Завдяки цьому процесу значно скорочується цикл звітності та надається можливість торговим представникам використовувати найбільш точні дані для підвищення прибутковості своїх продажів.

Список літератури

1. *Курс акцій. URL:* https://www.google.com/finance/quote *(дата звернення: 15.11.2021)*
2. *IQVIA - компанія, що надає послуги у фармацевтичній та біофармацевтичній областях та корпоративного аутсорсингу. URL:* https://www.iqvia.com/ *(дата звернення: 15.11.2021)*
3. *Технологія для управління всіма відносинами та взаємодією компанії з клієнтами та потенційними клієнтами. URL:* https://crm.ua/ *(дата звернення: 15.11.2021)*
4. *What is Power BI? URL:* https://powerbi.microsoft.com/en-gb/what-is-power-bi/ *(дата звернення: 15.11.2021)*

УДК 004.8(075)

Крохмалюк В.В., здобувач освіти,
Потапова Н. А., к.е.н., доцент,
доцент кафедри інформаційних технологій

ПРОБЛЕМА КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Донецький національний університет імені Василя Стуса, м. Вінниця

Питання кіберзлочинності актуальне від самого початку розвитку інформаційних технологій. Майже усі сфери діяльності людини використовують інформаційні технології. Україна все більше вливається в цифрові новинки, а злочинці знаходять все більше можливостей для здійснення своїх планів.

Надзвичайно актуальною загрозою сьогодні є розвідувальна та підривна діяльність у кіберпросторі проти України, яка пов’язана з розвідувальною діяльністю іноземних держав, насамперед Російської Федерації, з метою розкрадання інформації (кібершпигунство) та диверсійних дій з метою порушення нормальної роботи критичні об'єкти. Кіберпростір використовується для фінансування терористичних груп.

Зростання кіберзлочинності в національному сегменті кіберпростору є широкомасштабною загрозою, яка завдає шкоди державним інформаційним ресурсам, публічним процесам, особисто громадянам, що знижує довіру населення до інформаційних технологій та призводить до значних матеріальних втрат. Ситуацію ускладнює низький рівень кіберграмотності населення, у тому числі й звичайних користувачів електронних послуг.

Державні інформаційні ресурси та об'єкти критичної інформаційної

інфраструктури, покликані забезпечити задоволення життєво важливих потреб громадянина, особи, суспільства і держави, недостатньо захищені від кібератак [1]. Кіберзлочинність – це поняття, яке охоплює комп'ютерну злочинність та інші зазіхання, де комп'ютер є знаряддям або способом злочину проти власності, авторських прав, громадської безпеки, моралі тощо [2].

Кіберзлочинність порушує приватне життя людей та безпеку їх даних, зокрема, злом, шкідливе ПЗ, крадіжка особистих даних, фінансове шахрайство, медичне шахрайство та певні правопорушення проти осіб, які включають розкриття особистої інформації, повідомлень, зображень, відео- та аудіозаписів без участі окремих осіб [3].

Проблема боротьби з кіберзлочинністю є однією з актуальних проблем для України. Закон України «Про ратифікацію Конвенції про кіберзлочинність» набрав чинності 1 липня 2006 року, але кримінально-процесуальне законодавство України наразі не відповідає положенням Будапештської конвенції. Це ускладнює судове переслідування злочинців, державно-приватне співробітництво та міжнародне співробітництво у роботі по боротьбі з кіберзлочинністю [4].

Згідно даних Державного департаменту США, повідомлення про онлайн-шахрайство та атаки на урядові міністерства та інформаційні портали України можуть обчислюватися тисячами щомісяця. А під час пандемії коронавірусу кількість інцидентів збільшилася, оскільки повсякденні справи переходять в онлайн [5]. Кіберзлочинність під час Covid-19 набула нових форм, зокрема: фішингові кампанії та розповсюдження шкідливих програм, програми-вимагачі, шахрайські схеми, дезінформація, кібершпигунство, darknet [6].

Основні суб'єкти боротьби з кіберзлочинністю в Україні є урядовою командою для реагування на комп'ютер надзвичайних ситуацій, Державний центр кіберзахисту та протидія кіберзагрозам CERT-UA, що діє в рамках Державного центру кіберзахисту держави служба спеціального зв'язку та інформації охорони України та розслідує інциденти в кіберпростір, аналізує вразливості інфраструктури, збирає інформацію про загрози, контролює стан захист і безпека інфраструктури.

Системою виявлення вразливостей і реагування на кіберінциденти та кібератаки на об'єктами моніторингу найбільше зафіксовані: спроби отримати права користувача - 49%; спроби отримати права адміністратора - 21%; порушення політики корпоративної безпеки – 7%; підозрілий виконуваний код - 11% . Переважна більшість з оброблених інцидентів належать до доменної зони UACOM (близько 99%). Основна кількість інцидентів стосується з: розповсюдження шкідливого ПЗ – 98%, несанкціонований доступ – 1%, фішинг – 1%. [7].

На сьогодні серед основних проблем в боротьбі з кіберзлочинністю в Україні є: недостатня координація політики; відсутність стратегії безпеки в кіберпросторі; відсутність виконання стратегічного плану; відсутність публічних звітів про загрози та кіберзлочинність; відсутність безпеки сайту; низький рівень компетентності початкової та середньої освіти в використання віртуального середовища; низька якість програми кібербезпеки на рівнях

бакалавра та магістра; відсутність асоціацій кібербезпеки [10].

В Україні за чотири місяці 2021 року, порівняно з минулим, кількість кіберзлочинів зросла на 25%. Зафіксували понад 1100 інцидентів. В зону відповідальності кіберполіції входять порушення авторства контенту і суміжних прав, контент, який пов'язаний з насильством, наркотиками, екстремізмом, створенням і поширенням дитячої порнографії, насильством над дітьми.

Україна імплементувала в своє законодавство такі міжнародні стандарти: ISO:27001 (Системи управління інформаційною безпекою – Вимоги), ISO:27002 (Кодекс практики управління інформаційною безпекою), ISO:27005 (Управління ризиками інформаційної безпеки) та ISO:27006 (Вимоги до органів, що здійснюють аудит та сертифікацію систем управління інформаційною безпекою) [6].

Таким чином, більшість кіберзлочинів здійснено тому, що наше суспільство недостатньо обізнане у сфері інформаційних технологій. Одним із шляхів вирішення даної проблематики є розповсюдження інформації про користування технологіями серед усіх верст населення. Вагом чинником є встановлення більш швидкої комунікації з підрозділами кіберполіції, зокрема, через спеціалізовані засоби інформаційно-комунікаційного зв’язку.

Список літератури

1. *Безпечний кіберпростір – запорука успішного розвитку країни. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf.*
2. *Проблеми боротьби із кіберзлочинністю на міжнародному рівні. URL: https://internationalconference2014.wordpress.com/2014/10/09/%D0%BF%D1%80%D0%BE%D0%B1%D0%BB%D0%B5%D0%BC%D0%B8%D0%B1%D0%BE%D1%80%D0%BE%D1%82%D1%8C%D0%B1%D0%B8-%D1%96%D0%B7%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B7%D0%BB%D0%BE%D1%87%D0%B8%D0%BD%D0%BD%D1%96%D1%81/.*
3. *Privacy and Data Protection. UNOD. [e. d.], URL: https://www.unodc.org/e4j/en/cybercrime/module-10/key-issues/cybercrime-that-compromises-privacy.html/.*
4. *CyberEast Interview: On Legislative Development and Training Activities on Cybercrime in Ukraine.URL: https://www.coe.int/en/web/cybercrime/-/cybereast-interview-on legislative-development-and-training-activities-on-cybercrime-in-ukraine.*
5. *Ukraine plan to tackle hackers sparks privacy fears. URL: https://www.reuters.com/article/us-ukraine-lawmaking-cyber-analysis-trfn-idUSKBN26S1GG.*
6. *EUAM launches a series of webinars on tackling cybercrime during Covid-19. URL: https://www.euam-ukraine.eu/news/latest-news/euam-launches-a-series-of-webinars-on tackling-cybercrime-during-covid-19/.*
7. *Ukraine 2020 Crime & Safety Report. OSAC. [e.d], URL: https://www.osac.gov/Content / Report /cfdde1cb-f15e-4281-96af-1957c70ec6ec.*
8. *Cybersecurity in Ukraine.URL: https://www.lexology.com/library/detail.aspx?g=e5d42a92-c71b-4d92-bcb3-450f54013d59.*
9. *Кіберзлочини в Україні 2021.URL : https://www.rbc.ua/ukr/news/kolichestvo kiberprestupleniy-ukraine-2021-1622012394.html.*
10. *Overcoming Cybercrime in Ukraine (Cyberterrorism). URL: https://www.koreascience.or.kr/article/JAKO202121055560981.pdf.*