10. МАТЕМАТИЧНІ МЕТОДИ, МОДЕЛІ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

DOI: https://doi.org/10.32838/2523-4803/70-2-73

УДК 331.27:339(100)-049.5(045)

Остапчук В.М.
генерал-майор,
Військовий інститут телекомунікацій та інформатизації
імені Героїв Крут
Ільєнко О.В.
доктор економічних наук, професор,
декан факультету транспорту, менеджменту і логістики,
Національний авіаційний університет

Ostapchuk Viktor
Military Institute of Telecommunications and Informatization
the name of Heroes of Kruty
Ilienko Oksana
National Aviation University

АНАЛІЗ ВПЛИВУ КІБЕРЗАГРОЗ НА СВІТОВИЙ ЕКОНОМІЧНИЙ РИНОК

Статтю присвячено дослідженню основних кіберзагроз та їхнього впливу на світовий економічний ринок. Проведений аналіз дав змогу визначити основні процеси, які призвели до зростання ризиків від кібератак у 2019 р. Розкрито основні загрози, які впливають на різні бізнес-процеси як на національному, так і на міжнародному ринках. Визначено найбільш уразливі місця хакерських атак. Подано приклади інцидентів, пов'язаних із кіберзагрозами у 2019 р. Визначено основні тенденції в галузі кібербезпеки, які необхідно подолати. Слід зауважити, що фінансовий вплив від кібератак може включати витрати на страхування, впливати на поведінку клієнтів, включати витрати на судові процеси, штрафи та вплив на технологічну інфраструктуру і витрати на науково-дослідну роботу. Доведено необхідність постійного оновлення програмних продуктів, які допоможуть ефективно запобігти даним атакам.

Ключові слова: *кібербезпека, кіберзлочинність, хакерські атаки, економічні загрози, ризики, світовий економічний ринок.*

Постановка проблеми. Розвиток кіберзлочинності сьогодні є найбільш проблемним питанням, з яким стикаються представники бізнесу будь-якої галузі, особливо якщо врахувати зростання цифрової економіки, яка, своєю чергою, супроводжується зростанням кіберзагроз.

База користувачів Інтернету постійно збільшується. У 2019 р. кількість користувачів зросла на 4,39 млрд (або на 57%) від загальної кількості населення, тому компаніям потрібне сховище для конфіденційних даних із більшими можливостями та ресурсами, щоб захистити їх. Окрім того, нові інноваційні технології також створюють нові ризики [7].

Підтвердженням важливості даної проблеми для України є побудова єдиної загальнодержавної системи протидії кіберзлочинності, що має забезпечити захист критичної інфраструктури, про що свідчить Рішення Ради національної безпеки і оборони України від 17 листопада 2010 р. «Про виклики та загрози національній безпеці України у 2011 році», введене в дію Указом Президента України від 10 грудня 2010 р. № 1119 [1].

Аналіз останніх досліджень і публікацій. Аналізом питання захисту від кібератак займалися такі провідні вчені, як М.В. Грайворонський, В.А. Ліпкан, І.В. Діордіца, Л.І. Рудник, О.Ю. Запорожець, В.М. Панченко. Проведені ними дослідження довели, що компанії впроваджують нові технології швидше, ніж можуть вирішувати проблеми кібербезпеки [6]. Як результат, порушення даних – один із найшвидше зростаючих злочинів, який збільшується за масштабами, вартістю та витонченістю, що становить серйозну загрозу для бізнесу та приватних осіб навіть сьогодні.

Сучасні компанії захищають дані користувачів, використовуючи багатофакторну автентифікацію,

керований доступ до доступу та керування паролем на основі апаратних засобів, щоб захистити чутливі дані, але дуже важливо бути в курсі останніх тенденцій кібербезпеки та нових засобів захисту від атак, оскільки від цього залежить репутація бізнесу.

Формулювання цілей статті. Особливістю будь-яких бізнес-процесів сьогодні є те, що будь-яка інформація у всьому світі швидко трансформується у цифрову форму на відкритих та глобально взаємопов'язаних технологічних платформах. Коли це відбувається, ризики від кібератак стають усе більш впливовими. Злочинці переслідують фінансову вигоду шляхом шахрайства та крадіжок особи. Конкуренти крадуть інтелектуальну власність або порушують бізнес, щоб скористатися перевагою від даної інформації. Отже, виникає нагальна проблема аналізу процесу впливу кібератак на розвиток світового економічного ринку з метою сприяння подальшому запобіганню даним загрозам.

Виклад основного матеріалу. До основних процесів, які призвели до зростання ризиків від кібератак у 2019 р., належать:

– збільшення кількості користувачів Інтернету, що викликає потребу в розробленні нових антихакерських програм;

– потреба у сховищах для конфіденційних даних із більшими можливостями та ресурсами, щоб захистити їх [4];

– нові інноваційні технології, які викликають нові ризики:

– впровадження нових технології відбувається швидше, ніж можуть вирішуватися проблеми кібербезпеки;

– порушення даних як один із найшвидше зростаючих злочинів, який збільшується за масштабами, вартістю та витонченістю і становить серйозну загрозу для бізнесу та приватних осіб.

До переліку основних загроз для приватних осіб належать такі:

1. *Шахрайські електронні листи,* які залишаються найбільш широко використовуваною та успішною атакою як на бізнес, так і на окремих осіб. Більшість кібератак починається з фішинг-електронних листів, які використовують вразливості людини та заражають комп'ютери викупними програмами або іншими видами зловмисних програм. Особливістю даних атак є те, що вони націлені на конкретні підприємства.

2. *Віруси/шпигунське/зловмисне програмне забезпечення* – друга найпоширеніша атака, яка продовжує приносити значні збитки. Віруси призводять до різних шкідливих ефектів, включаючи видалення або крадіжку інформації, завантаження шкідливих програм, надання хакерам несанкціонованого доступу до комп'ютера тощо. Шпигунське програмне забезпечення дає змогу злочинцям збирати інформацію про користувачів, облікові дані кредитної картки, паролі користувачів та іншу особисту інформацію.

3. *Ransomware* – це зростаюча загроза, яка дає змогу хакерам автоматизувати атаки, і, таким чином, збільшувати їхні масштаби та прибутки за рахунок шантажу. Він блокує користувача або компанію від комп'ютера або всієї мережі, вимагаючи грошових компенсацій.

4. *Несанкціонований доступ* може здійснюватися за допомогою різних шкідливих методів та інструментів. Це призводить до крадіжки інформації, від якої зараз страждають багато організацій.

5. *Атаки відмови у користуванні* спрямовані на те, щоб запобігти доступу користувачів до сервера. Цей тип кіберзлочинності може призвести до помітного збою або повної недоступності сервера, що спричинить подальше вторгнення в мережу та втрату конфіденційних даних.

На рис. 1 подано частку впливу основних хакерських загроз на приватних осіб у 2019 р.

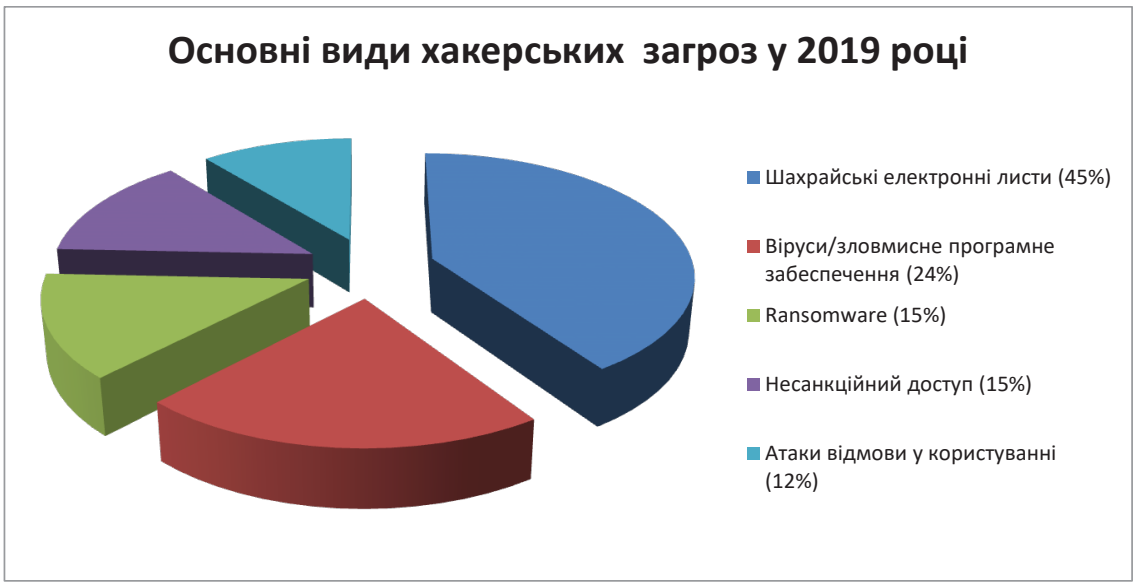

Рис. 1. Частка впливу основних хакерських загроз на приватних осіб у 2019 р.

Найбільш уразливими для хакерських місцями (на ринку послуг) є такі [5]:

1. *Фінансовий ринок:*

– банки мають високий ризик, оскільки вони зберігають дані та кошти приватних клієнтів, і вони надають доступ до їхніх послуг через безліч онлайн та цифрових каналів. Успішна атака на великі, системні банки може становити ризик на загальному рівні, що відображає їх високу ступінь взаємопов'язаності; компанії із цінними паперами, які мають на меті здійснити масштабні крадіжки, а також складні напади, покликані створити операційний зрив або привернути до себе рекламу;

– постачальники ринкової інфраструктури, до яких належать біржі та клірингові компанії.

2. *Ринок охорони здоров'я:*

– лікарні, в яких відбувається збір даних про стан хворих. Привабливість для хакерів становлять вразливості, що виникають від усе більш підключених медичних пристроїв. Система електронних медичних записів є основним інструментом, що використовується для збору клінічних даних та даних, пов'язаних із платежами. Даний сегмент є найбільш ризиковим, адже вартість захисних програм дуже висока і лікарні не здатні придбати їх;

– фармацевтичні компанії як установи, які мають величезний обсяг цінної особистої інформації, тому вже давно визначаються як чіткі цілі для нападу;

– виробники медичних виробів, які потребують захисту. Керування сучасними фармацевтичними підприємствами відбувається з використанням Інтернет-технологій, що також робить їх уразливими щодо хакерських атак.

Сьогодні немає жодної галузі, в якій не використовуються Інтернет-технології, відповідно, не існує жодної галузі як на національному, так і на світовому ринку, яка б не була в зоні ризику від кіберзагроз [3]. Наведемо приклади наймаштабніших кібератак на світовий ринок:

– Фірма електронної пошти Epsilon утратила 225 млн дол. США загальних витрат унаслідок нещодавнього порушення даних, масштабної події, яка свідчить про часто недооцінений ризик хмарних обчислювальних систем.

– Порушення Epsilon зачепило 75 компаній, або 3% клієнтів Epsilon, а не 2%, як повідомлялося раніше, це в кінцевому підсумку може коштувати цим компаніям у цілому 412 млн дол. Загальна вартість утрат становила 637 млн дол. Окрім того, CyberFactors консервативно оцінили кількість постраждалих електронних листів у порушенні Epsilon у 60 млн дол.

– Нещодавній розрив служб хмарних обчислень Amazon, який порушив послуги на популярних сайтах, таких як Foursquare і Quora, є ще одним прикладом відмови у хмарі, яка може виявитися вкрай дорого в довгостроковій перспективі.

– У 2018 р. найбільша у світі мережа готелів зазнала чергового масштабного порушення даних. Система бронювання дочірніх компаній Marriott Starwood, яка містила особисті дані 500 млн клієнтів, була порушена через несанкціонований доступ. Це порушення було особливо тривожним, оскільки поряд з іменами, адресами, електронними листами та номерами телефонів деякі викрадені записи включали номери паспортів, місця подорожі та номери кредитних карток. Інцидент виявився ще більш згубним, оскільки хакери отримали доступ до гостьової бази Starwood із 2014 р.

Проведений аналіз довів, що хакерські атаки стають усе більш агресивними в кіберпросторі, створюючи економічне середовище, яке мало хто розуміє і до якого готується ще менше [2].

Для більш чіткого розуміння проблематики в табл. 1 нами подано інциденти, пов'язані з кіберзагрозами, та їхній вплив на економічний розвиток країн за 2019 р.

Отже, проведений нами аналіз дав змогу визначити основні тенденції в галузі кібербезпеки, на які слід звернути увагу та які необхідно подолати [6]:

1. *Вибух кіберзлочинності.* До 2021 р., за прогнозами, кіберзлочинці обійдуться світовій економіці понад 6 трлн дол. щорічно, що перевищує 3 трлн дол. у 2015 р. Можливо, ніде ця тенденція не є більш вираженою, ніж у бізнес-секторі.

Понад 43% американських підприємств зазнали порушень кібербезпеки за останні 12 місяців (згідно з опитуванням порушень кібербезпеки у 2018 р.), і щонайменше під 50 кібератак щомісяця потрапляють понад чотири з п'яти (83%) фінансових компаній. Дані атаки мають свою особливість. Як тільки хакери отримують доступ до цих мереж, вони в середньому залишаються непоміченими (6–12 місяців). За цей час вони крадуть інтелектуальну власність, поширюють критичні дані і, таким чином, доводять діяльність компанії до хаосу.

Середня вартість порушення корпоративної кібербезпеки сьогодні становить від 1,25 до 8,19 млн дол. Це роз'яснює привабливість кібератак та їх процвітання.

2. *Економічна війна з підтримкою кібератак.* Десятиліттями провідні країни світу дотримувалися свідомої стратегії використання своїх зовнішньополітичних та розвідувальних спільнот для копіювання та крадіжки технологій. Ці стратегії починають давати значущі результати, адже кілька закордонних технологічних компаній зараз законно конкурують з американськими лідерами технологій як за інноваціями, так і за ринковою капіталізацією. Якщо залишити дане питання без розгляду, це може стати викликом не тільки для нашої економічної безпеки, а й для нашої більшої національної безпеки.

3. *Зростаюче використання програм проти підприємств та урядів.* Яскравим прикладом у цьому питанні є Ransomware, яке, як і будь-яке шкідливе програмне забезпечення, обмежує чи заважає комусь користуватися своїм комп'ютером або доступом до файлів. У 2017 р. ця загроза вийшла на зовсім новий рівень. Після зростання на 4,3% варіантів викупового програмного забезпечення (включаючи атаки WannaCry та NotPetya), які стали глобальними для щонайменше 15% підприємств, які увійшли до топ-10 галузей промисловості, були заражені, а майже третина постраждалих була вимкнена зі своїх систем протягом п'яти і більше днів. Слід звернути

Таблиця 1

Перелік інцидентів, пов'язаних із кіберзагрозами у 2019 р.

№ п/п	Назва місяця	Інциденти за 2019 р.
1.	Грудень	– імовірна китайська групова хакерська група напала на державні установи та керувала постачальниками послуг, минаючи двофакторну автентифікацію; – підозрювана в'єтнамська державна хакерська група напала на мережі BMW та Hyundai; – Microsoft виграла судову боротьбу за контроль над 50 вебдоменами, які використовувала північнокорейська група хакерів для націлення на державних службовців, експертних центрів аналітичного центру, працівників університету
2.	Листопад	– дослідники з питань безпеки Microsoft виявили, що в минулому році іранська хакерська група здійснила «розбризкування пароля» на тисячі організацій; – імовірний недержавний актор націлив на британську партію лейбористів велику атаку DDoS, яка тимчасово зняла комп'ютерні системи партії в автономному режимі
3.	Жовтень	– було встановлено, що рекламований урядом китайський пропагандистський додаток із більш ніж 100 млн користувачів запрограмовано мати задній пристрій, що надає доступ до даних про місце знаходження, повідомлення, фотографії та історію перегляду, а також віддалено активує аудіозаписи; – державна авторизована хакерська кампанія збила в автономному режимі понад 2000 вебсайтів по всій Грузії, включаючи вебсайти уряду та суду, що містять матеріали справ та особисті дані; – китайські хакери взяли участь у багаторічній кампанії між 2010 та 2015 рр. із метою придбання інтелектуальної власності у іноземних компаній для підтримки розвитку китайського авіалайнера C919
4.	Вересень	– Airbus виявив, що хакери, націлені на комерційну таємницю, займалися серією атак на ланцюги поставок, націлених на чотирьох субпідрядників компанії; – китайська державна хакерська група, відповідальна за напади на три американські комунальні компанії в липні 2019 р., виявила, що згодом націлила на сімнадцять інших; – Huawei звинуватив уряд США у втручанні в його внутрішню мережу та внутрішні інформаційні системи та порушенні його ділових операцій
5.	Серпень	– Китай використовував компрометовані вебсайти для розповсюдження зловмисного програмного забезпечення серед населення Уйгуру, використовуючи раніше не розкриті подвиги для телефонів Apple, Google та Windows; – виявлено, що китайські хакери, які фінансуються державою, націлили кілька американських ракових інститутів для отримання інформації, що стосується передових досліджень у галузі раку
6.	Липень	– китайські хакери, які фінансуються державою, провели акцію підводного підбору проти працівників трьох великих американських комунальних підприємств; – виявлено, що китайська хакерська група націлила державні установи по всій Східній Азії, які займалися інформаційними технологіями, зовнішніми справами та економічним розвитком; – урядові відомства Хорватії зазнали нападів під час низки нападів невстановлених державних хакерів
7.	Червень	– урядові відомства Хорватії зазнали нападів під час низки нападів невстановлених державних хакерів; – американський регулятор енергоресурсів NERC виніс попередження про те, що велика група злому, у якої підозрюються російські зв'язки, проводить розвідку в мережі електричних мереж
8.	Травень	– Іран розробив мережу вебсайтів та облікових записів, які використовувалися для поширення неправдивої інформації про США, Ізраїль та Саудівську Аравію; – повідомлялося, що під керованою владою Китаєм хакерською групою було націлено на невстановлених осіб на Філіппінах
9.	Квітень	– хакери використовували підроблені електронні адреси для проведення дезінформаційної кампанії у Литві, щоб дискредитувати міністра оборони, поширюючи чутки про корупцію; – гонконгський офіс Amnesty International оголосив, що став жертвою нападу китайських хакерів, які отримали доступ до особистої інформації прихильників офісу
10.	Березень	–держава підтримала в'єтнамські хакери, спрямовані на іноземні автомобільні компанії на придбання IP; – урядовці США повідомили, що щонайменше 27 університетів у США були націлені китайськими хакерами в рамках кампанії з розкрадання досліджень військово-морських технологій
11.	Лютий	– Європейська аерокосмічна компанія Airbus виявляє, що націлили її на китайські хакери, які вкрали особисту та IT-ідентифікаційну інформацію деяких її європейських співробітників; – Міністерство юстиції США оголосило про операцію зі зриву північнокорейського ботнету, який використовувався для націлювання на компанії в засобах масової інформації, аерокосмічній, фінансовій та критичній інфраструктурі
12.	Січень	– Міністерство національної оборони Південної Кореї оголосило, що невідомі хакери порушили комп'ютерні системи в міністерстві; – колишні американські спецслужби, як було виявлено, працюють в ОАЕ, щоб допомогти країні проникнути до телефонів активістів, дипломатів та іноземних урядовців

увагу на той факт, що після подібних атак WannaCry та NotPetya, їхні організації так і не здійснили ніяких шагів для посилення безпеки своїх систем.

Глобальні напади викупних програм коштували приватним особам та бізнесу 5 млрд дол. у 2017 р., що на 400% більше порівняно з минулим роком. Але зараз ці напади роблять поворот до атак уряду.

Висновки. Зважаючи на те, що кібератаки (віруси, приманка, атаки, фітинг та ін.) залишаються найпоширенішими методами загроз, стає очевидним, що хакери зосереджуються на використанні саме людського фактору як головної слабкості. Навіть добре розроблені системи безпеки можуть бути підірвані за допомогою одного шкідливого діяння, спрямованого на людський фактор.

Витрати від кібзагроз не закінчуються на технічних втратах. Фінансовий вплив кібератаки, окрім основних витрат на відновлення інформації, може також включати витрати на страхування, вплив на поведінку клієнтів, витрати на судові процеси, штрафи та вплив на технологічну інфраструктуру та витрати на науково-дослідну роботу.

Проведений нами аналіз впливу кібератак на світовий економічний ринок довів необхідність у постійному оновленні програмних продуктів, які допоможуть ефективно запобігти даним атакам. Мережа, яка погано захищена, дає можливість хакерам здійснювати атаки через задні двері мережі навіть не помічаючи її.

Наймогутніші компанії світу, такі як Microsoft, Google та Facebook, витрачають близько 1 млрд дол. на рік на забезпечення своїх продуктів та пропозицій. Дуже невелика кількість компаній мають ресурси або технічний талант цих технічних титанів, а менші компанії стикаються з багатьма тими ж загрозами, включаючи все більше зростаючу кількість атак.

Отже, виникає потреба в більш широкому аналізі питання впливу кіберзагроз, що й буде результатом наших подальших досліджень.

Список літератури:

1. Про рішення Ради національної безпеки і оборони України «Про виклики та загрози національній безпеці України у 2011 році» : Указ Президента України від 10 грудня 2010 р. № 1119. *Офіційний сайт Верховної Ради України*. 2010. URL : http.//rada.gov.ua (дата звернення: 29.02.2020).

2. Грайворонський М.В. Сучасні підходи до забезпечення кібернетичної безпеки. *Теоретичні і прикладні проблеми фізики, математики та інформатики :* матеріали XIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих учених, м. Київ, 21–23 травня 2015 р. Київ : НТУУ «КПІ», 2015. С. 10–17.

3. Рудник Л.І. Право на доступ до інформації : дис. … канд. юрид. наук : 12.00.07. Київ, 2015. 247 с.

4. Лахно В.А. Побудова адаптивної системи розпізнавання кіберзагроз на основі нечіткої кластерізації ознак. *Восточноевропейский журнал передових технологій*. 2016. № 2(9). С. 18–25. DOI : 10.15587/1729-4061.2016.85600.

5. Панченко В.М. Зарубіжний досвід формування систем захисту критичної інфраструктури від кіберзагроз. *Інформаційна безпека людини, суспільства, держави.* 2012. № 3(10). С. 100–109.

6. Запорожець О.Ю. Кібервійна: концептуальний вимір. *Актуальні проблеми міжнародних відносин*. 2014. Вип. 121. Ч. І. С. 80.

7. Kitchen K. A major treats to our economy – three cuber trends he US must address to protect itself, 2019, *The heritage foundation :* вебсайт. URL : https://www.heritage.org/cybersecurity/commentary/major-threat-our-economy-three-cyber-trends-the-us-must-address-protect (дата звернення: 29.02.2020).

References:

1. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy «Pro vyklyky ta zahrozy natsionalnii bezpetsi Ukrainy u 2011 rotsi» : Ukaz Prezydenta Ukrainy vid 10 hrudnia 2010 r. № 1119 (2010) [On the Decision of the National Security and Defense Council of Ukraine "On Challenges and Threats to National Security of Ukraine in 2011": Presidential Decree No. 1119 of December 10, 2010]. *Ofitsiinyi sait Verkhovnoi Rady Ukrainy*. Available at: http.//rada.gov.ua (accessed 29.02.2020).

2. Grayvoronskyi M. V (2015) Suchasni pidkhody do zabezpechennia kibernetychnoi bezpeky [Current approaches to cyber security]. Proceedings of the *Teoretichni ta prikladni problem fiziki, matematiki na informatiki* (Kyiv, Ukraine, May 21-23, 2015), Kyiv : NTUU «KPI». pp. 10-17

3. Rudnik L. I. (2015) Pravo na dostup do informatsi [Right to access information] (PhD Thesiss) Kyiv: National University of Life and Environmental Sciences of Ukraine.

4. Lahno V. A. (2016) Pobudova adaptyvnoi systemy rozpiznavannia kiberzahroz na osnovi nechitkoi klasterizatsii oznak [Construction of an adaptive cyber-threat recognition system based on fuzzy feature clustering]. East European Journal of Advanced Technology, № 2(9), pp. 18-25. DOI: 10.15587/1729-4061.2016.85600.

5. Panchenko V. M. (2012) Zarubizhnyi dosvid formuvannia system zakhystu krytychnoi infrastruktury vid kiberzahroz [Zarubizhny dosvid formvannya systems zystu critical infrastructure id kiberzagroz]. *Information security of the person, society, state*, no. 3 (10), pp. 100-109.

6. Zaporogec O. U. (2014) Kiberviina: kontseptualnyi vymir [Cyberworld: a conceptual dimension]. *Topical problems of international relations*, no. 121, p. I, pp. 80.

7. Kitchen K. (2019) A major treats to our economy – three cuber trends he US must address to protect itself. *The heritage foundation.* Available at: https://www.heritage.org/cybersecurity/commentary/major-threat-our-economy-three-cyber-trends-the-us-must-address-protect/ (accessed 29.02.2020).

АНАЛИЗ ВЛИЯНИЯ КИБЕРУГРОЗ НА МИРОВОЙ ЭКОНОМИЧЕСКИЙ РЫНОК

Статья посвящена исследованию основных киберугроз и их влиянию на мировой экономический рынок. Проведенный анализ позволил определить основные процессы, которые привели к росту возможных рисков от воздействия кибератак в 2019 г. Раскрыты основы, которые влияют на различные бизнес-процессы как на национальном, так и международном рынках. Исследованы наиболее уязвимые зоны для хакерских атак. Представлен перечень инцидентов, связанных с киберугрозами в 2019 г. Выделены основные тенденции в области кибербезопасности, которые необходимо преодолеть. Определено, что финансовое воздействие от кибератак может включать расходы на страхование, влиять на поведение клиентов, включать расходы на судебные процессы, штрафы и влияние на технологическую инфраструктуру, а также расходы на научно-исследовательскую работу. Доказана необходимость в постоянном обновлении программных продуктов, которые помогут эффективно предотвращать подобные атаки.

Ключевые слова: *кибербезопасность, киберпреступность, хакерские атаки, экономические угрозы, риски, мировой экономический рынок.*

ANALYSIS OF THE IMPACT OF CYBER THREATS ON THE WORLD ECONOMIC MARKET

This article is dedicated to exploring major cyberthreats and their impact on the global economic market. The analysis made it possible to identify the major processes that lead to increasing risks of cyberattacks in 2019. Most important of the seare the need form or esecured at a storage facilities to protect them, as well as the introduction of new technology that is faster than cybersecurity can solve. By 2021, cyber criminals are projected to cost the world economy over $ 6 trillion annually, inexcessof $ 3 trillionin 2015. Therefore, this trend is most pronounced in the business sector. It should be noted that the seat tack shave their own peculiarity. As soon as hackersgain access to these net works, theyr emain unnoticed on average (6-12 months). This explains the attractive nessand prosperity of cyberattacks. During this time, they stealin tell ectual property, dissemin at ecritical data, and thus bring the company's activity to chaos. The analys is proved that hacker attack sare becoming more aggressive in cyber space, creating an economic environment that few understand and a repreparing for evenless. Foundations that affect various business processesin both the national andinternational markets, including fraudulent emails, viruses / spyware / malware, ransomware, unauthorizedaccess, denial-of-service attacks, aredisclosed. The major vulnerabilities identifi ed by the financial markets (banks, securiti es companies and market infrastructure providers), as well as the health care market (hospitals, pharmaceutical companies, medicaldevices manufacturers) are identified. Examples of cyberthreats incidents in 2019 are presented. Key trend sincyber security have been identified, such as the explosion of cybercrime, the economic war with support for cyberattacks, and the increasing use of program sagainst businesses and governments. It has been proven thatc yberattack financial impact caninclude-insuranc ecosts, affect customer behavior, include litigation costs, fines, and impacton technology infrastructure and research costs. It should be noted that cyberattacks (viruses, bait, attacks, phishing, etc.) remain the most common methods of threats, it be comesap parent that hackers focus on using the human factoras a weakness. So, today there is a need for constant updating of software products that will help to prevent these attacks effectively.

Key words: *cybersecurity, cybercrime, hackerattacks, economicthreats, risks, theworldeconomicmarket.*