показників, що показують ступінь задоволеності потреб суспільства. Незважаючи на певні досягнення, що виражаються в зниженні споживання алкоголю, все ще є необхідність у проведенні заходів щодо збереження здоров'я нації в обмеженні споживання спиртного не стільки внаслідок заходів державного контролю над виробництвом і збутом алкогольної продукції, а внаслідок підвищення рівня життя і вдосконалення соціальних механізмів.

Отже, якісний моніторинг та аналіз економічної злочинності на споживчому ринку дозволить виробити своєчасні заходи протидії та забезпечити стале функціонування кожного з елементів споживчого ринку. Наближення до стійкої рівноваги за допомогою збалансованості між обсягом і структурою попиту населення та пропозиції матеріальних благ і послуг, між оборотом грошових і товарних ресурсів стане якісним результатом підтримки економічної безпеки.

Бібліографічні посилання

1. Сандул В. А. Злочини у сфері інтелектуальної власності – основний чинник економічної загрози споживчому ринкові України. Науковий вісник Львівського державного університету внутрішніх справ. Серія економічна. 2012. Вип. 1. С. 128–138. URL: http://nbuv.gov.ua/UJRN/Nvldu_e_2012_1_16
2. Ніпіаліді О. Б. Профілактика економічної злочинності як важливий напрямок діяльності правоохоронних органів: стан, тенденції, проблеми. *Актуальні проблеми правознавства*. 2020. Вип. 4. С. 61–67. URL: http://nbuv.gov.ua/UJRN/aprpr_2020_4_11
3. Денисов С. Ф., Філей Ю. В. Причини та умови злочинності у сфері економіки. *Криміналістика і судова експертиза*. 2021. Вип. 66. С. 272–283. URL: http://nbuv.gov.ua/UJRN/krise_2021_66_30

Кочкіна Д. А., курсант 2-го курсу
факультету підготовки фахівців
для органів досудового розслідування
Науковий керівник – Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
*(Дніпропетровський державний
університет внутрішніх справ)*

ВИТІК ДАНИХ ЯК ОДИН З ОСНОВНИХ РІЗНОВИДІВ КІБЕРАТАК

Україна в XXI сторіччі стала частиною всесвітньої науково-технічної революції, яка спричинила утворення нового інформаційного суспільства, що бере участь в економічному та соціальному розвитку країн всього світу. Проте з часом позитивним аспектам такої глобальної субстанції стала

загрожувати низка проблем, зумовлених високою вразливістю інфосфери щодо стороннього кібернетичного впливу. Інформаційний та кібернетичний простори піддаються таким кібератакам, як фішинг, атаки програм-вимагачів, шкідливі програмні забезпечення, витік даних, DDoS-атаки, атаки «людина посередника» (MitM), SQL-ін'єкції, експлойти нульового дня, атаки методом повного перебору (брутфорс) тощо. Наприклад, декілька років тому стався витік 2,5 мільйона облікових даних компанії Drizly, починаючи з 2013 року було розкрито номери кредитних карт більше ніж 10 млн клієнтів Prestige Software, і це вже не кажучи про витік даних із соціальних мереж. Отже, виникла потреба у створенні надійної системи кібернетичної безпеки для належного контролю над відповідними відносинами, що відіграє велику роль у геополітичній конкуренції більшості країн світу [1, с. 4].

Основними суб'єктами національної системи кібербезпеки України, що відповідають за становлення, розвиток і захист кіберпростору, є Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національний банк України, Міністерство інфраструктури України, Міністерство оборони України, Збройні сили України. Вони здійснюють свою діяльність на основі таких нормативно-правових актів, як: Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що ухвалюються на виконання законів України.

Зараз більшість організацій користуються багаторівневими системами обробки інформації (хмарні сховища, корпоративні мережі тощо) з метою передачі даних, які надалі перетворюються на можливий осередок їх витоку. Витік даних можна тлумачити як процес неконтрольованого розголошення (поширення) важливої приватної інформації.

Залишивши десь якусь інформацію, вам тут же надходить комерційна пропозиція, заснована на них; купивши автомобіль, на наступний день вам починають надходити дзвінки від компаній з пропозицією оформити страховку – це все є сигналами про те, що ваші особисті дані потрапили у відкритий доступ [4].

Для того щоб запобігти поширення через мережу ваших особистих даних, необхідно: по-перше, встановлювати складні багатоструктурні паролі, різні для кожного сайту; по-друге, уважно ознайомлюватись з умовами обробки персональних даних; по-третє, не встановлювати маловідомі додатки, що потребують доступу до даних стаціонарних, портативно персональних комп'ютерів чи смартфонів; по-четверте, не вводити логіни й паролі, перебуваючи в незнайомій Wi-Fi мережі (власник відповідної мережі

бачить ці дані, що може призвести до можливого їх витоку).

Для запобігання витоку комерційних даних є декілька дієвих методів, по-перше, це шифрування даних. Переваги цього способу полягають у простоті застосування (реалізація шифрування проводиться спеціальним ПЗ), у разі потреби передачі важливих електронних документів за межі комерційної мережі вони будуть зберігатися на флеш-носії, хмарному носії або в клієнтській пошті тільки в зашифрованому вигляді, високий ступінь надійності. По-друге, це контроль персоналу за допомогою систем обліку робочого часу, що характеризується як комплексне апаратне та програмне забезпечення, яке документує точний час прибуття на роботу, час виходу, діяльність персоналу за комп'ютером, записує листування корпоративної пошти, здійснює відеоспостереження і передає всі ці дані керівництву фірми або людині з відділу безпеки. Далі вся отримана інформація аналізується і виявляється кількість працівників, які могли поширювати комерційну таємницю [5].

Отже, в цій науковій роботі було зазначено поняття «витоку даних», яке можна визначити як один із видів кібератак, що відбувається, коли конфіденційна інформація користувача стає вразливою; перелічена низка методів, які слугують превентивними заходами щодо запобігання стороннього кібернетичного впливу. Також було надано перелік нормативно-правових актів, що регулюють цю сферу діяльності в Україні й допомагають накопичувати важливий досвід у захисті власної ІТ-інфраструктури, та органи, через які відбувається механізм їх реалізації.

Бібліографічні посилання

1. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект. Київ : Державний університет телекомунікацій, 2015. 4 с.

2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 10.10.2021).

3. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 45. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 10.10.2021).

4. Самые популярные виды кибератак в 2021. URL: https://10guards.com/ru/articles/the-most-common-types-of-cyber-attacks-in-2021/ (дата звернення: 10.10.2021).

5. Витік даних: як виявити та виправити? URL: https://indevlab.com/uk/blog-ua/vitik-danih-br-yak-viyaviti-ta-vipraviti/ (дата звернення: 10.10.2021).