УДК 32.019.51

Олена Бондаренко

***Бондаренко О.І.**, доцент, кандидат психологічних наук, доцент кафедри міжнародної інформації та країнознавства Хмельницького національного університету (Україна, Хмельницький), elenaivbond@gmail.com*

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

Аналіз загроз забезпеченню приватності особи крізь призму злочинності в інформаційній сфері

Бондаренко О.І. Аналіз загроз забезпеченню приватності особи крізь призму злочинності в інформаційній сфері. Метою дослідження є аналіз сучасного стану розвитку загроз приватності особи в умовах зростання злочинності в інформаційній сфері. Для вирішення поставленої мети були використані наступні методи дослідження: інформаційно-пошуковий, статистичний, порівняльний, системний аналіз, регресійне моделювання. Вихідними даними для аналізу загроз забезпеченню приватності особи в інформаційній сфері були використані статистичні дані наступних показників: рівень доступу до мобільного зв'язку та широкосмугового Інтернет у світі, рівень доступу до мобільного зв'язку та Інтернет за рівнем розвитку країн, поширення глобальних інцидентів з порушеннями даних, поширення глобальних вірусів – здирників (ransomware), кількість нових мобільних уразливостей, кількість поширених уразливостей і ризиків ІТ-безпеки у світі та сума грошового збитку, викликаного кіберзлочинністю, кількість компрометованих даних у світі. У статті проаналізовано сучасний стан розвитку ІКТ у світі, встановлено, що із зростанням розвитку ІКТ та мережевих технологій, зростає і рівень загроз від злочинності в інформаційній сфері. Досліджені види загроз приватності особи. Підтвержено факт, що крадіжки особистих даних є найбільш поширеним злочином проти приватності особи, а особиста інформація стала цінним товаром для кіберзлочинців. Проаналізований рівень збитків від злочинної діяльності в інформаційній сфері. Встановлено, що на рівень захисту приватності особи найбільше впливає рівень компрометованих даних, тобто даних, які втрачені, розкриті або викрадені у наслідок дій кіберзлочинців. Зроблено прогноз кількості компрометованих даних у світі на 2018 р. Оскільки компрометовані дані пов'язані не тільки з приватністю особистості, а і з організаціями і підприємствами, тому подальший напрямок дослідження буде полягати у визначенні загроз безпеці розвитку країн крізь призму злочинності в інформаційній сфері. Дослідження рівня загроз приватності та безпеки країни

може допомогти Україні завчасно реалізовувати заходи щодо покращення рівня кібербезпеки.

Ключові слова: кібербезпека, приватність особи, персональні дані, кіберзлочин.

Bondarenko Olena. The Analysis of Threats to Personal Privacy Through the Prism of Crime in the Information Sphere. The purpose of the study is to analyze the development of threats to personal privacy for today as crimes in the information sphere increase. The following research methods were used to reach the set purpose: information retrieval, statistical, comparative, system analysis, regression modeling. The baseline data for the analysis of threats to the personal privacy in the information sphere were the following statistics: the level of access to mobile communication and broadband Internet in the world, the level of access to mobile communication and Internet by the level of countries' development, the spread of global incidents of data violation, the spread of global ransomware viruses, the number of new mobile vulnerabilities, the number of common vulnerabilities and risks of IT security in the world, the amount of monetary damage caused by cybercrime and the quantity of breached data in the world. In the article the current state of ICT development in the world was analyzed. It was found that as the level of ICT and networking technologies development increases, the level of crime threats in the information sphere grows too. Types of threats to the personal privacy were studied. It was confirmed that a theft of personal data is the most common crime against the personal privacy, and personal data have become valuable goods for cybercriminals. The level of losses from criminal activity in the information sphere has been analyzed. It was determined that the degree of breached data (the lost data) influences at most on the level of privacy protection. The forecast of breached data quantity in 2018 was done. The further direction of the research will be to determine the threats to the security of countries' development through the prism of crime in the information sphere, as the breached data is linked not only to personal privacy, but also to privacy of organizations and enterprises. The study of the level of threats to privacy and countries' security can help Ukraine to implement measures for cybersecurity improvement in advance.

Key words: cybersecurity, personal privacy, personal data, cybercrimes

Постановка наукової проблеми та її значення. Інформаційна безпека є складним, системним, багаторівневим явищем, на стан якого впливають зовнішні і внутрішні чинники, зокрема політична обстановка у світі; внутрішньополітична обстановка в державі; стан і рівень інформаційно-комунікаційного розвитку країни тощо. Якість сучасного життя людини

пов’язують з проникненням інформаційно-комунікативних технологій. Саме унікальні особливості інформаційної технології полегшують її використання в деструктивних цілях. Активне використання персональних даних органами державної влади, комерційними та громадськими організаціями суттєво посилює ризик несанкціонованого вторгнення сторонніх осіб в приватне життя, створює загрозу порушення права на недоторканність приватного життя. Приватність – фундаментальне право людини, визнане в Загальній декларації прав людини ООН, Міжнародному пакті про громадянські й політичні права та в багатьох інших міжнародних і регіональних угодах. Приватність тісно пов'язана з людською гідністю й іншими ключовими цінностями, такими як свобода асоціацій та свобода слова. Вона стала одним із найбільш важливих питань у галузі прав людини новітнього часу. Персональні дані – будь-які дані або сукупність даних, які дозволяють ідентифікувати індивіда. Поняття «захист персональних даних» не зводиться до вимог забезпечення якості та безпеки обробки даних, оскільки включає і захист права суб'єкта персональних даних контролювати дані про себе. Однак проблема контролю та можливостями правопорушень з персональними даними невирішена. **Мета** дослідження: аналіз сучасного стану розвитку загроз приватності особи в умовах зростання злочинності в інформаційній сфері. **Методологічна база** дослідження: інформаційно-пошуковий метод, статистичний, порівняльний, системний аналізи, регресійне моделювання.

Теоретичні підходи до аналізу політики щодо захисту персональних даних розглядаються в дослідженнях А. Уестіна (Westin, A.), Ч. Рааба (Raab, C.), К.Беннета (Bennett, C.), К. Грінлефа (Greenleaf, G.). У рамках цих підходів ефективний режим політики щодо персональних даних визначається як використання комплексу різноманітних інструментів регулювання і залученням різних кластерів акторів в процеси структурування проблеми захисту персональних даних і прийняття рішень в цій сфері. К.Беннетт і Ч.Рааб у роботі «The Governance of Privacy: Policy Instruments in Global Perspective» [1], розглядаючи регулювання конфіденційності даних, прийшли до висновку:

існування та формальна сила законодавства про конфіденційність даних є лише одним із факторів, за допомогою яких ми повинні вимірювати захист приватного життя в країні, а також два інші ключові аспекти – ефективність застосування та масштаб спостереження. А. Лукас у роботі «What is privacy? The history and definition of privacy» [2] зазначає, що захист приватного життя не може бути відокремлений від технологічного розвитку: в наші дні, завдяки розвитку науки та технологій, можливість втручатися в чужі конфіденційність збільшилася. Важливість приватного життя може бути пов'язана з тим, що конфіденційність має тісний зв'язок з людською гідністю, свободою та незалежністю особистості, і це все більше і більше ускладнюється в епоху швидкого технологічного розвитку інформаційного суспільства.

Виклад основного матеріалу й обґрунтування результатів дослідження. Характерною рисою трансформації злочинності у сучасну добу є активне використання інформаційно-комунікаційних технологій. Зрозуміло, чим вищий рівень розвитку ІКТ, тим більше злочинців будуть намагатися використовувати останні досягнення для здійснення неправомірних дій. Важливим є не стільки і не тільки розвиток комп’ютерної техніки, як розвиток комп’ютерних мереж, долучення великої кількості користувачів до соціальних мереж, використання мережевих технологій підприємствами, державними установами, транзакції коштів, онлайн банкінг, тощо.

Сьогодні доступ до Інтернет у світі має близько 53% населення, тим не менш, середній рівень його використання складає 47,6% [3]. Важливість доступу до Інтернет підтверджується і тим, що Рада з прав людини ООН ухвалила резолюцію (2016 р.), яка прирівнює доступ до мережі Інтернет до базових прав людини. Документ, зокрема, забороняє кому б то не було (в тому числі, владним структурам) обмежувати доступ або відмовляти в ньому [4]. Сучасний розвиток ІКТ поступово зміщується від використання комп’ютерів до застосування у повсякденному житті для доступу до інформації, у тому числі і виходу у Інтернет, мобільного стільникового зв’язку (рис.1).

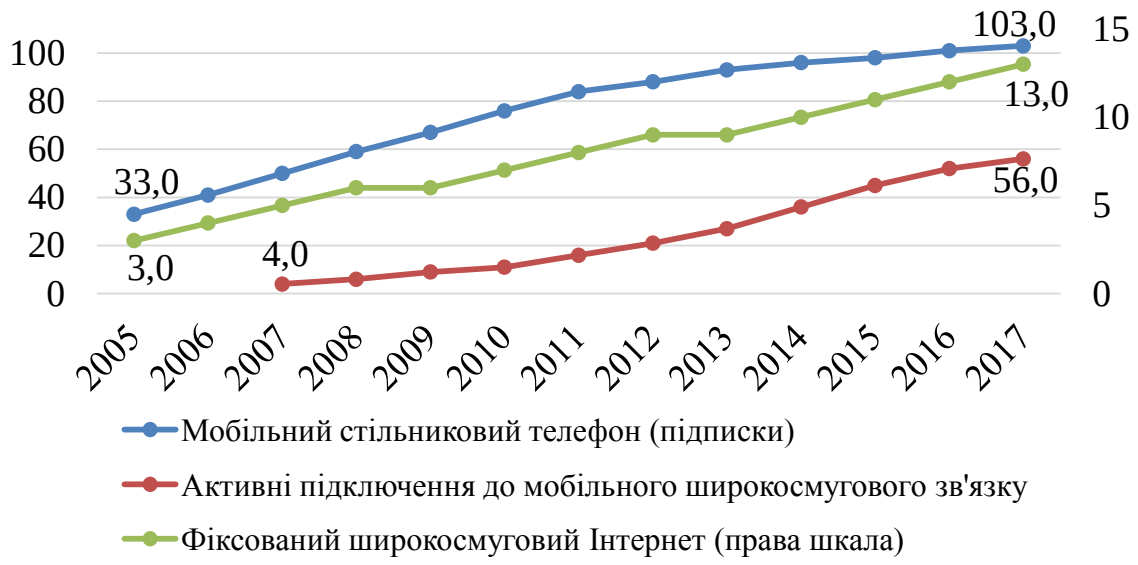

Рис. 1. **Рівень доступу до мобільного зв'язку та широкосмугового Інтернет у світі, % [3]**

Серед різних регіонів світу найнижчі показники доступу до Інтернет та мобільного зв'язку станом на 2017 р. мало населення Африки – 77,8%, у той же час найвищі показники мали громадяни Європи – 118,2%. У країнах СНД населення користується одночасно декількома операторами мобільного стільникового зв'язку телефоном, про що свідчить показник у 141,1% [3]. За цим показником СНД навіть випереджає Європу та Америку. Найнижчі показники серед всіх видів доступу до інформації за допомогою ІКТ має фіксований широкосмуговий Інтернет (Африка 0,4%, арабські держави 5,3%, АТР 12,3%, СНД 16,5%, Європа 30,9%, Америка 19,6%) [3]. Невисокі показники доступу до широкосмугового Інтернет у добу глобалізації та проникнення ІКТ в усі сфери життя змусило більшість країн сформувати національні програми розвитку широкосмугового доступу, які покликані в період до 2018-2020 рр. забезпечити можливість практично для 100% домогосподарств і 100% населення доступ до сервісів Інтернету. Причому в кожній країні такі програми формуються на державному рівні і передбачають державну участь там, де створення таких мереж комерційно невигідно.

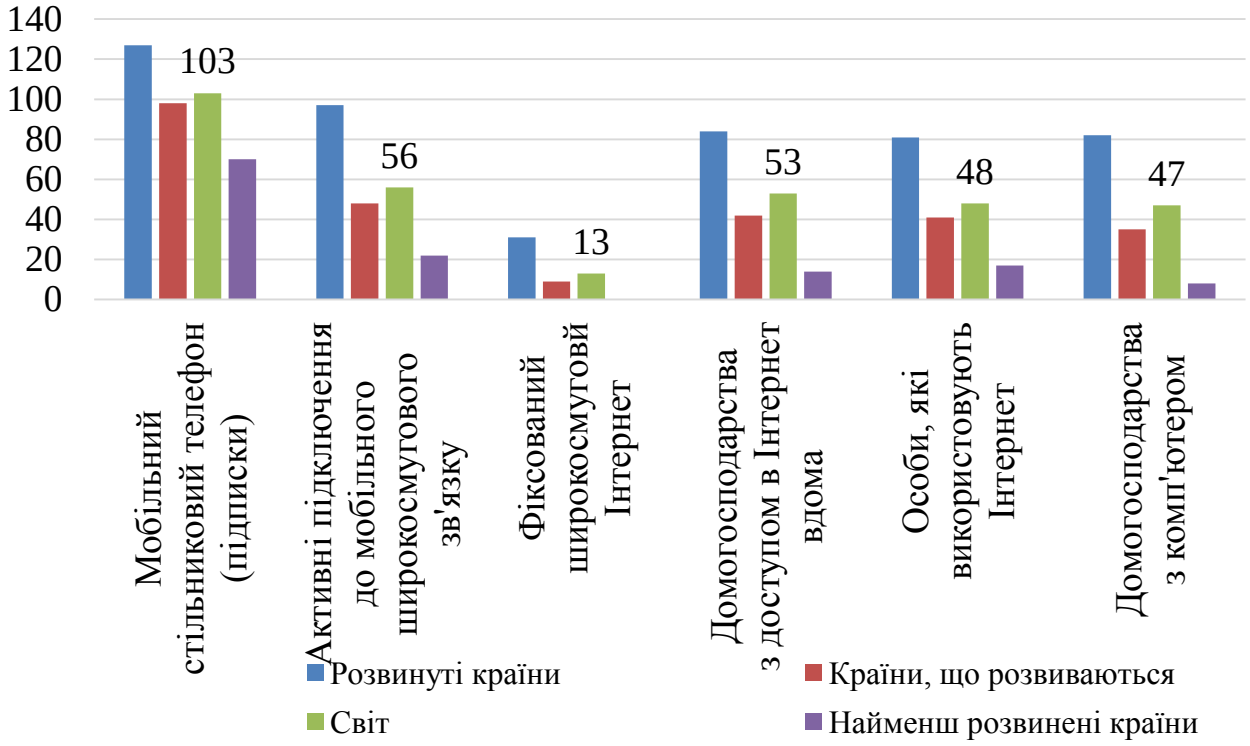

Рис. 2. **Рівень доступу до мобільного зв'язку та Інтернет за рівнем розвитку країн у 2017 р., % всього населення [3]**

Суттєва різниця у доступі до Інтернет та використання досягнень ІКТ спостерігається і серед країн з різним рівнем розвитку (рис. 2). Найменш розвинені країни та країни, що розвиваються мають показники доступу до Інтернет та використання досягнень ІКТ нижчі за середні по світу. Цей факт, викликає стурбованість в експертному середовищі, урядових та неурядових організаціях. Так, у новій доповіді Світового банку «Отримання цифрових дивідендів: ефективне використання інтернету для розвитку в Європі і Центральній Азії» [5] зазначається, що розвиток інтернет-технологій не тільки надає країнам нові можливості для розвитку, але і вимагає розробки заходів для адаптації до нових умов з метою недопущення зростаючої нерівності та ізоляції, для чого країни ЄС повинні вжити заходів, які б допомагали працівникам адаптуватися до нових робочих місць, створюваним завдяки розвитку інтернет-технологій.

Соціальні мережі сьогодні є одним з провідних онлайн напрямків діяльності в усьому світі. У 2020 р. експерти оцінюють 2,95 млрд. осіб будуть

мати регулярний доступ до соціальних мереж [6]. Велика частина цього зростання, за прогнозами, буде надходити з мобільних пристроїв, оскільки ринки, що розвиваються швидко опановують онлайн-зв'язок. Найбільш поширеними у світі, зокрема на європейському та американському континентах є соціальні мережі Facebook, Instagram, LinkedIn, Twitter та відеохостінг YouTube. Кількість користувачів у світі, які щоденно активно користуються Facebook з 2011 р. по 2017 р. зросла у 3,8 рази і склала 1368 млн. осіб. [6]

Особиста інформація - цінний товар, тому не дивно, що кіберзлочинці атакують онлайн-провайдерів в надії отримати дані, які вони зможуть потім продати або використати для майбутніх атак на користувачів і бізнес. У 2017 р. від витоку даних постраждали багато великих компаній, в тому числі Yahoo (повідомлення про злом, який трапився в 2013 р.), Avanti Markets, Election Systems & Software, Dow Jones, America Link Link Alliance і Equifax [7] (табл. 1).

Таблиця 1

Кількість викрадених облікових записів користувачів станом на 2017 р., [6]

Компанія	Дата інциденту	Кількість записів (млн. од.)
Yahoo	Серпень'13, виявлено Грудень'16, оновлено Жовтень'17	3000
River City Media	Лютий'17	1370
Yahoo	2014 рік, виявлено Серпень'16	500
MySpace	Травень'16	427
Friend Finder Network Inc	Жовтень'16	412
US Voter database	Грудень'15	191
Adobe	Вересень'13	152
eBay	Березень'14	145
Equifax	Травень-липень'17, повідомлено Вересень'17	143
Heartland	Січень'09	130
LinkedIn	Червень'12, виявлено Травень'16	117
VK	Червень'16	100
T.J. Maxx	Березень'07	94
AOL	Грудень'14	92
Dailymotion	Жовтень'16	82,5
Anthem	Лютий'15	80
Sony PSN	Квітень'11	77

US Military	Січень'09	76
JP Morgan Chase	Липень'14	76

У листопаді 2017 р. було оприлюднено інформацію про злом Uber, який мав місце в жовтні 2016 р. і призвів до витоку даних 57 млн. клієнтів і водіїв. Деякі з цих атак призвели до витоку величезних обсягів даних, причому в більшості випадків цьому можна було запобігти. У 2017 р. були зламані бази багатьох організацій, з витоком колосальних обсягів даних, наслідки чого можуть відчуватися роками. Статистика, яка наведена у табл. 1 є вибіркою найбільших онлайн-порушень даних по всьому світу станом на жовтень 2017 р., за кількістю вкрадених записів.

У серпні 2016 р. було виявлено злом онлайн-платформи Yahoo в 2014 р., що торкнулося не менше 500 мільйонів облікових записів користувачів. У грудні 2016 р. компанія виявила ще один злом, що відноситься до 2013 р., яка торкнулася 1 млрд. записів користувачів. Вплив другого повідомленого злому Yahoo було оновлено у жовтні 2017 р., коли компанія виявила, що 3 млрд. облікових записів були вкраденими, що робить його найбільшим порушенням даних в історії. У 2011 р. музична служба Sony PlayStation Network і музична служба Qriocity були атаковані зломом колективу Lulzsec. Sony PlayStation Network був відключений 43 днів і 77 млн. записів даних були вкрадені. [6]

Зі збільшенням використання цифрових файлів і використанням цифрових даних багатьма корпораціями крадіжка особистих даних стала досить поширеною в останнє десятиліття. Наприклад, число порушень даних в США збільшилася з 157 млн. у 2005 р. до 781 млн. в 2015 р., в той час як кількість відкритих записів зросла з 67 млн. до 169 млн. протягом того ж періоду часу. [6]

У секторі послуг була найбільша кількість випадків, виявлених у цьому році - майже 260 млн. На цей показник припадало трохи більше 60% всіх повідомлень про злочини, які були виявлені в результаті порушень даних у 2015 р., на фінансовий сектор також сильно впливає кіберзлочинність. Крадіжка даних безпосередньо про сам доступ до даних є другим найбільш поширеним типом порушення даних, на який припадає 22% всіх порушень

даних. У 2015 р. в цьому секторі було виявлено 120 млн. ідентифікаційних записів.

Крадіжка особистих даних є найбільш поширеним типом інциденту з порушенням даних в світі. У 2015 р. крадіжка особистих даних становила понад 50% усіх глобальних порушень даних і близько 40% усіх скомпрометованих записів, у 2016 р. ця цифра збільшилася до 59% усіх випадків порушення глобальних даних. У першій половині 2017 р. цей тип злочину зріс до 74% розподілу глобальних інцидентів з порушеннями даних (рис. 3).

Рис. 3. **Поширення глобальних інцидентів з порушеннями даних у 1-й половині 2017 року, за типом [6]**

У 2017 році на неприємні атаки припадало лише 1% порушень даних в цьому році. У той же час на екзистенціальні дані – дані, які впливають на існування самої особистості, її безпековий вимір – припадало до 6% всіх випадків.

Електронна пошта є частиною ландшафту загроз, і тому необхідно робити все, щоб захистити себе та свій бізнес від них. Електронна пошта є найпопулярнішим способом для зловмисників розповсюджувати шкідливий код. У середньому один із дев'яти користувачів електронної пошти у першій половині 2017 р. стикався з шкідливим програмним забезпеченням електронної пошти [8]. Найбільш масштабним ураженням через електронну пошту останніми роками стали віруси-шифрульники-здирники (ransomware). Кількість нових сімей таких вірусів, що вимагають гроші за дешифрування файлів, різко

зросла протягом 2016 р. з 30 нових сімейств, які щорічно з'являлися протягом 2014 і 2015 рр., це число зросло більше, ніж у три рази – до 98 у 2016 р. [8]

Більше третини всіх випадків викупу, зафіксованих у 2017 р., припадає на США (34%), Японія (9%), Італія (7%), Канада (4%) та Індія (4%) також сильно постраждали. Такі європейські країни, як Нідерланди (3%), Росія (3%), Німеччина (3%) та Великобританія (3%) також потерпали від зараження. Статистичні дані свідчать, що нападники, які вимагали викуп за дешифрування даних, концентрувалися на розвинених, стабільних економіках. [6]

Дані табл. 2 свідчать, що протягом 2017 р. найбільша частка 7,71% користувачів, які зазнали нападу за допомогою шифрування, зіткнулися з WannaCry.

Таблиця 2

Провідні типи шифрування ransomware у 2017 р., [6]

Назва вірусу	Частка користувачів, які постраждали	Назва вірусу	Частка користувачів, які постраждали
WannaCry	7,71%	Spora	2,19%
Locky	6,70%	Purgen/GlobeImposter	2,11%
Cerber	5,89%	Shade	2,06%
Jaff	2,58%	Crysis	1,25%
Cryrar/ACCDFISA	2,20%	CryptoWall	1,13%

Жертви ураження таким вірусом повинні були виплачувати шахраям викуп. Розрахункова середня сума викупу, яка вимагалась зловмисниками у всьому світі з 2014 р. до першої половини 2017 р. суттєво коливалась (з 373 дол. до 544 дол. відповідно). Найбільшу суму зловмисники-порушники вимагали від своїх жертв у 2016 р. 1071 дол. США. [6]

Більшість випадків інфікування ransomware протягом 2016 р. відбулися на комп'ютерах споживачів (70%). Це несуттєво менше за 2015 р., коли частка інфікування ransomware на комп'ютерах споживачів становила 71% (рис. 4). [9]

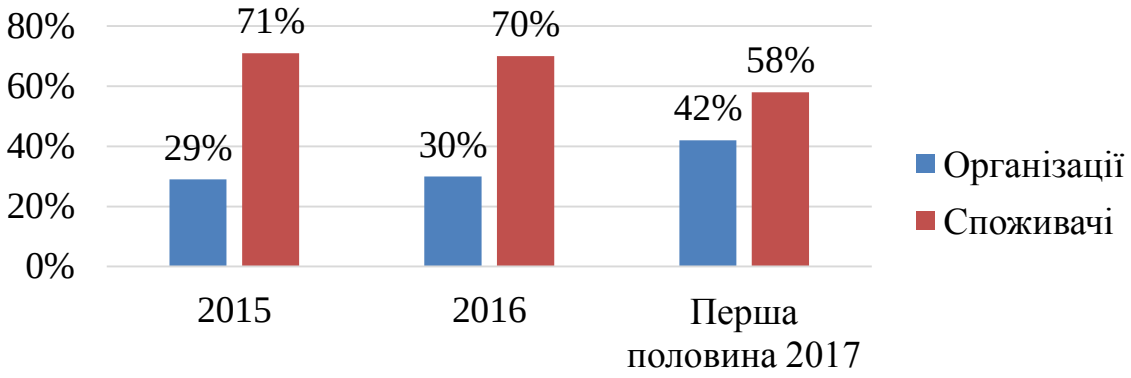

Рис. 4. **Поширення глобальних вірусів – здирників (ransomware) у 2015 - 2017 рр. за групою жертв [6]**

Зі збільшенням кількості мобільних пристроїв, розширенням сфери їх застосування та зростанням числа мобільних користувачів підвищується ймовірність появи і активного розвитку мобільних шкідливих програм (рис. 5). Так формується постійна «гонка озброєнь» між кіберзлочинцями, розробниками ПЗ та фахівцями з кібербезпеки.

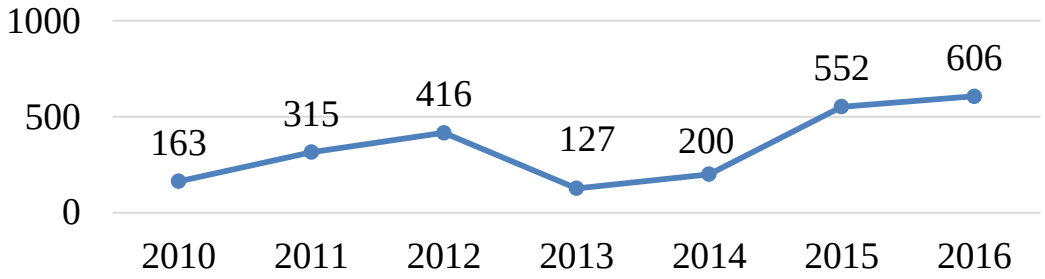

Рис. 5. **Кількість нових мобільних уразливостей у 2010 - 2016 р. [6]**

У 2017 р. через заражені троянцями мобільні додатки користувачі зіткнулися з агресивною рекламою, атаками здирників і крадіжкою грошей через системи SMS- і WAP-білінгу. Більшість випадків інфікування ransomware протягом 2016 року відбулися на комп'ютерах споживачів (70%). У першому півріччі 2017 року, значно зросла кількість мобільних троянців-здирників – кількість інсталяційних пакетів збільшилася в 1,6 рази в порівнянні з усім 2016 роком.

Фахівці Avast [10] відзначають 40% зростання числа мобільних кібератак: середньомісячний показник збільшився з 1,2 млн. до 1,7 млн. Дослідники з'ясували, що в місяць в середньому з'являється 788 нових варіантів вірусів - на

22,2% більше, ніж у другому кварталі 2016 р. У звіті Avast вказується, що три найпоширеніші мобільні загрози - це ПЗ, розроблене для шпигунства і крадіжки особистих даних («перехоплювачі root-доступу»), а також для показу користувачам небажаної реклами («завантажувачі / дроппер» і «фейковий додатки»). Топ-3 мобільних загроз у другому кварталі 2017 р: перехоплювачі root-доступу / rooters (22,8%), завантажники (22,76%), фейкові додатки (6,97%).

Кількість поширених уразливостей і ризиків безпеки IT, виявлених у світі в період з 2009 р. по 2017 р. постійно зростає. В останній рік було виявлено 14712 нових загальних уразливостей і ризиків IT, ніж в два рази більше, ніж 6447 таких уразливостей у попередньому році (рис. 6). Суми збитку, заподіяного кіберзлочинністю за повідомленням IC3 (США) з 2001 по 2016 рік зростала практично з однаковим щорічним приростом (рис. 6).

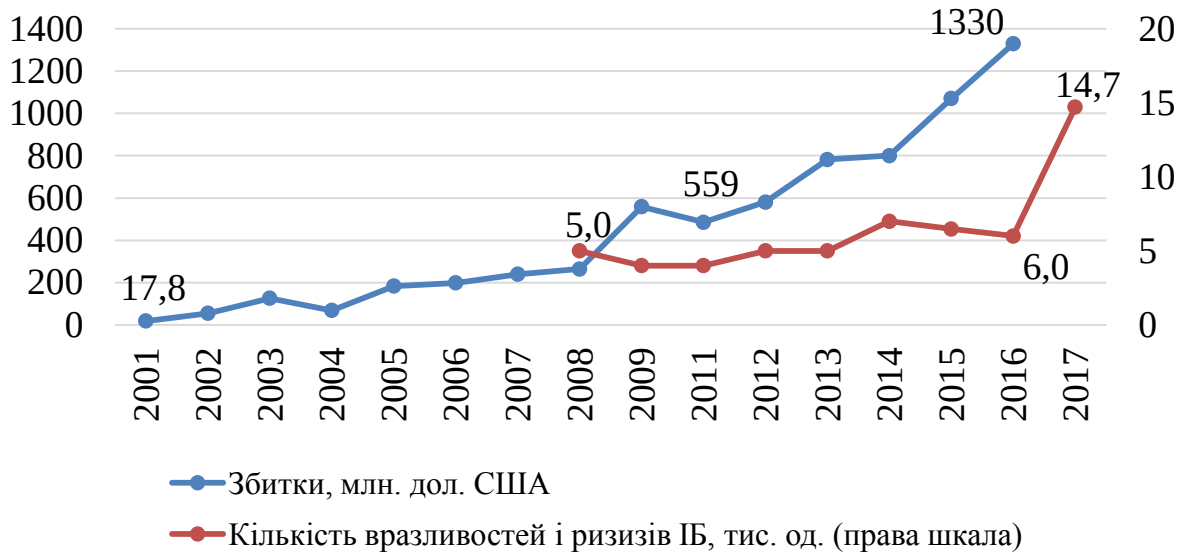

Рис. 6. **Кількість поширених уразливостей і ризиків IT-безпеки у світі та сума грошового збитку, викликаного кіберзлочинністю [6]**

У 2016 р. щорічні втрати від кібер-злочинів за оцінкою IC3 склали 1,33 млрд. дол., у порівнянні з 781,84 млн. дол. у 2013 р. Більшість інцидентів з порушеннями даних були пов'язані з крадіжкою особистих даних, за якими слідували фінансові та облікові дані.

У звіті про шахрайство компанії Javelin за 2017 р. вказується, що 15,4 млн. американських споживачів (зростання на 17,5%) втратили 16 млрд. дол. через шахрайство з ідентифікацією особистості у 2016 р. Ці показники

зростають з 2015 р., коли 13,1 млн. жертв втратили 15,3 млрд. дол. [11]

Аналіз показав, що спостерігається зростання кібер-небезпек. Стурбованість населення щодо у кібер-безпеки ілюструє опитування громадян США у 2017 р., одне з питань у якому було: «Доступ до якої з наступних типів вашої особистої інформації є найбільш цікавим онлайн-хакерам?». За результатами опитування 73% респондентів заявили, що вони будуть відчувати найбільшу стурбованість з приводу того, що хакери отримують доступ до їх особистої банківської інформації [6]. Наступне опитування інтернет-користувачів США (2017 р.) показало, які проблеми найбільш викликають у них стурбованість щодо використання Інтернету. Результати опитування засвідчили, що 59% респондентів турбує кібер-злочинність, наслідком якої є те, що в Інтернеті викрадаються їх гроші чи особисті дані, 49% турбує Інтернет-атаки через Інтернет, щоб зіпсувати життя в США (наприклад, крадіжка секретної інформації в Інтернеті), 31% – неправдиві новини та пропаганда в соціальних мережах, 30% – компанії збору та обміну особистими даними в Інтернеті з іншими організаціями, 26% – Інтернет-спостереження за громадянами урядом США, 23% – те, що діти користуються онлайн-вмістом неприйнятного характеру, 7% - розміщенням в Інтернеті образливих або особистих речей про них. [6]

На рівень захисту приватності особистості та безпеку країни найбільше впливає рівень компрометованих даних, тобто даних, які втрачені, розкриті або викрадені у наслідок дій кіберзлочинців. Крім того, рівень успішних атак проти інформаційної інфраструктури країни та окремих комп’ютерних систем, баз даних та приватних мереж буде тим вище, чим буде вищим рівень уразливостей та ризиків ІТ безпеці, які будуть виявлені та використані кіберзлочинцями. Тому для прогнозування рівня кіберзлочинності були обрані щомісячні показники стосовно порушень (компрометації) даних, які надають укладачі The Breach Level Index [12], попередньо вони були об’єднані у піврічні показники.

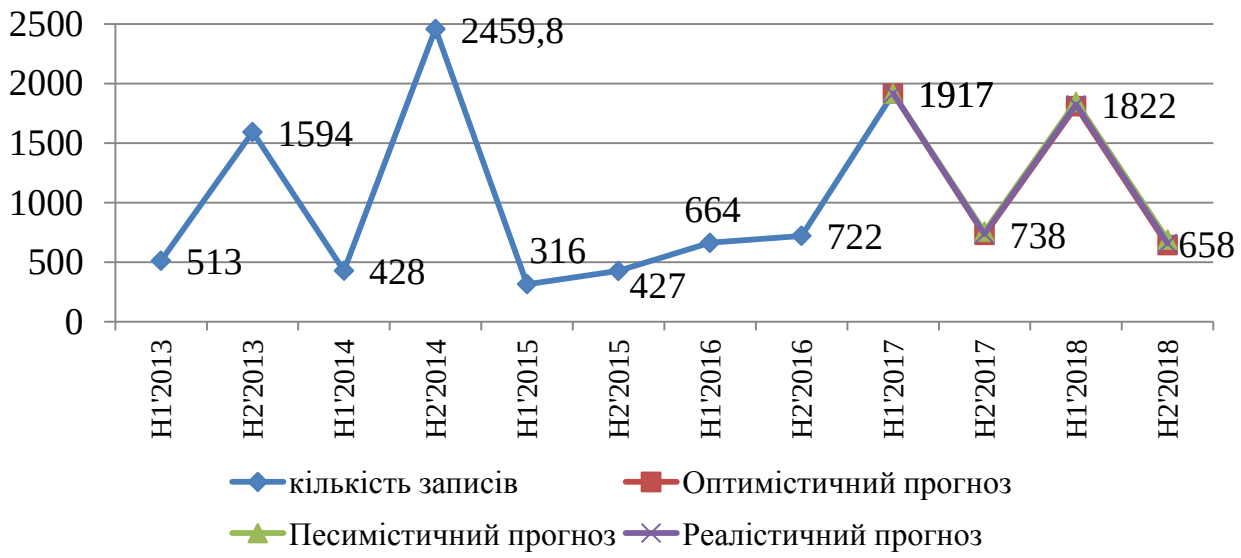

Рис. 7. **Прогноз кількості компрометованих даних у світі, млн. записів**

За реалістичним сценарієм кількість компрометованих даних у світі у H2'2018 р. складатиме 658,55 млн. записів, що відповідає зменшенню на 65,7% порівняно з H1'2017 р. Слід зауважити, що прогнозування показало, що обсяг компрометованих даних у першому півріччі за реалістичним сценарієм буде меншим за аналогічний показник 1-го півріччя 2017 р. лише на 5% і складе 1822,14 млн. записів. Це свідчить про те, що кіберзлочинці знаходять вразливості у IT безпеці, на які з певним запізненням реагують спеціалісти з захисту інформації. На підставі проведеного аналізу можна рекомендувати зменшувати час реакції на кібер-втручання в інформаційну систему та розробляти превентивні заходи, що є більш доцільними у таких обставинах.

Висновки та перспективи подальших досліджень. Аналіз загроз забезпеченню приватності особи крізь призму злочинності в інформаційній сфері показав, що із зростанням розвитку ІКТ та мережевих технологій, зростає і рівень загроз від злочинності в інформаційній сфері. Крадіжки особистих даних є найбільш поширеним злочином проти приватності особи, а особиста інформація стала цінним товаром для кіберзлочинців. На рівень захисту приватності особи найбільше впливає рівень компрометованих даних, тобто даних, які втрачені, розкриті або викрадені у наслідок дій кіберзлочинців. Прогнозування показало, що обсяг компрометованих даних 2018 р. буде

знижуватися. Подальший напрямок дослідження полягає у визначенні загроз безпеці розвитку країн крізь призму злочинності в інформаційній сфері.

Джерела та література

1. The governance of privacy : policy instruments in global perspective. [Elektronnyiy resurs] / Colin J. Bennett, Charles D. Raab. - Aldershot ; Burlington, VT : Ashgate, 2006, 257 p. – Rezhym dostupu: http://bookgede-book.tk/downloads/the-governance-of-privacy-policy-instruments-in-global-perspective.pdf
2. What is privacy? The history and definition of privacy. [Elektronnyiy resurs] / Lukác A. – Rezhym dostupu: http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf
3. Key ICT indicators for developed and developing countries and the world (totals and penetration rates). [Elektronnyiy resurs] / ITU World Telecommunication. – Rezhym dostupu: https://www.itu.int/en/ITUStatistics/Documents/statistics/2017/ITU_Key_2005-2017_ICT_data.xls
4. OON: pravo na Internet - bazovoe pravo dlya vseh. [Elektronnyiy resurs] /EuroNews. – Rezhym dostupu: http://ru.euronews.com/2016/07/05/un-denounces-disruption-of-internet-access-as-human-rights-violation
5. Reaping Digital Dividends: Leveraging the Internet for Development in Europe and Central Asia. [Elektronnyiy resurs] / T.Kelly, A.Liaplina, W. Tan, H.Winkler. – Rezhym dostupu: https://openknowledge.worldbank.org/bitstream/ handle/10986/26151/9781464810251.pdf?sequence=9&isAllowed=y
6. Statistics and Studies from more than 22,500 Sources. [Elektronnyiy resurs] /. The Statistics Portal «Statista». – Rezhym dostupu: https://www.statista.com/accounts/
7. Kaspersky Security Bulletin: 2017. [Elektronnyiy resurs] / Kaspersky. – Rezhym dostupu: https://cdn.securelist.ru/files/2017/12/KSB_Review-of-2017_final_RU.pdf
8. Internet Security Threat Report v22. [Elektronnyiy resurs] / Symantec Corporation. – Rezhym dostupu: https://www.symantec. com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf
9. Symantec. ISTR – 2017. [Elektronnyiy resurs] / Symantec Corporation World Headquarters. – Rezhym dostupu: https://www.symantec.com/content/dam/symantec/docs/reports/ istr-22-2017-en.pdf
10. Avast Reports 40% Increase in Mobile Cyberattacks. [Elektronnyiy resurs] / Avast Press. – Rezhym dostupu: https://press.avast.com/avast-reports-40-increase-in-mobile-cyberattacks
11. Javelin Strategy & Research. [Elektronnyiy resurs] / Javelin. – Rezhym dostupu: https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-

million-us-victims-2016-16-percent-according-new

12. Total records lost by month. [Elektronnyiy resurs] / The Breach Level Index. – Rezhym dostupu: http://www.breachlevelindex.com/#!breach-database