конфіденційних даних, що застосовуються при прийнятті управлінських рішень, вагоме місце в забезпеченні інвестиційної безпеки відіграє рівень інформаційної безпеки.

Основні заходи щодо підвищення інвестиційної безпеки України в сучасних умовах наступні: оновлення основних виробничих фондів; структурна перебудова економіки; підвищення рівня кластеризації регіонів; використання інноваційного потенціалу країни; підвищення ефективності інноваційної діяльності; вдосконалення механізмів фінансування інвестиційних проектів; використання пільгового оподаткування та механізмів державної підтримки розвитку бізнесу; розвиток інфраструктури інвестиційних об'єктів.

Отже, не зважаючи на економічну кризу та інші негативні явища в країні, можна сказати, що Україна й зараз залишається привабливою для інвестицій. Водночас вона не знаходиться осторонь світових процесів, є достатньо інтегрованою у світове господарство і порушення макростабільності на зовнішніх ринках має свій відголос в Україні також.

Список використаних джерел

1. Барановський О. І. Фінансова безпека в Україні (методологія оцінки та механізми забезпечення): монографія. Київ: Київ. нац. торг.-екон. ун-т, 2004. 759 с.

2. Кириленко В.І. Інвестиційна складова економічної безпеки: монографія / В.І. Кириленко. – К.: КНЕУ, 2005. – 232 с.

3. Про затвердження Методики розрахунку рівня економічної безпеки України № 60: наказ Міністерства економіки України від 02.03.2007 / [Електронний ресурс]. – Режим доступу: http://zakon.nau.ua

4. Шлемко В. Т., Бінько І. Ф. Економічна безпека України: сутність і напрямки забезпечення. Київ: НІСД, 2007. 280 с.

Лозова А. Д., студентка гр. МФПп-201
Сидоренко А. В., студентка гр. МФПп-201
Науковий керівник – **Парубець О. М.,** д.е.н., професор
Національний університет «Чернігівська політехніка» (м. Чернігів, Україна)

СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Наш час можна сміливо назвати епохою інформаційного суспільства, адже інформаційні технології та телекомунікаційні системи відіграють значну роль в усіх сферах життєдіяльності населення, бізнес-структур та держави в цілому. Впровадження інформаційних технологій, цифровізація економіки прискорює з одного боку розвиток науково-технічного прогресу, з іншого збільшує кількість кібератак. За даними опублікованими Українським інститутом майбутнього в умовах пандемії кількість кіберзлочинів зросла на 300 % і до 2021 року у світі планувалося витратити на забезпечення кібербезпеки 6 трильйонів доларів США. Згідно з оцінками університету Меріленд, у світі кібератаки відбуваються кожні 39 секунд і найбільша їх кількість, а саме 95 % відбувається по причині впливу людського фактору, тобто спричинених людиною помилок.

На початок 2020 року за оцінками Міжнародного союзу електрозв’язків, Інтернетом користувалося трохи більше 51% населення Землі, або 4 мільярди чоловік.

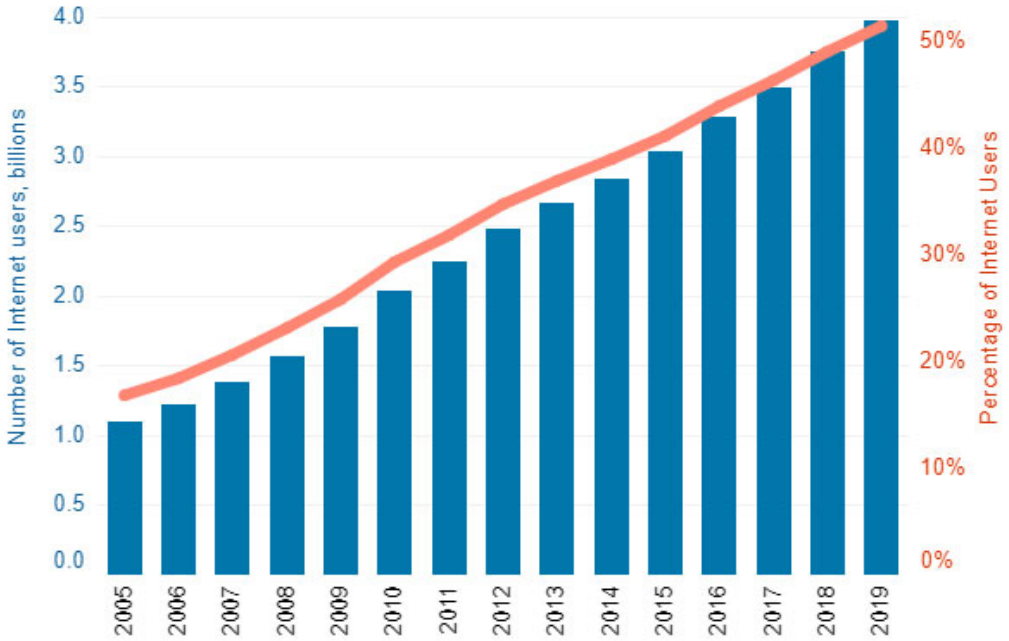

Рисунок 1 –. Кількість користувачів Інтернетом в світі, 2005-2019
Джерело : складено авторами на основі [1]

Але щоденно контактуючи пліч-о-пліч з телекомунікаціями і глобальною комп'ютерною мережею, слід розуміти, які можливості для злочинів створюють ці інформаційні та цифрові технології. Жертвами хакерів в наш час стають не тільки окремі фізичні і юридичні особи, але і держави в цілому.

Після кібератак шкода може бути колосальною, а наслідки – непоправними. Найпоширенішими з них є: пропаганда, збір секретної інформації, відмова сервісу, втручання в роботу обладнання, атаки на об'єкти критичної інфраструктури тощо. Тому забезпечення кібербезпеки є одним із найактуальніших напрямів досягнення національної та економічної безпеки країни.

У сьогоднішній цифрової реальності кіберзагрози розвиваються прискореними темпами, а шкідливі кіберзлочинці стають все більш витонченими, краще організованими та транснаціональними. При поширенні кіберзагроз вкрай важливо, щоб суб'єкти національної системи кібербезпеки мали точне уявлення про цю проблему, адекватні сучасні інструменти, а також необхідні ресурси для її вирішення з урахуванням впливу ендогенних і екзогенних факторів.

Пандемія COVID-19 призвела до розширення використання інтернету та залежності людей від нього, оскільки майже всім довелося працювати і вчитися вдома. Під час кризи кібератаки також посилилися в усьому світі, в тому числі проти критично важливих медичних установ, які були метою атак шахраїв, що використали скрутну ситуацію в своїх особистих інтересах.

Автори роботи [3] зазначають, що розвиток у сфері боротьби з міжнародною та національною кіберзлочинністю було започатковано з підписанням Конвенції Ради Європи про кіберзлочинність. Згідно до зазначеного документу передбачено кримінальну відповідальність на національному рівні за такі групи злочинів: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями); комп'ютерні правопорушення (підробка та шахрайство із застосуванням комп'ютерів); правопорушення, пов'язані зі змістом (правопорушення, пов'язані з дитячою порнографією); правопорушення віднесені до порушення авторських та суміжних прав [3]. У вересні 2005 р. до зазначеної Конвенції приєдналася Україна. При цьому Україна залишила за собою право повністю або частково не застосовувати вищезазначені статті Конвенції.

Згідно до Національного індексу кібербезпеки 2020 розробленого академією Belter Center,серед 160 країн світу за підсумками 2019 р. Україна посіла 25 місце і у порівнянні з 2018 р. піднялася у рейтингу на п'ять позицій [4]. У той же час за оцінкою компанії Specops Software наша держава посідає 6 місце серед 10 країн світу, на які здійснювалися найнебезпечніші кібератаки, загальною кількістю 16 одиниць у період з травня 2006 р. по червень 2020 р.[5].

Для забезпечення кібербезпеки Україна повинна використовувати такі рівні захисту своєї інформації:

– запобігання — доступ до певного виду інформації та технологій надається тільки певній кількості людей, які отримали до цього доступ та мають відповідні фахові навички;

– виявлення — виявлення злочинів і зловживання на ранніх сталях, навіть якщо злочинцям вдалося обійти механізми захисту

– обмеження — зменшення розміру втрат, якщо все ж таки злочин скоєний, попри те що заходи для його запобігання і виявлення були здійснені

– відновлення — забезпечення ефективного відновлення втраченої інформації за наявності всіх документів і перевірених планів з відновлення.

Посилення кібербезпеки в Україні потребує перш за все розвитку кіберстрахування як перспективного сектору страхового ринку України [5,6]. Також необхідно посилити кримінальну відповідальність за вчинені кіберзлочини, особливо на державні органи та об'єкти критичної інфраструктури; фінансово підтримувати фундаментальні та прикладні дослідження у сфері боротьби з кіберзлочинністю та кібератаками; удосконалити існуючі законодавчо-нормативні акти та розробити низку нових спрямованих на розвиток міжнародного співробітництва в напряму забезпечення кібербезпеки; робробити ефективні напрями державної політики в сфері забезпечення кібербезпеки та зменшення кількості кібератак.

Список використаних джерел

1. Кібербезпека. Новий підхід в Україні. URL : https://uifuture.org/publications/kiberbezpechna-ukrayina-novyj-pidhid/

2. Бойко В.Д., Василенко М. Д., Кухаренко С. В. Кібербезпека в ЄС та країнах-членах: генезис та проблеми її підвищення. Національна академія служби безпеки України. URL : http://academy.ssu.gov.ua/ua/page/page_1581426437.htm

3. Про ратифікацію Конвенції про кіберзлочинність Закон України від 07.09.2005 URL :https://zakon.rada.gov.ua/laws/show/994_575#Text

4. Specops Software. URL https://specopssoft.com/case-studies/

5. Ільчук В. П., Парубець О. М., Сугоняко Д. О. Інноваційні підходи до розвитку ринку кіберстрахування в Україні [електронний ресурс]. ефективна економіка. – 2018. – № 5. – режим доступу: http://www.economy.nayka.com.ua/?op=1&z=6295.

6. Парубець О. М., Гонта О. І. проблеми забезпечення кібербезпеки в Україні. мультисекторальна безпека соціально-економічного розвитку в умовах інформатизації суспільства : матеріали наук.-практ. круглого столу (М. чернігів, 13 груд. 2017 р). – Чернігів : ЧНТУ, 2017. – с. 19-21.