взаємозв'язків. Не менш важливими є пошук інструментів фінансово-інвестиційної підтримки МСП і розробка механізму спрощеної системи оподаткування для інвесторів МСП.

Бібліографічні посилання

1. Гусєв В. О. Державна інноваційна політика: методологія формування та впровадження : монографія. Донецьк : Юго-Восток, 2011. 624 с.
2. Макаренко І. П., Трофимчук О. М., Кузьменко В. П. Проблеми становлення інноваційної політики в Україні / за ред. І. П. Макаренко. Київ : УІДНСРіР: Ін-т еволюц. економіки, 2004. 123 с.
3. Про інноваційну діяльність : Закон України в поточній ред. від 05.12.2012 р. URL : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=40-15.
4. Horiashchenko Y., Taranenko I., Yaremenko S., Shevchenko V., Mishustina T., Klimova I. Integrated System of Enterprises' Innovative Development Management Under the Conditions of Post-Fordism. Postmodern Openings. 2021. Vol. 12. Issue 3 Sup1. S. 45–60.
5. Юринець З. В. Формування інноваційних стратегій: теорія, методологія, практика : монографія. Львів : СПОЛОМ, 2016. 412 с.

Гребенюк А. М.,
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

КІБЕРЗЛОЧИННІСТЬ В УКРАЇНІ

Широке впровадження комп'ютерів в усі види діяльності, постійне нарощування їхньої обчислювальної потужності, використання комп'ютерних мереж різного масштабу призвели до того, що загрози втрати конфіденційної інформації в системах обробки даних стали невід'ємною частиною практично будь-якої діяльності [1].

На сьогодні в зв'язку з карантином та дистанційною формою праці з впровадженням хмарних технологій та розвитком торгових платформ кількість кіберзлочинів в Україні за останні два роки збільшилась.

Кіберзлочинці можуть полювати за персональними даними, банківськими рахунками, паролями та іншою інформацією, яка наявна в електронному вигляді, а також, використовуючи різні платформи по продажу товарів та послуг, виманювати гроші. Потерпілими можуть стати як звичайні люди, так і будь-які підприємства.

Кіберзлочини бувають:

- спрямовані на заволодіння коштами;
- спрямовані на заволодіння інформацією (для власного

використання або для подальшого продажу);

– втручання в роботу інформаційних систем (для навмисного пошкодження за винагороду або через хуліганство);

– поширення спаму і вірусних програм тощо.

Всі ми добре пам'ятаємо, як у 2017 році в Україні відбулася масштабна атака вірусом Petya: були вражені енергетичні компанії, українські банки, аеропорт «Бориспіль», аеропорт Харкова, Чорнобильська АЕС, урядові сайти, київський метрополітен тощо. Подібного безпрецедентного масштабного вторгнення в сервери вітчизняних компаній наша країна ще не знала. За даними експертів Міжнародного валютного фонду, економічні втрати від атаки вірусу Petya становили приблизно 850 млн доларів. При цьому заяви потерпілих компаній в кіберполіцію про втрату даних часто залишалися без відповіді, адже знайти і притягнути до відповідальності зловмисника в цьому разі виявилося неможливо. На рис. 1 наведені у відсотках збитки компаній в Україні за 2020 р.

Сьогодні практично всі фахівці у сфері інформаційних технологій визнають, що ситуація з кіберзлочинністю у світі погіршується. Організована злочинність все частіше і частіше використовує Інтернет з метою приховування своєї діяльності. Зараз нікого не здивуєш існуванням мережі «Даркнет», за допомогою якої злочинці фактично створили чорний ринок для збуту наркотиків, зброї, крадених товарів тощо. Завдяки технологіям, які забезпечують мережеву анонімність, ця частина Інтернету залишається абсолютно безконтрольною, а тому безпечної для діяльності різних злочинних угруповань. За даними, наданими Національною поліцією України, кількість організованих груп і злочинних організацій, що здійснюють кримінальні правопорушення з використанням високих інформаційних технологій, за останній рік збільшилася на 36 %.

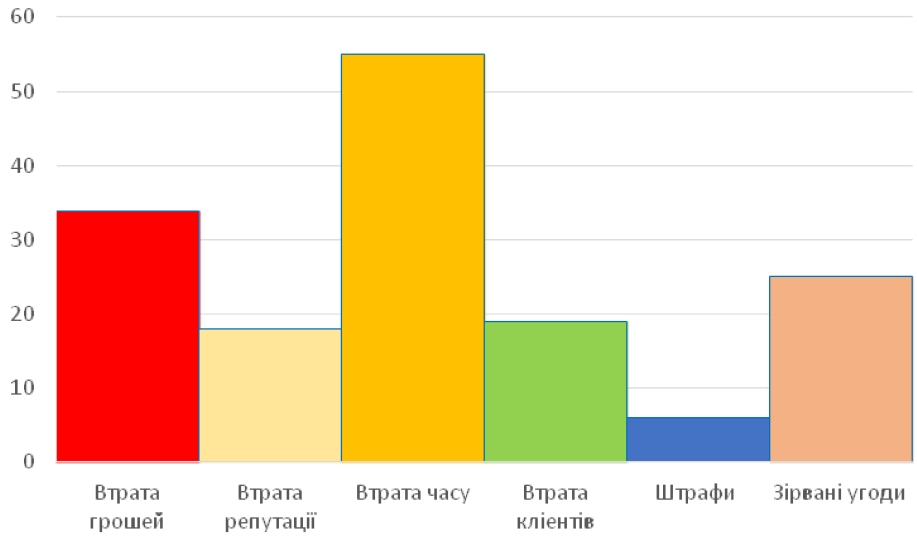

Рис. 1. Збитки компаній внаслідок кіберзлочинів

Закон України «Про основні засади забезпечення кібербезпеки України» визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Український Кримінальний кодекс передбачає 4 статті за інформаційні злочини [2]:

– Ст. 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

– Стаття 361-1. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут незалежно від того, робиться це безкорисливо або за гроші.

– Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації

– Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (якщо ви перед звільненням знищите на своєму службовому комп'ютері важливу інформацію, то ваші дії підпадають під цю статтю).

Збільшення кількості таких злочинів в останні два роки (рис. 2) великою мірою пов'язано з тим, що поступово штат співробітників кіберполіції все-таки розширюється і відповідно більше порушується кримінальних справ. Але, на жаль, левова частина таких справ не доходить до суду або розвалюється в суді через погане збирання доказів слідчими органами [3].

До основних способів допомоги в боротьбі з кіберзлочинністю належать централізоване впровадження основних заходів безпеки, підвищення прозорості з боку організацій та урядів, стандартизація і координація вимог кібербезпеки, навчання співробітників обізнаності про кібербезпеки і розробка планів запобігання і реагування.

Зараз в нашій країні пріоритетними внутрішньополітичними напрямами для розвитку є саме кібербезпека і протидія кіберзлочинності. Тому будемо сподіватися, що рівень безпеки в інтернет-просторі України незабаром підвищиться, а популярні шахрайські схеми в мережі будуть знищені.

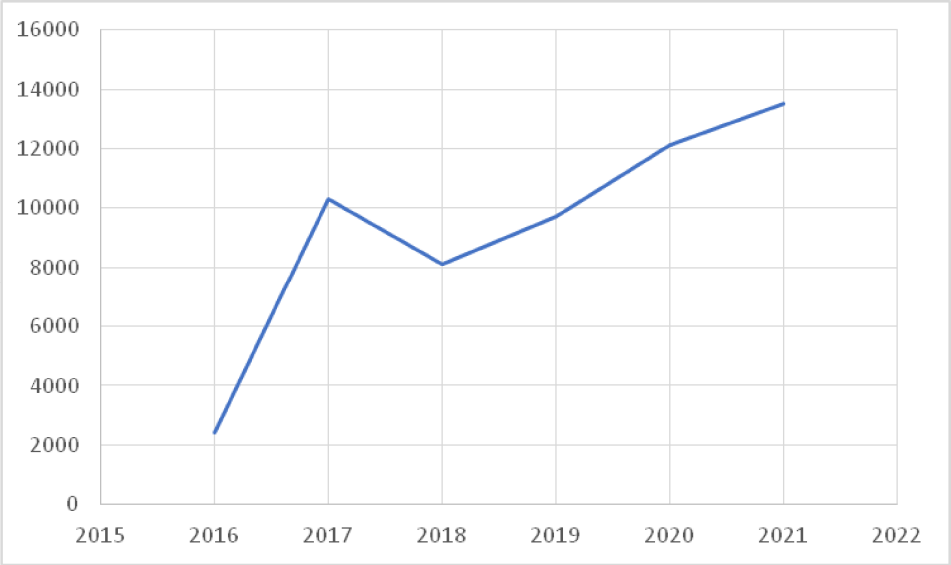

Рис.1. Судові рішення щодо кіберзлочинів в Україні

Але для цього потрібно змінювати та вдосконалювати законодавчу базу для швидкого реагування представників кіберполіції.

Бібліографічні посилання

1. Вишня В. Б., Гавриш О. С., Рижков Е. В. Основи інформаційної безпеки : навч. посіб. Дніпро : Дніпропетр. держ. ун-т внутр. справ, 2020. 126 с.
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/T172163.html
3. Кримінальний кодекс України. URL: https://kodeksy.com.ua/kriminal_nij_kodeks_ukraini/statja-361.htm
4. Opendatabot. URL: https://opendatabot.ua/blog/ru/375-hackers
5. Платформа LIGA:ZAKON. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/EA013606.html

Дараган В. В., завідувач кафедри оперативно-розшукової діяльності Дніпропетровського державного університету внутрішніх справ, доктор юридичних наук, доцент

ДЕЯКІ ПРОБЛЕМИ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ БЮРО ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ

22 березня 2021 року Президент України Володимир Зеленський підписав Закон України «Про Бюро економічної безпеки України» № 1150-IX, який Верховна Рада України ухвалила 28 січня 2021 р. Як зазначив Глава