Ковальчук А. Ю.,
доктор юридичних наук, професор,
начальник відділу дослідження проблем протидії
кіберзлочинності та загрозам інформаційній безпеці
Міжвідомчого науково-дослідного центру з проблем боротьби з
організованою злочинністю при РНБО України
(м. Київ, Україна)

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ: СУЧАСНІ ПІДХОДИ ТА ПЕРСПЕКТИВИ РЕАЛІЗАЦІЇ КОНВЕНЦІЇ ГЕНЕРАЛЬНОЇ АСАМБЛЕЇ ООН ВІД 24 ГРУДНЯ 2024 РОКУ

Сучасні масштабні кібератаки набули такого розмаху, що спричиняють руйнівні наслідки як і будь-яка фізична зброя на війні. У нових кримінальних інцидентах відмічається ускладнення кібератак: поєднання штучного інтелекту з удосконаленим шкідливим програмним забезпеченням, застосування методів соціальної інженерії та соціального хакінгу. Сучасні атаки відрізняються й ціллю їх здійснення, більшість кібератак орієнтована на контроль ланцюга поставок та/або дані. У атаках, орієнтованих на контроль, зловмисники пошкоджують керуючі дані (наприклад, вказівник функції чи адресу повернення), щоб перенаправити потік інформації, або керування програмою з метою заволодіння доступу до системи. Трендом 2023-2024 року стають комбіновані атаки, які вчиняються за допомогою методів соціальної інженерії, їх питома вага складає 17% усіх порушень відносно даних і 10% випадків встановлення контролю, що робить соціальну інженерію одним із трьох найпоширеніших засобів вчинення кібератак [2]. Наприклад, хакерська атака на "Київстар" стала можливою завдяки обліковому запису одного зі співробітників компанії. Кібератаки та витоки даних стають дедалі частим явищем для українців. 19 грудня 2024 року, сталася наймасштабніша кібератака на державні реєстри України. Для розуміння масштабів можливих витоків даних слід розуміти, що користувачами лише мобільного застосунку «Дія» є 13,5 млн. українців.

Для реалізації такого масштабу операцій кіберзлочинцями залучаються багато фахівців. І це змінює структуру кіберзлочинності. Нова тенденція сучасної кіберзлочинності полягає в тому, що злочинці-одинаки поступово витісняються з кримінального ринку законспірованими, добре організованими і розгалуженими злочинними групами, що об’єднують людей з різних регіонів або країн світу. Учасники подібних кримінальних спільнот мають свою злочинну спеціалізацію, і ефективність їх діяльності досить висока. Фахівці також відмічають, що завдяки тому, що національні нормативно-правові акти у сфері протидії кіберзлочинності значно різняться, все більшого поширення набувають так звані розподілені схеми мережевої кіберзлочинності. Організовані злочинні угруповання будують свою діяльність розбиваючи її на ланцюги операцій таким чином, що в цілому кібердії не є злочинними, оскільки кожна операція сама по

собі здійснюється в окремій країні, де саме ця операція є дозволеною або ж законодавчо не врегульованою.

Враховуючи такі тенденції у формуванні і функціонування організованих злочинних угрупувань 24 грудня 2024 року Генеральна Асамблея ООН приймає Конвенцію Організації Об'єднаних Націй проти кіберзлочинності; зміцнення міжнародного співробітництва у боротьбі з певними злочинами, скоєними з використанням інформаційно-комунікаційних систем, та в обміні доказами в електронній формі, що належать до серйозних злочинів [3]. Конвенцією передбачається посилення контролю не лише за кіберзлочинами, а й будь якими серйозними злочинами, які вчиняються у інформаційно-комунікативних системах (стаття 2). У Конвенції наголошується на єдиних стандартах криміналізації дій, які можуть завдати шкоди інформаційно-комунікативним системам таки як:

1. Незаконний доступ: діяння яке вчиняється навмисно і створює умови для неправомірного доступу до інформаційно-комунікаційної системи загалом чи до її частин.
2. Незаконне перехоплення: діяння здійснюється навмисно і неправомірно за допомогою технічних засобів перехоплення непублічних передач електронних даних в інформаційно-комунікаційній системі, з неї чи в ній, в тому число електромагнітного випромінювання від інформаційно-комунікаційної системи, що переносить такі електронні дані.
3. Вплив на «електронні дані»: діяння здійснюються навмисно і неправомірно, і вчиняються шляхом пошкодження, видалення, псування, зміну або блокування електронних даних.
4. Вплив на «інформаційно-комунікаційну систему»: діяння відбувається навмисно і неправомірно, полягає у перешкоджанні функціонуванню інформаційно-комунікаційної системи шляхом введення, передачі, пошкодження, видалення, псування, зміни чи блокування електронних даних.
5. Неправомірне використання пристроїв: отримання, продаж, придбання пароля, реквізитів доступу, електронного підпису або аналогічних даних, що дозволяють отримати доступ до всієї інформаційно-комунікаційної системи або її частини.
6. Підробка з використанням інформаційно-комунікаційної системи: діяння здійснюються навмисно і полягає у введенні, зміні, видалення або блокування електронних даних, що призводять до виникнення неавтентичних даних, з наміром, щоб вони розглядалися або використовувалися в юридичних цілях як автентичні, незалежно від того, чи піддаються ці дані безпосередньому прочитанню і чи є зрозумілими.

Висновки. Передбачення у чинному КК України визначених кримінальних правопорушень створить юридичну основу для побудови ефективної міжнародної системи протидії кіберзлочинності. Окремо, уніфікованість визначення кіберзлочинів буде сприяти ефективності обміну інформацією, яка й досі характеризується певною невизначеністю. Як свідчать дослідження фахівців, на сьогодні у світі не існує ні релевантної статистики, яка відображає

реальний стан кіберзлочинності, ні надійних методів збору таких даних та й збитки від кіберзлочинів, є досить приблизними. Окрема проблема це низький рівень безпекової культури громадян у цифровому просторі і не розуміння реальних проблем, що пов’язанні з ідентифікуючими та персональними даними.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України. Закону України № 2163-VIII від 5 жовтня 2017 року Відомості Верховної Ради (ВВР), 2017, № 45, ст.403. URL:https://zakon.rada.gov.ua/laws/show/2163-19#Text
2. Top 10 Best-Known Cybersecurity Incidents and What to Learn from Them (2024). URL: https://www.ekransystem.com/en/blog/top-10-cyber-security-breaches
3. Конвенцію Організації Об'єднаних Націй проти кіберзлочинності; зміцнення міжнародного співробітництва у боротьбі з певними злочинами, скоєними з використанням інформаційно-комунікаційних систем, та в обміні доказами в електронній формі, що належать до серйозних злочинів. 24 грудня 2024 року. URL: https://documents.un.org/doc/undoc/gen/n24/372/06/pdf/n2437206.pdf
4. Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws. Науково-дослідна служба Конгресу США. URL: https://www.everycrsreport.com
5. Реєстри відновили. Які наслідки кібератаки для України (2025). URL: https://www.bbc.com/ukrainian/articles/c5ye75y8415o
6. Whatis a cyberattack? Chathamhouse. URL: https://www.chathamhouse.org/2022/02/what-cyber-attack