнвехтера, а також наукові праці В. Даттона, Д. Дрезнера, Д. Макліна, М. Пельтьє, Д. Хоффмана. Крім того, аналізом процесів управління Інтернетом з позицій теорії міжнародних режимів займаються як М. Франда, Д. Когбурн, М. Мюллер, Д. Матіасон і Х. Кляйн. Питання забезпечення безпеки критичних інформаційних інфраструктур досліджують Коротков А.В., Кононов О.О., Черешкін Д.С., Васенін Д.А. Серед зарубіжних видань в цій сфері найбільш авторитетним є щорічна Хрестоматія з питань захисту критичних інфраструктур, редакторами якої виступають А. Вегнер, В. Мауер, М. Кавелті.

Виклад основного матеріалу й обґрунтування результатів дослідження. Разом з позитивними наслідками впровадження ІКТ у всіх сферах розвитку країни виникають проблеми безпекового виміру. Так, кількість поширених уразливостей і ризиків безпеки ІТ, виявлених у світі в період з 2009 по 2017 рік постійно зростає. За останній рік було виявлено 14712 нових загальних уразливостей і ризиків ІТ, що в два рази більше, ніж у попередньому році - 6447 таких уразливостей (рис. 1).

Суми збитку, заподіяного кіберзлочинністю за повідомленням IC3 (США) з 2001 по 2016 рік зростала практично з однаковим щорічним приростом (рис. 1). За останній звітний період – 2016 р. щорічні втрати від кіберзлочинів за оцінкою IC3 склали 1,33 млрд. дол., у порівнянні з 781,84 млн. дол. у 2013 р. Найбільші наслідки кібератаки для глобальних компаній у 2016 р. були втратами, викликаними збоєм бізнесу і втратою інформації. Цього року більшість інцидентів з порушеннями даних були пов'язані з крадіжкою особистих даних, за якими слідували фінансові та облікові дані.

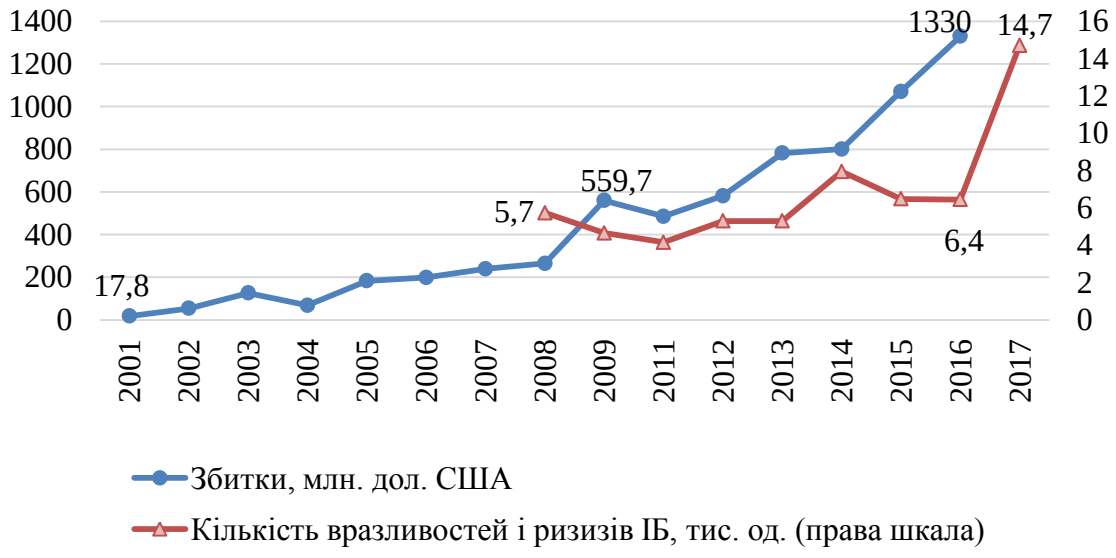

Рис. 1. Кількість поширених уразливостей і ризиків ІТ-безпеки у світі та сума грошового збитку від кіберзлочинності [1, 2]

Витрати, які несуть компанії від кіберзлочину, високі для сектору фінансових послуг. У табл.1 представлені середні річні витрати, викликані кіберзлочинністю по всьому світу станом на серпень 2017 р., відсортовані за галуззю. У 2017 р. найбільше постраждав глобальний сектор фінансових послуг, де через кіберзлочинність середній річний збиток склав 18,28 млн. дол.

Таблиця 1

Середньорічні витрати від глобальної кіберзлочинності

за серпень 2017 р. у промисловості (в млн. дол. США) [3]

Сектор	Середньорічні витрати	Сектор	Середньорічні витрати
Фінансові послуги	18,28	Державний сектор	8,28
Комунальні та енергетичні ресурси	17,2	Перевезення	7,36
Аерокосмічна та оборонна	14,46	Споживацькі товари	7,34
Технологія та програмне забезпечення	13,17	Зв'язок	7,1
Охорона здоров'я	12,47	Наук про життя	6,47
Послуги	11,05	Освіта	5,07
Промислове виробництво	10,22	Готелі	5,04
Роздрібна торгівля	9,3		

Другим за рівнем збитків від кіберзлочинності після сектору фінансових послуг є комунальні та енергетичні ресурси. Це є достатньо небезпечно, оскільки зупинка цього сектору може спричинити колапс у країні.

Однією з головних причин таких збитків експерти називають проблему компрометування, порушення даних. Йдеться про викрадення особистих даних, у тому числі облікових даних, паролів. Порушення даних все більше впливає на ціни акцій, у тому числі майже на половину відсотка зниження частки компаній у наслідок порушення даних [4]. Як видно з даних, наведених компанією Gemalto, світового лідера в сфері цифрової безпеки, найбільша кількість інцидентів з 2013 по 2017 р. припадала на крадіжку особистих даних (рис. 2).

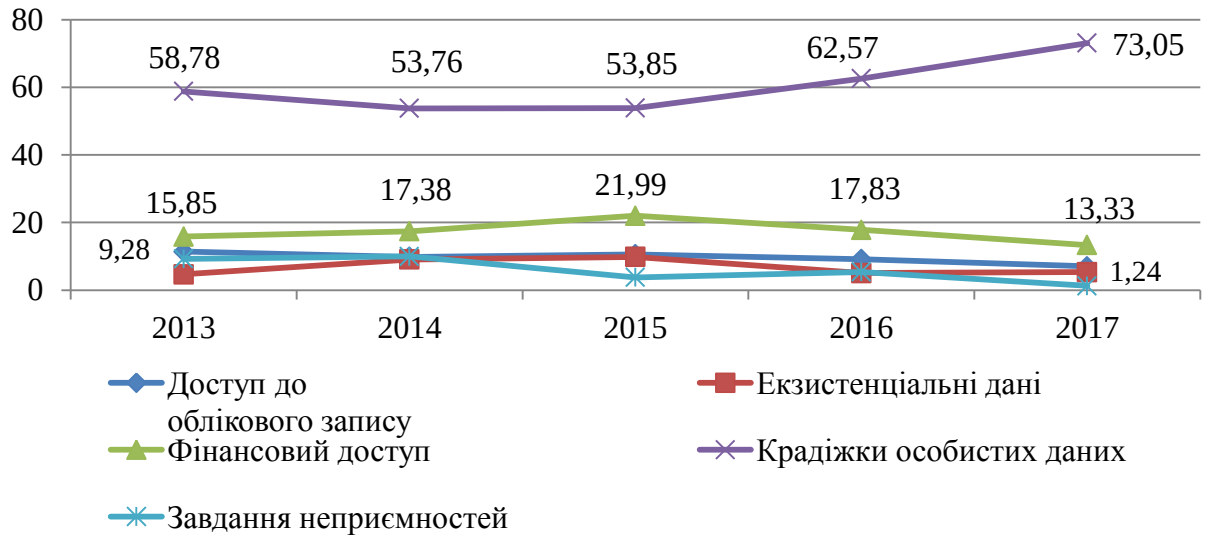

Рис. 2. Динаміка поширення глобальних інцидентів з порушеннями даних проти організацій у 2013 – 2017 рр. за типом, % [5]

Згідно даних Gemalto у першій половині 2017 р. 918 витоків привели до того, що було скомпрометовано 1,9 млрд. записів по всьому світу. У порівнянні з другим півріччям 2016 р. кількість загублених, вкрадених або скомпрометованих записів збільшилася на 164%. Більша частина даних була вкрадена внаслідок найбільш масштабних витоків, які налічують 22 випадки, кожен з яких привів до більш ніж мільйону скомпрометованих записів даних.

З 918 витоків більш ніж у 500 випадках (59% від усіх прецедентів) кількість скомпрометованих записів залишилася невідомим або не було зафіксовано [6]. Протягом першого півріччя 2017 р. основним типом витоків було розкрадання ідентифікаційних даних, яке становило 73% всіх витоків, що на 49% більше, ніж в минулому півріччі. Кількість скомпрометованих даних в результаті розкрадання ідентифікаційних даних збільшилася на 255%.

Велика частина витоків даних (74%), що відображає зростання випадків на 23%, сталася внаслідок злочинних дій (рис. 2.13). Однак на це джерело припадає лише 13% всіх вкрадених, загублених або скомпрометованих записів даних. Внутрішні атаки зловмисників становлять лише 9% від всіх витоків, а кількість скомпрометованих записів з 500 тис. збільшилася до 20 млн., що перевищує показник минулого півріччя більш ніж на 4114%.

У більшості підприємств, що відслідковуються компанією Gemalto, кількість скомпрометованих, вкрадених або загублених записів даних збільшилася більш ніж на 100% (рис.3). У сфері освіти був зафіксований один з найбільших показників зростання витоків (103%) зі збільшенням кількості скомпрометованих записів більш ніж на 4000%. Це є результатом внутрішніх атак зловмисників, які скомпрометували мільйони записів у найбільшій приватній освітніх компанії Китаю. У сфері охорони здоров'я спостерігався схожий показник витоків даних у порівнянні з другим півріччям 2016 р., кількість вкрадених, скомпрометованих або загублених записів збільшилася до 423%. У числі п'яти об'єктів, які найбільше постраждали від масштабних витоків даних за перше півріччя, знаходиться Національна служба охорони здоров'я Великобританії, де число скомпрометованих записів перевищує 26 мільйонів.

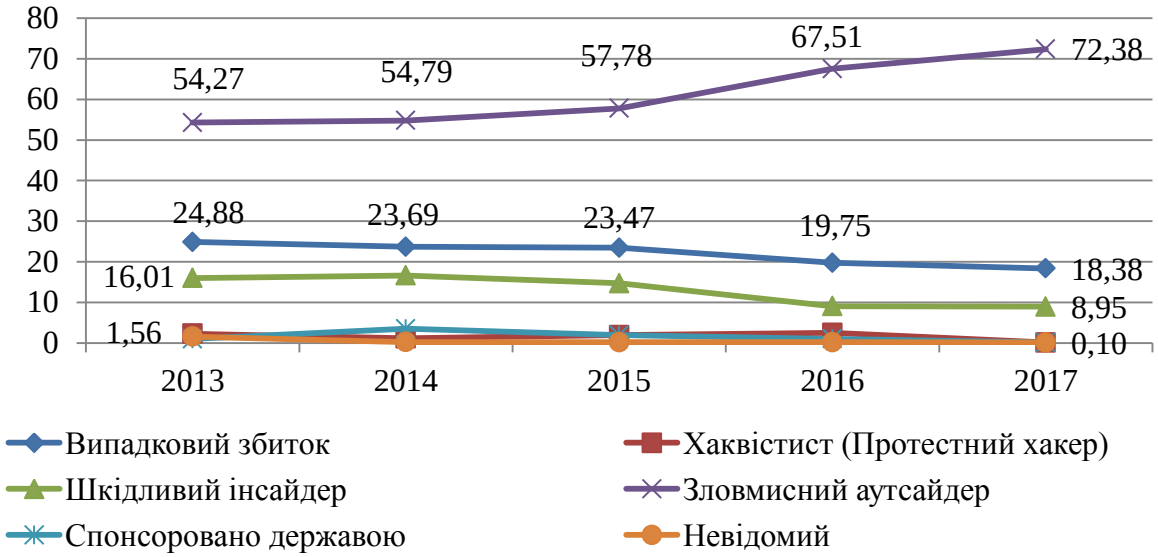

Рис. 3. Розподіл випадків порушень даних проти організацій у 2013 – 2017 рр. за джерелом [5]

У фінансовій сфері, урядовому секторі і сфері розваг також спостерігалося значне збільшення кількості витоків записів даних. За перше півріччя 2017 р. у сфері розваг було зафіксовано на 220% більше випадків витоків записів даних (рис.4).

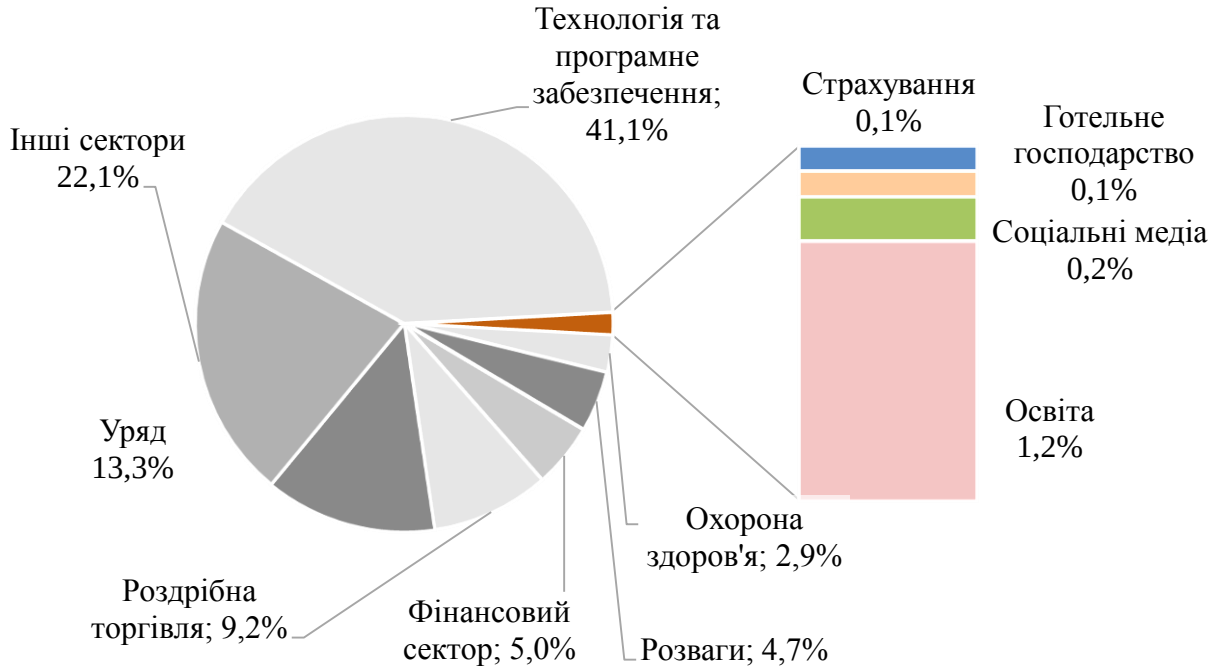

Рис. 4. Розподіл записів даних, викрадених або втрачених промисловістю у 2013 – 2017 рр. [5]

Компанії, що розробляють рішення для IT безпеки, стверджують, що кількість унікальних шкідливих програм, які були виявлені вперше з 2014 р. по 2016 р. зростає. В останній звітний період було виявлено 357 млн. нових варіантів шкідливого ПЗ в порівнянні з 355 млн. варіантів шкідливого ПЗ у 2015 р. і 274 млн. у 2014 р.[7]. У табл. 2 представлені типи кіберзлочинності з найбільшою кількістю втрат потерпілих у 2016 р. Протягом звітного періоду онлайн-шахрайство з довірою становило 219,8 млн. дол.

Таблиця 2

Типи кіберзлочинності з найбільшою кількістю втрат потерпілих у 2016 р. (в млн. дол. США) [8]

Тип кіберзлочину	Обсяг втрат
BEC / EAC (шахрайство, орієнтоване на підприємства, від невеликих до великих корпорацій)	360,51
Шахрайство / Романтика	219,81
Несплата / Не доставка	138,23
Інвестиції	123,41
Порушення корпоративних даних	95,87
Інший	73,09
Розширений платіж	60,48
Порушення особистих даних	59,14
Крадіжки особистих даних	58,2
Громадянські справи	57,69

Небезпечним трендом розвитку кіберзлочинності є атаки на інфраструктуру країни. Такі атаки часто переходять до терористичних дій. Зловживання технологіями та законними онлайновими інструментами та службами не є винятком у ландшафті тероризму. Терористи стають дедалі більш розумними, ховаючи свої сліди та дії, використовуючи анонімні інструменти та служби шифрування. Крім того, анонімність, надана криптовалютами, і їх переважне використання в торгівлях, що відбуваються на «темних» ринках, підтримується терористами, які інвестують у цю валюту. Товари та послуги, пропоновані на Darknet, такі як Tor, доступні різним групам акторів, включаючи терористичні групи. Це варіанти від шкідливого програмного забезпечення до незаконних товарів, таких як викрадення зброї, до переповнення сайтів (DDoS-атаки), що стають інструментами терористичних груп.

Терористичні угруповання широко використовують соціальні медіа-платформи для участі в кадрових кампаніях, пропаганди, підбурюванні терористичних актів та відповідальності за напади. Соціальні медіа були ключем до пропаганди деяких терористичних груп, вони використовуються для розповсюдження своїх цілей та

досягнень, і, часто, є вирішальними у процесі радикалізації та саморадикалізації. Цей процес важко контролювати, навіть коли платформи швидко видаляють вміст через швидкість та простоту розповсюдження інформації в Інтернеті. Деякі правоохоронні органи відзначають, що зростаюча тенденція процесу саморадикалізації, можливо, є результатом швидкого та легкого доступу до онлайн-пропаганди.

Розподіл регіонів за кількістю кібератак є достатньо нерівномірним (табл.3). Протягом 2016 р. було виявлено, що у Північній Америці відбулося 49% всіх випадків кібератак.

Таблиця 3

Географічне розташування постраждалих від шкідливих даних у 2016 р. за кількістю атак [9]

Регіон	Частка кібер-атак
Північна Америка	49%
Азіатсько-Тихоокеанський регіон	21%
Європа, Близький Схід та Африка	20%
Латинська Америка та Карибський басейн	10%

Фактично, багато компаній, які займаються безпекою Інтернет, постійно вказують на людський фактор як найслабший ланцюжок кібербезпеки. Вплив людей на дії проти власних інтересів або інтересів організації часто є простим рішенням, ніж вдавання до зловмисного програмного забезпечення чи злом. Як правоохоронна, так і фінансова індустрія вказують на те, що соціальна інженерія продовжує надавати можливість зловмисникам, які не мають технічних навичок, мотивації використовувати людей або ресурси найму. Крім того, цілеспрямована соціальна інженерія дозволяє тим, хто технічно обдарований, організувати змішані атаки, минаючи як людські, так і апаратні або програмні лінії оборони.

Більшість основних загроз ІБ залишаються незмінними. Однак, сьогодні провідними шкідливими загрозами стали кіберздирництво (Ransomware, наприклад, «WannaCry», «Bad Rabbit», «Petya») та банківські троянські програми. Дані компанії Symantec показують, що за останні роки майже кожен промисловий сектор постраждав від викупу. Однак деякі типи компаній більш уразливі або частіше піддаються нападкам кіберзлочинців, які намагаються вимагати гроші за дані, ніж інші. Аналіз показує, що сектор послуг був найбільше зачепленим кіберздирництвом у 2016 р. (рис. 5). Протягом 2015-2016 рр. на сектор послуг доводилося 38% глобальних здирницьких вірусів. Виробництво посіло друге місце з 17% вірусів.

Рис. 5. Поширення кіберздирництва у світі з січня 2015 р. по квітень 2016 р. за галузями [10]

Протягом 2016 р. освіта мала найбільшу частку серед підприємств, які зазнали нападу з допомогою викупу (рис. 6). Роздрібна торгівля мала 16% всіх нападів з викупом.

Більшість потерпілих були в Росії, але напади також спостерігалися в Україні, Туреччині та Німеччині. Фірма з кібербезпеки ESET також виявила випадки «Bad Rabbit» в Японії та Болгарії. Інша компанія, Avast, додає до цього списку США, Південну Корею та Польщу [12].

Згідно з даними, наданими інститутом AV-Test IT-безпеки, здирницькі програми (наприклад, «WannaCry» і «Petya») становлять лише невелику частку всіх шкідливих програм, виявлених у всьому світі [13]. Однак це просто показує, що кількість зразків певного виду шкідливого ПЗ не відображає його фактичного потенціалу для пошкодження.

Рис. 6. Галузі промисловості з найбільшою часткою серед підприємств, які зазнали кібернападів з викупом в 2016 р. [11]

Середній обсяг викупу, який повинен був бути виплачений клієнтами MSP (Сервіс-провайдери) після атак в другому кварталі 2017 р. коливався від 10 до 20000 дол. Згідно з опитуванням, 47% Сервіс-провайдерів (MSP) заявили, що їм було запропоновано заплатити середню суму викупу від 500 до 2000 доларів [14], суму у $100 - $500 виплатили 25%, на найвищий викуп - $20,000+ припадало тільки 1% потерпілих.

Серед кіберзлочинних нападів на сектор критичної інфраструктури (СКІ) у 2016 р. телекомунікації були головним сектором уваги злочинців. Сектор телекомунікацій був джерелом найбільш шкідливої діяльності у 2016 р., що становить 89,6 % нападів та 98,1 % вихідних IP-адрес, що надходять з мереж СКІ (табл. 4).

Таблиця 4

Галузі промисловості, які зазнали кібератаки на сектор критичної інфраструктури у 2016 р. [15]

Галузь промисловості	% активності джерела CIP	% IP-адрес джерела CIP

Телекомунікації	89,6%	98,1%
Повітряний транспорт	5,5%	0,0%
Виконавча, законодавча та інша державна гілка	1,9%	0,5%
Фінанси та страхування	1,2%	0,3%
Виробництво комп'ютерних та електронних виробів	0,4%	0,2%
Страхові компанії та пов'язана з ними діяльність	0,3%	0,2%
Амбулаторні послуги охорони здоров'я	0,3%	0,1%
Виробництво транспортного обладнання	0,2%	0,1%

Кібератаки постійно здійснюються і на державні органи влади. Більшою мірою ці атаки переслідують не мету стягнення коштів, а порушення нормальної роботи установи, дестабілізацію в наданні послуг тощо. Достатньо поширеним видом таких атак є розсилка спаму через електронну пошту. Так, наприклад у 2016 р. серед вього потоку електронної пошти, яка надходила до Державного департаменту США (U.S. Department of State) на спам припадало 51,6% всіх листів, на Міністерство фінансів США / Департамент казначейства США (United States Department of the Treasury) - 52,2%, на Департамент охорони здоров'я та соціальних служб США (The U.S. Department of Health and Human Services) - 50,1%. В цілому рівень атак на державні органи влади у США зростає з кожним роком (рис. 7).

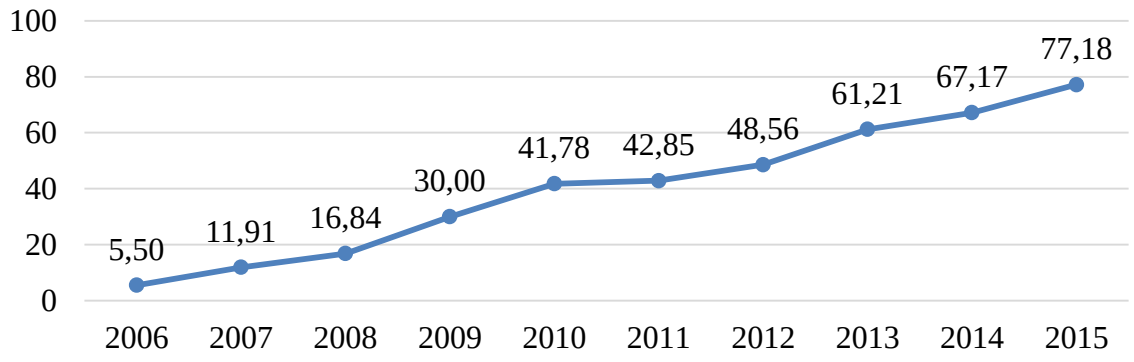

Рис.7. Кількість інцидентів, пов'язаних з порушенням кібербезпеки федеральних агентств у США, з 2006 по 2015 р., тис. випадків [16]

Окремі атаки на органи державної влади, військові організації, провідні компанії крім отримання безпосередньо від жертви коштів або дестабілізації їхньої роботи, направлені на викрадення секретної інформації, результатів наукових розробок. На рис. 8 представлена інформація про поширення кібершпигунства в окремих країнах-жертвах у світі у 2013 р. При загальній частці 54% в США у 2013 р. спостерігався найвищий

рівень кібершпигунства серед обраних країн-жертв.

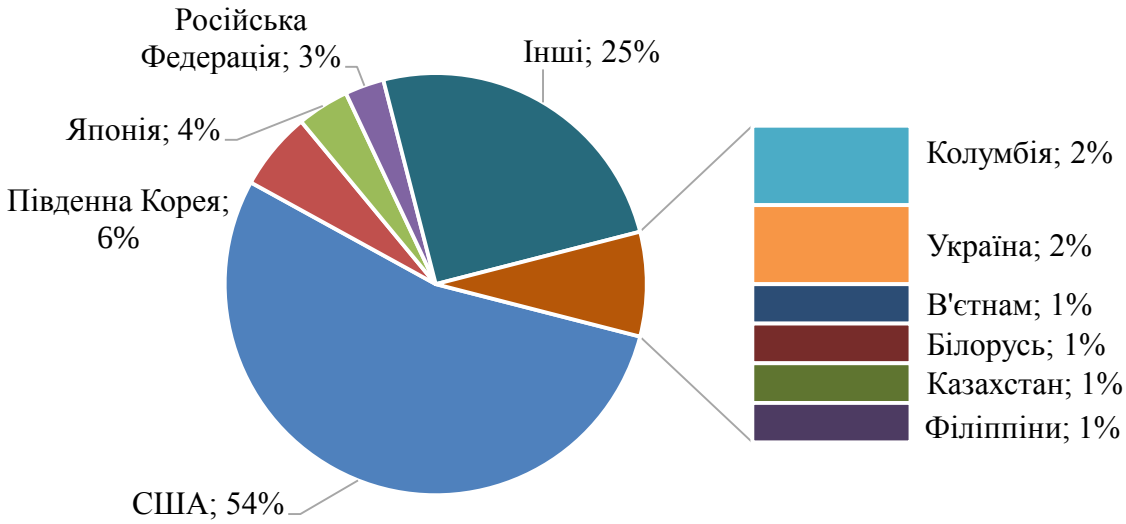

Рис. 8. Країни-жертви, найбільш зачеплені кібершпигунством у 2013 р., за кількістю інцидентів [17]

Оцінку готовності країн протистояти кіберзагрозам представляє Глобальний індекс кібербезпеки (GCI). У 2017 р. Сінгапур зайняв перше місце за індексом кібербезпеки з оцінкою GCI 0,925 [18]. Сполучені Штати зайняли друге місце з оцінкою GCI 0,919 індексних пунктів. Російська Федерація GCI 0,788 зайняла 10 місце, Україна має GCI 0,501 - 59 місце.

У зв'язку із зростанням кількості кіберзлочинів, а також втрат підприємств, організацій, державних та недержавних установ країн у світі зростає попит на пристрої безпеки. Згідно даних Total global security appliance market revenue 2014-2016 загальні доходи від реалізації пристроїв безпеки у 2016 р. досягли рівня 10,26 млрд. дол., що майже на 13% більше ніж за попередній, 2015 р., у якому загальні доходи склали 9,027 млрд. дол. У 2016 р. тільки одна компанія Cisco випустила пристроїв безпеки на суму 1,7 млрд. доларів [19]. Тільки витрати на забезпечення інформаційної безпеки та кібербезпеки провідними компаніями світу зросли до 14% на рік.

За оцінкою компанії Microsoft повна потенційна вартість кіберзлочинності для світової спільноти склала 500 млрд. дол. [20]. У звіті про шахрайство компанії Javelin за 2017 р. вказується, що 15,4 млн. американських споживачів (зростання на 17,5%) втратили 16 млрд. доларів через шахрайство з ідентифікацією особистості у 2016 р. Такі показники демонструють зростання з 2015 р., коли 13,1 млн. жертв втратили 15,3

млрд. доларів [21].

Для визначення тенденції загроз безпеці розвитку країн крізь призму кіберзлочинності було використано показник рівня уразливостей та ризиків ІТ безпеці [22]. Дані прогнозу на 2019 р. представлені на рис. 9.

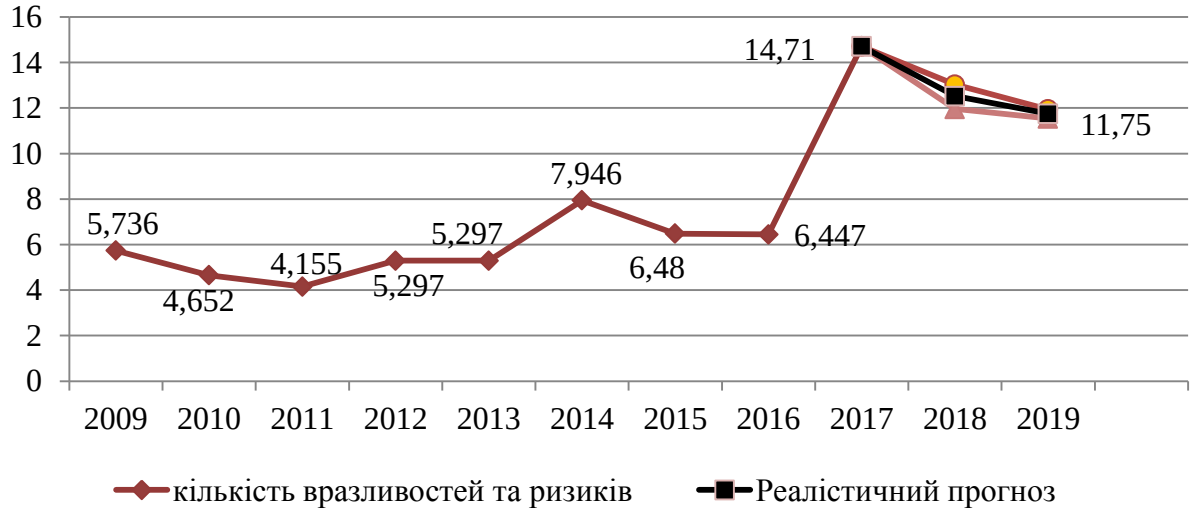

Рис. 9. Прогноз рівня уразливостей та ризиків ІТ безпеці у світі, тис. випадків

За песимістичним сценарієм прогнозування максимальний рівень уразливостей та ризиків ІТ безпеці у світі у 2019 р. складатиме 11,94 тис. випадків, що відповідає зменшенню на 18,8% порівняно з 2017 р. За реалістичним сценарієм цей показник складатиме 11,75 тис. випадків (зменшенню на 20,1%). За оптимістичним сценарієм ця цифра зменшиться на 21,6% і складатиме 11,54 тис. випадків. Таким чином, прогнозування показало, що після важких наслідків кібератак у 2016 та 2017 рр. спеціалісти з розробки захисту інформації та експерти з удосконалення безпеки ІТ зменшили кількість відомих уразливостей та ризиків для інформаційної інфраструктури, але у порівнянні даних за 2016 р. з прогнозованими даними у 2019 р. кількість уразливостей та ризиків збільшиться майже у двічі.

Висновок. Аналіз світових тенденцій показав, що злочинність в інформаційній сфері чинить суттєві перешкоди для розвитку країн. Серед найбільш небезпечних напрямків кіберзлочинності є атаки на інфраструктуру, руйнування роботи підприємств, державних установ, кібершпигунство, а також прямі економічні збитки через шахрайства, здирництва, компрометацію даних, тощо. Як показав прогноз,

кількість уразливостей та ризиків IT безпеці у світі зростає, тому необхідне посилення міжнародної політики та розробки механізмів протидії кіберзлочинності. Тому наступним кроком дослідження розробка когнітивної моделі загроз безпеці країн.

Список використаних джерел

1. Common IT vulnerabilities and exposures worldwide 2009-2017. *The Statistics Portal.* URL: https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures/
2. Amount of monetary damage caused by reported cyber crime to the IC3 from 2001 to 2016 (in million U.S. dollars) *The Statistics Portal*. URL: https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/
3. Cyber Crime. Annualized costs caused by cyber crime worldwide 2017, by industry. The Statistics Portal. https://www.statista.com/statistics/474928/average-annual-costs-caused-by-cyber-crime-worldwide/
4. Data breach price. *Comparitech*. URL: https://www.comparitech.com/blog/information-security/data-breach-share-price/
5. Number of Breach Incidents By Type. Attackers use a variety of techniques against organizations. *BREACH STATISTICS.* URL: http://www.breachlevelindex.com/#!breach-database
6. 2017 Breach Level Index Report: Identity Theft and Poor Internal Security Practices Take a Toll. *BREACH STATISTICS.* URL: https://safenet.gemalto.com/About_SafeNet/News_and_Media/News_Items_-_DP/2017/First_Half_2017_Breach_Level_Index_Report__Identity_Theft_and_Poor_Internal_Security_Practices_Take_a_Toll/
7. Number of unique malware variants 2014-2016. *The Statistics Portal.* URL: https://www.statista.com/statistics/224128/number-of-unique-variants-of-malware/
8. Amount of victim loss in million U.S. dollars. *The Statistics Portal.* URL: https://www.statista.com/statistics/234987/victim-loss-cyber-crime-type/
9. Geographic location of malicious data breach victims in 2016, ranked by share of attacks. *The Statistics Portal.* URL: https://www.statista.com/statistics/256653/most-targeted-victim-countries-of-cyber-attacks/
10. Cyber Crime. Distribution of global ransomware infections 2015-2016, by industry. *The Statistics Portal.* URL: https://www.statista.com/statistics/696004/leading-ransomware-infected-industry/
11. Industries with the highest ransomware infection rates 2016 *The Statistics Portal.* URL: https://www.statista.com/statistics/653720/leading-ransomware-infected-industries/
12. New ransomware attack hits Russia and spreads around globe. *CNN Tech.* URL: http://money.cnn.com/2017/10/24/technology/bad-rabbit-ransomware-attack/index.html
13. Report Facts At A Glance. *AV-Test Security.* URL: https://www.av-test.org/ en / news / news-single-view / current-risk-scenario-av-test-security-report-facts-at-a-glance /
14. Amount of ransom demanded during ransomware attacks 2017. *The Statistics Portal.* URL: https://www.statista.com/statistics/701003/average-amount-of-ransom-requested-to-msp-clients/
15. Internet Security Threat Report. – 2017. *Symantec. ISTR.* URL: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf
16. Annual number of cyber incidents according to U.S. federal agencies 2006-2015. *The Statistics Portal.* URL: https://www.statista.com/statistics/677015/number-cyber-incident-reported-usa-gov/
17. Distribution of cyber espionage in selected victim countries worldwide 2013. *The Statistics Portal.* URL: https://www.statista.com/statistics/330286/cyber-espionage-selected-victim-countries/
18. Global Cybersecurity Index 2017. *ITU*. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
19. Total global security appliance market revenue 2014-2016, by vendor. *The Statistics Portal.* URL: https://www.statista.com/statistics/526213/global-security-appliance-revenue-vendors-market-revenue/
20. Microsoft Security Intelligence Report. URL: https://download.microsoft.com/download/1/A/E/1AE5C1D8-8874-481B-94F8-57B41D4E8965/Microsoft_Security_Intelligence_Report_Volume_17_English.pdf
21. Javelin Strategy & Research. *Upcoming Events.* URL: https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new
22. Common IT vulnerabilities and exposures worldwide 2009-2017. *The Statistics Portal.* URL: https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures/

Bondarenko O.I. The Analysis of Threats to the Security of Countries' Development Through the Prism of Cybercrime. In the article the analysis of threats to the security of countries' development through the prism of cybercrime was done. To solve the set goal, the following research methods were used: information retrieval, statistical, comparative and system analysis, regression modeling. The statistical data of twelve indicators revealing threats to the security of countries' development and this data dynamics were analyzed in the article. It was determined that the crime in the information sphere inhibits significantly the development of countries. Among the most dangerous cybercrimes for countries' development are attacks on infrastructure, the destruction of enterprises' and government institutions' functioning, cyber espionage, as well as direct economic losses due to various types of fraud, extortion and data compromise. It was found that in 2017 the global financial services sector suffered the most. Today the leading harmful threats are cyber-extortion and banker Trojans. During 2015-2016 the service sector got 38% of global robber viruses, the manufacturing took the second place with 17%. Among various industries exposed to cyber-extortion, the education had the largest share of these that suffered losses due to ransom demand. Most of these attacks are done not for the purpose of collecting funds, but for violation of institution's normal operation and destabilization of service provision. The work provides a forecast of the level of vulnerabilities and IT security risks in the world. According to a realistic scenario of the forecast, the maximum level of vulnerabilities and IT security risks in the world in 2019 will be 11 750 cases, that is 20,1% less than in 2017. The analysis revealed that the development of the world community is currently impossible without the development of ICT and network technologies, but with this development the level of threats from crime in the information sphere is also growing.

Key words: cybersecurity; cyber-extortion; crime in the information sphere; attacks with ransom demand; economic damage.

Матеріал надійшов до редакції