

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»

Інститут інформаційної безпеки, радіоелектроніки та
телекомунікацій
Кафедра кібербезпеки та програмного забезпечення

КОНСПЕКТ ЛЕКЦІЙ
з дисципліни

«ЦИФРОВА КРИМІНАЛІСТИКА»

для здобувачів першого (бакалаврського) рівня вищої освіти
за спеціальністю 125 Кібербезпека
освітня програма «Кібербезпека»

Одеса: Одеська політехніка, 2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»

Інститут інформаційної безпеки, радіоелектроніки та
телекомунікацій
Кафедра кібербезпеки та програмного забезпечення

КОНСПЕКТ ЛЕКЦІЙ
з дисципліни

«ЦИФРОВА КРИМІНАЛІСТИКА»

для здобувачів першого (бакалаврського) рівня вищої освіти
за спеціальністю 125 Кібербезпека
освітня програма «Кібербезпека»

Затверджено
на засіданні кафедри
кібербезпеки та програмного
забезпечення
Протокол №1 від 26.08.23р
Узгоджено з НМВ
№ 4199 – РС - 2024

Одеса: Одеська політехніка, 2023

Конспект лекцій з дисципліни «Цифрова криміналістика» для здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 125 Кібербезпека / укладач Зоріло Вікторія Вікторівна. Одеса: Одеська політехніка, 2023. – 253с.

Укладач: Зоріло Вікторія Вікторівна, к.т.н.

ЗМІСТ

Анотація	6
Семестровий модуль 1	8
Змістовий модуль 1. Основні види кіберзлочинності. Правова база.	8
Лекція 1. Вступ. Кіберзлочинність. Роль сучасних комп'ютерних технологій в розвитку кіберзлочинності	8
1.1. Глобальні тенденції в сфері використання технологій та Інтернету.....	8
1.2. Тенденції у сфері кіберзлочинності.	15
1.3. Попередження кіберзлочинності.	22
Лекція 2. Основні види кіберзлочинності.....	25
2.1. Злочини проти конфіденційності, цілісності та доступності комп'ютерних даних або систем	25
2.2. Правопорушення, пов'язані з використанням комп'ютерних засобів.	28
2.3. Комп'ютерні злочини, пов'язані з використанням персональних даних, і спам	31
2.4. Комп'ютерні злочини, що порушують авторські права або товарні знаки.....	32
2.5. Дії, що використовують експлуатацію комп'ютера з метою заподіяти шкоди	34
2.6. Залучення дітей або «грумінг».....	36
2.7. Правопорушення, пов'язані зі змістом комп'ютерних даних.	36
Лекція 3. Правова база. Роль законодавства про кіберзлочинність у цифровій криміналістиці.	44
3.1. Законодавство про кіберзлочинність.....	44
3.2. Уніфікація законодавства.	55
3.3. Міжнародні та регіональні правові документи	57
3.4. Міжнародне право в галузі прав людини та законодавство про кіберзлочинність	59
ЗМІСТОВИЙ МОДУЛЬ 2. Цифрові докази. Стандарти та методи цифрової криміналістики....	75
Лекція 4. Основи цифрової криміналістики.	75
4.1. Цифрові докази.....	75
4.2. Криміналістична експертиза «розумних» транспортних засобів	88
4.3. Криміналістична експертиза Інтернету речей	89
4.4. Антикриміналістика.....	91
Лекція 5. Розслідування кіберзлочинів	94
5.2.Органи кримінального правосуддя.....	94
5.3. Приклад рівня ЗНС слідчого у справах про кіберзлочинність	94
5.3.Органи національної безпеки.....	94
5.1. Повідомлення про кіберзлочини.....	94
5.2.Органи кримінального правосуддя.....	96
5.3. Приклад рівня ЗНС слідчого у справах про кіберзлочинність	99
5.4.Органи національної безпеки.....	102
Лекція 6. Практичні аспекти цифрової криміналістики.	125

6.1. Правові та етичні зобов'язання	125
6.2. Правила поведінки з цифровими доказами	126
6.3. Допустимість цифрових доказів	141
Лекція 7. Міжнародне співробітництво у боротьбі з кіберзлочинністю.....	148
7.1. Суверенітет та юрисдикція.....	148
7.2. Офіційні механізми міжнародного співробітництва	151
7.3. Неофіційні механізми міжнародного співробітництва.....	158
7.4. Зберігання та забезпечення збереження даних та доступ до даних	161
7.5. Проблеми, пов'язані з екстериторіальними доказами.....	163
Змістовий модуль 3. Стратегії, політика та програми боротьби з кіберзлочинністю.	169
Лекція 8. Кібербезпека та попередження кіберзлочинності: стратегії, політика та програми ..	169
8.1. Управління Інтернетом.....	169
8.2. Стратегії кібербезпеки: основні особливості.....	172
8.3. Міжнародне співробітництво з питань кібербезпеки	179
8.4. Стан справ у галузі кібербезпеки.....	186
Лекція 9. Кіберзлочинність. Стратегія, політика, програми протидії.....	191
9.1. Активи, уразливості та загрози.....	191
9.2. Ситуаційне попередження злочинності	201
9.3. Виявлення інцидентів, реагування на них, відновлення та забезпечення готовності	204
Лекція 10. Конфіденційність та захист даних. Недоторканність приватного життя	206
10.1. Недоторканність приватного життя	206
10.2. Конфіденційність та безпека.....	208
10.3. Карта світу: закони та правила, що стосуються шифрування даних	210
10.4. Непередбачені ризики для безпеки.....	211
10.5. Кіберзлочини, що порушують конфіденційність	212
10.6. Законодавство про захист даних.....	216
10.7. Право на забуття.....	220
10.8. Законодавство про повідомлення про пошкодження систем безпеки даних	224
10.9. Контроль за дотриманням законодавства про конфіденційність та захист даних.....	226
Лекція 11. Злочини у сфері інтелектуальної власності, здійснювані за допомогою кібертехнологій	230
11.1. Види інтелектуальної власності.....	233
11.2. Причини, підстави та передбачувані мотиви правопорушень, що стосуються авторських прав та товарних знаків, що скоюються за допомогою кібертехнологій.....	243
11.3. Зусилля із захисту та профілактики	246
РЕКОМЕНДОВАНА ЛІТЕРАТУРА	241

АНОТАЦІЯ

Дисципліна «Цифрова криміналістика» відповідає освітньо-професійній програмі, навчальному та робочому планам підготовки фахівців першого (бакалаврського) освітньо-професійного рівня вищої освіти за спеціальністю 125 Кібербезпека і є складовою циклу дисциплін професійної підготовки обов'язкової частини навчального плану.

Предмет дисципліни «Цифрова криміналістика» – вивчення видів кіберзлочинності та методів пошуку цифрових слідів.

Метою дисципліни є опанування теорії, методик та отримання досвіду з пошуку цифрових доказів.

Компетентності:

СК 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

СК 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної безпеки та/або кібербезпеки.

СК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки та/або кібербезпеки.

Результати навчання:

ПРН7. (З, У/Н) Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки.

ПРН9. (З, У/Н, К) Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

ПРН49. (З, У/Н) Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.

ПРН52. (З, У/Н) Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

ПРН50. (З, У/Н) Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

ПРН51. (З, У/Н) Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.

Семестровий модуль 1

Змістовий модуль 1. Основні види кіберзлочинності.

Правова база.

Лекція 1. Вступ. Кіберзлочинність. Роль сучасних комп'ютерних технологій в розвитку кібеззлочинності

План

1.1. Глобальні тенденції в сфері використання технологій та Інтернету.

1.2. Тенденції у сфері кіберзлочинності.

1.3. Попередження кіберзлочинності.

1.1. Глобальні тенденції в сфері використання технологій та Інтернету.

Комп'ютерна система може бути представлена настільними або портативними комп'ютерами. Однак мобільні телефони, планшетні комп'ютери та пристрої Інтернету речей (IoT), що є пристроями, підключеними до Інтернету (наприклад, побутові прилади та розумні годинники), які взаємопов'язані та взаємодіють один з одним і дозволяють відстежувати об'єкти, людей, тварин та/або рослини, а також обмінюватися інформацією про них з метою надання користувачам цих пристроїв певні послуги, а також багато інших пристроїв теж можуть розглядатися як комп'ютерні системи.

Існують різні визначення *комп'ютерної системи*. Наприклад, стаття 1(а) Конвенції Ради Європи про кіберзлочинність 2001 року визначає «комп'ютерну систему» як «будь-який пристрій або групу взаємопов'язаних або суміжних пристроїв, один або більше з яких, діючи відповідно до програми, здійснює автоматизовану обробку даних». У той же час у статті 1 Конвенції Африканського союзу про кібербезпеку та

захист персональних даних 2014 року комп'ютерна система визначається як «електронний, магнітний, оптичний, електрохімічний або інший високошвидкісний пристрій обробки даних або група взаємопов'язаних чи сполучених пристроїв, що виконують логічні, арифметичні функції чи функції зберігання, включаючи засіб зберігання даних або засіб зв'язку, що безпосередньо пов'язаний з таким пристроєм або такими пристроями або працює в поєднанні з таким пристроєм або такими пристроями».

Комп'ютерні системи мають властивість обробляти *дані*. Стаття 2(3) Конвенції Ліги арабських держав про боротьбу зі злочинами в галузі інформаційних технологій 2010 року визначає дані як «все, що може зберігатися, оброблятися, генеруватися та передаватися за допомогою інформаційних технологій, наприклад цифри, літери, символи і т.д.». Для позначення даних використовуються й інші терміни: у статті 1 (b) Конвенції Ради Європи про кіберзлочинність використовується термін «комп'ютерні дані» («будь-яке подання фактів, інформації або понять у формі, що підходить для обробки в комп'ютерній системі, включаючи програму, що підходить для того, щоб комп'ютерна система виконувала функцію»; у статті Конвенції Африканського союзу про кібербезпеку та захист персональних даних 2014 року використовується термін "комп'ютеризовані дані", який має практично таке ж визначення даних, що і термін, який використовується в Конвенції Ради Європи про кіберзлочинність 2001 року (будь-яке подання фактів, інформації або понять у формі, що підходить для обробки в комп'ютерній системі)), а у статті 1(b) Угоди про співпрацю держав-учасниць Співдружності Незалежних Держав у боротьбі зі злочинами у сфері комп'ютерної інформації 2001 року використовується термін «комп'ютерна інформація» («інформація, що знаходиться в пам'яті ти комп'ютера, на машинних чи інших носіях у вигляді, доступної сприйняттю ЕОМ, чи що передається каналами зв'язку»).

Більшість комп'ютерних систем, з якими ми знайомі, зберігають дані. Наприклад, смартфон може створити фотографію за допомогою вбудованої камери (обробка даних) і він також може зберегти цю фотографію для подальшого доступу (зберігання даних). Дані зазвичай зберігаються у внутрішній постійній пам'яті, наприклад, *жорсткий диск*.

Особи, які надають послуги, пов'язані з комп'ютерною системою, називаються *постачальниками послуг*. Стаття 2 (2) Конвенції Ліги арабських держав про боротьбу зі злочинами в галузі інформаційних технологій 2010 року визначає постачальника послуг як «будь-яка фізична чи юридична особа, чи то публічна, чи то приватна, яка надає абонентам послуги, необхідні для здійснення комунікації з використання інформаційних технологій, або яка обробляє або зберігає інформацію від імені служби зв'язку або її користувачів».

Послуги домашніх комп'ютерів та мобільних телефонів надаються постачальниками послуг Інтернету. Постачальник Інтернет-послуг використовує комп'ютерні системи, які можуть надсилати дані на комп'ютери або телефони та отримувати дані, що надсилаються з комп'ютерів або телефонів. Коли два або більше комп'ютерів можуть обмінюватися даними, надсилаючи їх один одному, створюється *комп'ютерна мережа*.

Уявіть собі електронну пошту. Коли ви використовуєте електронну пошту, ви, можливо, відкриваєте браузер і підключаєтеся до веб-сайту. Після входу в систему ви можете надсилати та отримувати електронні листи. Цілком ймовірно, цей сайт належить не вам, а іншій організації. Ця організація надає послуги електронної пошти та може вважатися постачальником послуг. Зверніть увагу, що послуги доступу до Інтернету та послуги доступу до електронної пошти – це дві абсолютно різні *послуги*.

Це призводить до *даних про трафік*, які визначаються у статті 1(d) Конвенції Ради Європи про комп'ютерні злочини 2001 року як «будь-які комп'ютерні дані, що стосуються передачі інформації за допомогою

комп'ютерної системи, що генеруються комп'ютерною системою, що є складовою відповідного комунікаційного ланцюжка, та вказують на джерело, призначення, маршрут, час, дату, розмір, тривалість або тип відповідного мережевого сервісу». Раніше ми говорили про комп'ютерні дані як дані, які зберігаються або обробляються комп'ютерною системою. Дані про трафік – це дані, які передаються через комп'ютерну мережу.

Тепер уявіть собі свою електронну пошту. Ви пишете свій електронний лист, а потім «надсилаєте» це повідомлення одержувачу. *Дані* в електронному листі *надсилаються* через мережу, доки не досягнуть адресата. Дані про трафік – це будь-які дані, необхідні для того, щоб електронний лист досяг свого адресата.

Хорошим прикладом є телефон. Уявіть собі, що ви захотіли зателефонувати до свого приятеля. І вам, і вашому приятелю потрібні телефони, і вам потрібні номери телефонів. Ваш *постачальник послуг* надасть вам номер телефону та доступ до мережі, якщо ви сплатите рахунок за телефон. Потім вам потрібно буде дізнатися номер телефону вашого приятеля, щоб зробити дзвінок. Після того, як ви та ваш приятель отримаєте послугу та дізнаєтесь номери один одного, ви зможете спілкуватися. Те саме, в принципі, можна сказати і про комп'ютерні мережі.

Коли ви бажаєте отримати доступ до веб-сайту, ви вводите *доменне ім'я* (наприклад, yahoo.com) в Інтернет-браузер (або веб-браузер) (наприклад, Google, Bing). Це доменне ім'я може бути пов'язане (тобто порівняно) з однією або декількома адресами Інтернет-протоколу (або *IP-адресами*), «унікальними ідентифікаторами, що присвоюються комп'ютерам або іншим цифровим пристроям, що підключаються до Інтернету, постачальником послуг Інтернету, коли вони підключаються до Інтернету». *Система доменних імен* (DNS) забезпечує доступ до Інтернету шляхом перетворення доменних імен на IP-адресу.

Як тільки ми отримаємо загальне уявлення про комп'ютерну систему, комп'ютерні дані, постачальників послуг, дані про трафік та інші поняття, що стосуються комп'ютерних технологій, ми зможемо зрозуміти, як їх можна використовувати для торгівлі, спілкування та скоєння злочинів.

На землі існує дуже мало місць, де ви не зможете отримати доступ до Інтернету. У більшості країн є щонайменше один постачальник Інтернет-послуг, який надає мережну інфраструктуру (апаратне забезпечення, таке як обладнання, кабелі та бездротовий доступ) для великих міст. Навіть у районах, де немає місцевих постачальників Інтернет-послуг, глобальні супутникові мережі можуть забезпечити доступ до Інтернету для віддалених районів.

Широкопasmогова технологія в країнах, що розвиваються, впроваджується повільними темпами, внаслідок чого населення цих країн для доступу в Інтернет використовує мобільні технології (Statista, 2018). Завдяки доступності Інтернет-послуг через мобільні пристрої, використання Інтернету неухильно зростає. Смартфони стають все менш дорогими і включають все більше функцій, а постачальники послуг мобільного зв'язку забезпечують більш надійний доступ в Інтернет через менш дорогі мережі стільникового зв'язку. Це сприяє підвищенню рівня проникнення Інтернету у багатьох країнах. 2016 став першим роком, коли більшість користувачів Інтернету в усьому світі для виходу в Інтернет стали використовувати мобільні пристрої (Statcounter, 2016).

Рівень проникнення Інтернету означає «відсоток загальної чисельності населення цієї країни чи регіону, який використовує Інтернет». Станом на вересень 2017 року рівень проникнення Інтернету у світі оцінюється у 51%. Таким чином, приблизно половина населення світу має доступ до Інтернету та можливість користуватися Інтернетом (див. рис. 1 із зазначенням рівня проникнення Інтернету з розбивкою по регіонах).

Джерело: Statista (2018). Рівень проникнення Інтернету у світі станом на вересень 2017 року з розбивкою у регіонах: Global internet penetration rate as of September 2017, за регіонами (рис.1).

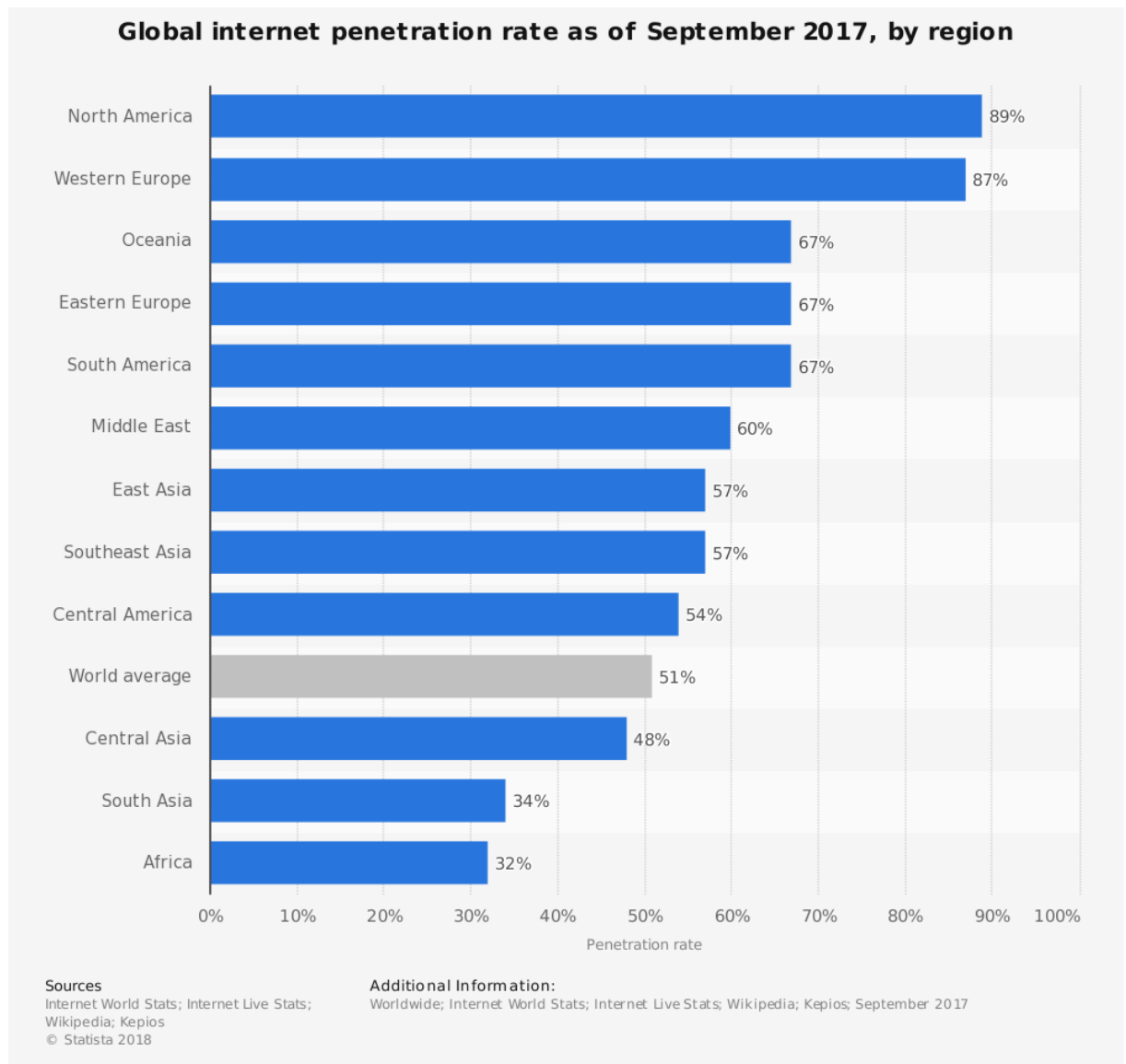


Рис. 1. Проникнення інтернету у різних регіонах, 2017 рік

У міру підвищення надійності доступу до Інтернету та збільшення кількості людей, що підключаються до Інтернету, зростає кількість важливих послуг, що надаються онлайн. Наприклад, підключення до Інтернету є дуже швидким та дуже надійним у Південній Кореї.

За оцінками Організації економічного співробітництва та розвитку (ОЕСР), у 2018 році рівень проникнення Інтернету у домогосподарствах у Південній Кореї становив 99,5%. За такої кількості людей, підключених до

Інтернету, корейський уряд і комерційні структури пропонують все більше онлайн-ових послуг.

Наприклад, якщо ви отримуєте квитанцію на оплату штрафу за перевищення швидкості (автоматично з підключеної до Інтернету камери фіксації порушень швидкісного режиму), ви можете відвідати урядовий веб-сайт, щоб переглянути інформацію про свою штрафну квитанцію. Потім ви можете негайно сплатити штраф через систему банківських електронних платежів. Цей процес розрахунку може бути повністю безпаперовим. У деяких випадках кількість державних послуг, що надаються *офлайн*, менше кількості онлайн-ових послуг.

Нині у Китаї склалася така ситуація, лише у ще більших масштабах. Відповідно до 41-го Статистичного звіту про розвиток Інтернету в Китаї, опублікованому в січні 2018 року, станом на «кінець грудня 2017 року кількість користувачів Інтернету в Китаї досягла 772 мільйонів людей, збільшившись на 40,74 мільйонів порівняно з кінцем 2016 року. Рівень проникнення Інтернету досяг 55,8%, що на 2,6 відсоткових пункти більше, ніж наприкінці 2016 року. До таких Інтернет-послуг, як миттєвий обмін повідомленнями, онлайн-платежі, онлайн-покупки, онлайн-доставка їжі або онлайн-бронювання поїздок, звертаються сотні мільйонів користувачів.

Такі програми, як WeChat (інструмент для миттєвого обміну повідомленнями) та Alipay (система платежів на користь третіх осіб), стали важливими програмами практично для кожного смартфона. Мобільні пристрої, мобільний Інтернет та ці додатки настільки популярні, що державні послуги, платежі, інвестиції, громадський та приватний транспорт та багато інших послуг повністю інтегровані з ними. В умовах, коли критично важливі послуги все частіше пропонуються в режимі онлайн, причому іноді це супроводжується скороченням кількості офлайн-ових послуг, також з'являється все більше можливостей для зловживання технологіями та скоєння злочинів.

1.2. Тенденції у сфері кіберзлочинності.

Немає загальноприйнятого визначення кіберзлочинності. Тим не менш, наступне визначення включає елементи, загальні для всіх існуючих визначень кіберзлочинності.

Кіберзлочин – це дія, що порушує закон, що вчиняється з використанням інформаційно-комунікаційних технологій (ІКТ) і або націлена на мережі, системи, дані, веб-сайти та/або технології, або сприяє скоєнню злочину.

Кіберзлочин відрізняється від традиційного злочину тим, що він «не визнає фізичні чи географічні кордони» і може відбуватися з меншими зусиллями, більшою легкістю і з більшою швидкістю, ніж традиційний злочин (хоча це залежить від виду кіберзлочину та виду традиційного злочину, з яким він порівнюється).

Європол (2018) поділяє кіберзлочини на

кіберзалежні злочини (тобто «будь-який злочин, який може бути скоєний лише з використанням комп'ютерів, комп'ютерних мереж або інших форм інформаційно-комунікаційних технологій»;

та злочини, що скоюються *за допомогою кібертехнологій* (тобто традиційні злочини, що скоюються за допомогою Інтернету та цифрових технологій).

Ключова відмінність між цими категоріями кіберзлочинності полягає в ролі інформаційно-комунікаційних технологій у скоєнні правопорушення – чи є ІКТ метою злочину чи невід'ємною частиною способу скоєння злочину (*modus operandi* або М.О.; тобто, методу дії), використаного злочинцем. Коли ІКТ є метою злочину, такий кіберзлочин негативно впливає на *конфіденційність, цілісність та/або доступність* комп'ютерних даних або систем. Конфіденційність, цілісність і доступність становлять так звану «Тріаду КІЦД»: простіше кажучи, конфіденційна інформація повинна залишатися конфіденційною, її не слід змінювати без дозволу власника, а дані, послуги та системи повинні бути доступними для

власника у будь-який час. Коли ІКТ є частиною способу скоєння злочину, кіберзлочинність включає традиційний злочин (наприклад, шахрайство і крадіжку), вчиненню якого тим чи іншим чином сприяють Інтернет і цифрові технології. Ці категорії кіберзлочинності та види кіберзлочинів, які підпадають під ці категорії, більш детально розглядаються в лекції 2.

Кіберзлочини можуть виконуватись фізичними особами, групами осіб, комерційними організаціями та державами. Хоча ці суб'єкти можуть застосовувати схожі тактичні методи (наприклад, використовувати шкідливе програмне забезпечення) та атакувати схожі цілі (наприклад, комп'ютерну систему), вони мають різні мотиви та наміри при скоєнні кіберзлочинів.

Було проведено різні дослідження кіберзлочинності (див., наприклад, дослідження, опубліковані в журналах «Deviant Behavior» та «International Journal of Cyber Criminology»). У цих дослідженнях кіберзлочинність вивчалася через призму психології, соціології та кримінології, а також інших наукових дисциплін.

В одних публікаціях дії злочинців тлумачаться як результат раціонального та вільного вибору, тоді як в інших публікаціях злочинність розглядається як результат дії внутрішніх та/або зовнішніх сил. В інших роботах вивчалася роль «простору» у кіберзлочинності, зокрема, роль онлайн-просторів та онлайн-спільнот у культурній трансмісії злочинних та/або кримінальних цінностей. Мета цих наукових досліджень про кіберзлочинність полягає в тому, щоб пролити світло на наслідки кіберзлочинності, «характер і масштаби кіберзлочинності, оцінити реакції на кіберзлочинність і наслідки цих реакцій, а також оцінити ефективність існуючих методів, що використовуються для боротьби з кіберзлочинністю, пом'якшення її наслідків».

Регіональні та міжнародні правоохоронні органи (наприклад, Європол та Інтерпол) та регіональні організації (наприклад, Африканський союз та Організація американських держав) публікують інформацію про

тенденції у сфері кіберзлочинності та кібербезпеки. Тенденції в галузі кіберзлочинності можна також визначити за щорічними звітами та/або даними з різних офіційних інструментів вимірювання злочинності та досліджень проблеми віктимізації: наприклад, Національна система обліку інцидентів (США); загальне соціальне дослідження (Канада); Огляд злочинності в Англії та Уельсі (Англія та Уельс). Ці інструменти вимірювання параметрів злочинності та дослідження проблеми віктимізації відрізняються з точки зору типів даних, що збираються і аналізуються про кіберзлочинність, а також методів, що використовуються для збору та аналізу даних.

Африканський союз, Сполучені Штати та Symantec є учасниками Ініціативи «Глобальний форум з кіберекспертизи» (GFCE), який опублікував свій перший звіт про тенденції в галузі кіберзлочинності та кібербезпеки у 2017 році. Звіти про тенденції в галузі кіберзлочинності та кібербезпеки публікують інші організації; наприклад, див Europol.

Компанії у сфері кібербезпеки та інші приватні організації, що займаються аналізом безпеки, бізнес-ризиків та/або загроз по всьому світу, публікують звіти про тенденції в галузі кіберзлочинності та/або кібербезпеки, засновані на інцидентах кібербезпеки, їх типах, частоті та наслідках. Наприклад, у 2018 році компанія Trend Micro визначила використання *вірусу-здирника* як тенденцію в галузі кіберзлочинності. При вчиненні такого виду кіберзлочину комп'ютерні системи заражаються шкідливим кодом (*шкідливою програмою*), і дані в них стають недоступними для власників та/або законних користувачів доти, доки кіберзлочинцю не будуть заплачені гроші. Хоча атаки з використанням вірусу-здирника не нові, збільшилася їх кількість, а також частота, інтенсивність та охоплення. Спочатку зловмисники, які чинили кіберзлочини такого роду, націлювалися на фізичних осіб і вимагали від них невеликі суми грошей, але потім вони почали націлюватися на комерційні підприємства, компанії та організації та, нарешті, на інших

суб'єктів у приватному та державному секторах, які надають критично важливі послуги (наприклад, лікарні).

Як приклад можна навести атаку з використанням вірусу-зидника (вимагача) WannaCry в 2017 році, яку було зафіксовано у 150 країнах, у тому числі понад 80 «організацій NHS (Національної служби охорони здоров'я) в одній тільки Англії, що спричинило скасування майже 20.000 записів на прийом, 600 клінічних лікарень загальної практики були змушені повернутися до паперового документообігу, а п'ять лікарень переадресовували карети швидкої допомоги в інші лікарні, оскільки більше не могли надавати термінову медичну допомогу». У 2017 році в доповіді Європолу «Оцінка загрози організованих злочинності в Інтернеті» вірус-вимагач був також визначений як тенденція в галузі кіберзлочинності.

****Достовірність даних, що використовуються для визначення тенденцій, також варіює залежно від конкретного агентства та організації. При складанні звітів про тенденції може виникати конфлікт інтересів, якщо компанії продають засоби забезпечення кібербезпеки, які можуть використовуватись людьми для захисту від кіберзлочинців, визначених як тенденції.****

З появою нових технологій (наприклад, Інтернету речей, дронів, роботів, безпілотних автомобілів) виявлятимуться нові тенденції в галузі кіберзлочинності. Більше того, як зазначено в доповіді Європолу «Оцінка загрози організованих злочинності в Інтернеті» за 2017 рік, заходи щодо охорони правопорядку та забезпечення безпеки впливають на кіберзлочинність та тактику, інструменти та цілі кіберзлочинців. Отже, ці заходи також впливатимуть на майбутні тенденції у сфері кіберзлочинності.

Технічні проблеми. Існує кілька технічних причин, які ускладнюють боротьбу з кіберзлочинністю.

Перша причина – *атрибуція* (лекція 5). Будь-який комп'ютер, підключений до Інтернету, може взаємодіяти з будь-яким іншим комп'ютером, підключеним до Інтернету. Зазвичай ми бачимо загальнодоступну *IP-адресу* комп'ютера (Cisco, 2016), коли комп'ютер з'єднується з нашим комп'ютером. IP-адреса – це, як правило, глобальний унікальний номер, який дозволяє нам визначити, з якої країни підключається цей комп'ютер, і до якого постачальника Інтернет-послуг він підключений. Проблема полягає в тому, що зловмисник має багато способів приховати свою IP-адресу або навіть вдати, що вона підключається з іншої IP-адреси. Більше того, злочинці можуть використовувати різні інструменти, щоб уникнути виявлення правоохоронними органами, утруднити доступ та приховати сайти в Даркнеті.

Друга технічна проблема пов'язана із програмним забезпеченням. Комп'ютерні програми є програмним забезпеченням. Програми на вашому телефоні або планшеті є програмним забезпеченням. Сервіси, до яких ви підключаєтеся в Інтернеті, наприклад веб-сайт, також є програмним забезпеченням. Дуже часто програмне забезпечення має *вразливість*. Вразливість може бути пов'язана з проблемою у програмі або неправильною конфігурацією, яка дозволяє зловмисникам робити те, що вони не повинні мати можливість робити (наприклад, завантажувати дані кредитної картки клієнта).

Компаніям-розробникам програмного забезпечення буває непросто виявити вразливості, особливо ті, які пов'язані з великими програмними проєктами, що часто змінюються. Іноді зловмисники знаходять вразливість раніше компанії, яка виробляє програмне забезпечення (тобто вразливість «нульового дня»).

На думку Білдж і Думітрас (Bilge and Dumitras, 2012), «поки вразливість залишається невідомою, вразливе програмне забезпечення не може бути виправлене, а антивірусні програми не можуть виявити атаку за

допомогою сканування на основі сигнатур». Компанії стає відомо про вразливість такого роду, коли вона використовується кіберзлочинцями для атаки на конфіденційність, цілісність або доступність програмного забезпечення та користувачів програмного забезпечення.

У 2017 році Equifax – американське бюро кредитних історій – втратило «конфіденційні персональні дані» 143 мільйонів американців через вразливість програмного забезпечення. Ця вразливість експлуатувалася протягом трьох місяців, доки не була усунена. Вразливості, що призводять до втрати даних, є відносно поширеними навіть для великих організацій, оскільки завдання створення, налаштування та захисту цифрових систем є належним чином скрутним.

Ще однією технічною проблемою є віртуалізована ІТ-інфраструктура (наприклад, хмара). Коли інфраструктура організації переміщується в хмару, це означає, що:

компанія перекладає частину відповідальності за кібербезпеку на постачальника послуг хмари (наприклад, безпека фізичної системи, безпека центру обробки даних);

коли відбуваються порушення безпеки, компанії доводиться працювати з постачальником хмарних послуг, щоб розслідувати інциденти, які можуть призвести до проблем технічного та правового характеру (правові проблеми, пов'язані з хмарними даними, детальніше розглядаються в лекції 7).

Правові проблеми. Кіберзлочинність є одним із видів транснаціональної злочинності, виконавці та жертви якої можуть перебувати в будь-якій точці світу, де є підключення до Інтернету. У зв'язку з цим слідчим, які ведуть розслідування кіберзлочинів, часто потрібний транскордонний доступ до даних та обмін ними. Це завдання може бути виконане у випадку, якщо дані, що запитуються, зберігаються постачальниками послуг і вживаються заходи, що дозволяють правоохоронним органам отримувати доступ до даних. Основними

правовими проблемами при розслідуванні кіберзлочинів та судовому переслідуванні кіберзлочинців є наступні.

Різні правові системи, що існують у різних країнах; відмінності в національних законодавствах про кіберзлочинність; відмінності в нормах доказового права та кримінального судочинства (наприклад, у процедурах отримання доступу до цифрових доказів правоохоронними органами; наприклад, на підставі законного розпорядження, такого як ордер на обшук або без нього); відмінності в охопленні та географічній застосовності регіональних та багатосторонніх договорів про боротьбу з кіберзлочинністю; та відмінності у підходах до захисту даних та дотримання прав людини.

Етичні проблеми. Правоохоронні органи повинні дотримуватись правових та етичних норм при розслідуванні злочинів (і кіберзлочинів), обробці, аналізі та тлумаченні доказів. Етичні проблеми можуть виникати не тільки під час здійснення правоохоронної діяльності, а й під час використання інформаційно-комунікаційних технологій (ІКТ) окремими особами, групами осіб, компаніями, організаціями та урядом.

Наприклад, етична поведінка при використанні ІКТ передбачає утримання від заподіяння шкоди іншим людям, системам та даним, а також дотримання принципу верховенства закону та прав людини. Викриття компанії Cambridge Analytica переконали всіх у необхідності приділяти увагу етичним питанням, пов'язаним із збиранням та використанням даних на платформах соціальних мереж. Зокрема, засоби масової інформації виявили, що компанія з обробки даних Cambridge Analytica заплатила за отримання особистих даних користувачів Facebook через стороннього дослідника Олександра Когана, який створив додаток для збору даних у формі опитувальника для перевірки особи, яка повідомляла користувачам (дрібним шрифтом), що інформація збирається виключно з науковою метою, причому це твердження не було перевірено компанією Facebook і виявилось хибним. Незважаючи на те, що лише

305.000 осіб взяли участь в опитуванні та дали згоду на збір своїх особистих даних, дані їхніх друзів також були отримані з їхніх облікових записів, внаслідок чого кількість постраждалих досягла 87 мільйонів осіб (АМА, 2018).

Інцидент із Cambridge Analytica пролив світло на неетичну поведінку тих, хто несе відповідальність за величезну кількість даних, зібраних про окремих осіб та використаних непередбачуваним чином для користувачів, які погодилися надати (деяку) інформацію, та неправомірно для тих, хто взагалі не давав жодної згоди на збір та використання будь-яких своїх даних. Навіть якщо те, що зробили Cambridge Analytica та інші причетні особи, які не вважають незаконними, їх дії були неетичними.

Оперативні проблеми. Одна з ключових оперативних проблем під час розслідування кіберзлочинів пов'язана із співпрацею з іншими країнами. Міжнародне співробітництво у розслідуванні кіберзлочинів потребує уніфікації законодавства у країнах, що співпрацюють. Такі інструменти, як *договори про взаємну правову допомогу* (тобто угоди, в рамках яких сторони погоджуються співпрацювати у розслідуванні та судовому переслідуванні правопорушень, кримінально караних відповідно до їх національних законодавств), можуть використовуватися для направлення офіційних запитів щодо надання допомоги з однієї країни до іншої. Однак запити про надання правової допомоги можуть займати багато часу і можуть не призвести до досягнення прийнятних результатів, таких як запобігання злочину або надання доказів для використання в суді. Оперативні проблеми також виникають через брак національного потенціалу (особливо в країнах, що розвиваються), необхідного для боротьби з кіберзлочинністю.

1.3. Попередження кіберзлочинності.

Кіберзлочинці найчастіше використовують як технічні, так і соціальні підходи до скоєння злочинів. Деяким видам кіберзлочинності

важко запобігти, проте користувачі технологій можуть робити певні дії, щоб захистити себе (якоюсь мірою) від кіберзлочинності.

Європол (2018) розміщує численні посібники з інформування громадськості та профілактики злочинності на своєму веб-сайті. Проте, навіть малі дії здатні привнести великі зміни. Нижче наведено деякі поради, які слід враховувати при підключенні до Інтернету.

Регулярно оновлюйте операційну систему та встановлене програмне забезпечення.

Регулярно видаляйте програмне забезпечення, яке ви більше не використовуєте.

Використовуйте антивірусну програму, розроблену компанією з гарною репутацією.

Не завантажуйте програмне забезпечення, фільми або музику з сайтів загального доступу – вони часто мають шкідливу програму.

Не завантажуйте вкладення та не натискайте на посилання від невідомих відправників.

Не вводьте особисту інформацію на невідомих веб-сайтах.

Підтвердьте правильність адреси веб-сайту під час введення фінансової інформації.

Висновок. В даній лекції була представлена вступна інформація про кіберзлочинність, пов'язані з нею концепції та проблеми, що виникають при розслідуванні кіберзлочинів і попередження кіберзлочинності. Крім того, були представлені деякі поняття, теми та проблеми, які детальніше розглядаються в інших лекціях. Розглянуті тенденції дають лише стислий огляд загроз кіберзлочинності, з якими стикаються країни сьогодні.

Питання для самоперевірки

1. Перелічити та пояснити сучасні тенденції у кіберзлочинності.
2. Пояснити відмінності між цифровими доказами та звичайними доказами. Навести приклади цифрових доказів.

3. Навести та пояснити основні правові проблеми в розслідуванні кіберзлочинів.

4. Пояснити, які існують моделі здійснення процесу цифрової криміналістики. Назвати та навести основні етапи будь-яких двох моделей.

5. Навести та пояснити технічні проблеми у розслідуванні кіберзлочинів.

6. Пояснити причини, через які жертви кіберзлочинності не звертаються по допомогу до поліції.

ЛЕКЦІЯ 2. ОСНОВНІ ВИДИ КІБЕРЗЛОЧИННОСТІ

План

- 2.1. Злочини проти конфіденційності, цілісності та доступності цифрових даних та комп'ютерних систем.
- 2.2. Правопорушення, пов'язані з використанням комп'ютерних засобів.
- 2.3. Комп'ютерні злочини, пов'язані з використанням персональних даних, і спам
- 2.4. Комп'ютерні злочини, що порушують авторські права або товарні знаки
- 2.5. Дії, що використовують експлуатацію комп'ютера з метою заподіяти шкоди
- 2.6. Залучення дітей або «грумінг»
- 2.7. Правопорушення, пов'язані зі змістом комп'ютерних даних.

2.1. Злочини проти конфіденційності, цілісності та доступності комп'ютерних даних або систем

Кіберзлочини включають в себе хакерські атаки; створення, зберігання та поширення шкідливих програм; атаки типу «відмова в обслуговуванні» (DoS); розподілені атаки типу «відмова в обслуговуванні» (DDoS); і порча веб-сайтів (тобто є форма онлайн-вандалізму, націлена на вміст веб-сайтів).

Приклад. Дії кіберзлочинців, спрямовані проти пацієнтів клініки пластичної хірургії. Кіберзлочинці отримали несанкціонований доступ до комп'ютерної системи литовської клініки пластичної хірургії та отримали конфіденційну інформацію про пацієнтів із різних країн світу, процедури, які вони проходили, фотографії пацієнтів у попередньому вигляді, медичні дані та інші види інформації (2017). Потім Кіберзлочинці вимагали від кожного пацієнта викуп, погрожуючи опублікувати

отримані дані. Розмір викупу змінювався в залежності від кількості та якості вкраденої інформації про пацієнта.

Крім отримання несанкціонованого доступу до систем, хакери можуть перехоплювати дані по їх мірі передачі через мережі.

Атака посередника (атака «людина всередині»). Злочинці перехоплюють повідомлення між клієнтами і серверами, створюючи два з'єднання (злочинець-клієнт і злочинець-сервер). Ціль цієї атаки – таємне перехоплення, отримання та/або відправка інформації між клієнтом і сервером.

DoS-атака створює перешкоди системам, перевантажуючи сервери та/або проміжні пристрої (наприклад, маршрутизатори) запитами, щоб перешкоджати доступу законного трафіку до сайту та/або використанню системи.

Розподілена атака типу «відмова в обслуговуванні» (або DDoS-атака) означає використання кількох комп'ютерів та інших цифрових технологій для проведення скоординованих атак з метою перевантаження серверів та/або посередницьких пристроїв для запобігання доступу законним користувачам. Принцип дії одного з типів DDoS-атак можна пояснити на наступному прикладі: уявіть собі, що багато комп'ютерів намагаються підключитися до одного комп'ютера (серверу) одночасно. Цей комп'ютер має обмежену обчислювальну потужність та пропускну спроможність мережі. Якщо надто багато комп'ютерів намагатимуться підключитися до нього одночасно, сервер буде не в змозі реагувати на кожне з'єднання досить швидко. В результаті сервер не зможе відповісти на запити реальним користувачам, оскільки він надто зайнятий помилковими запитами.

DDoS-атаки можуть проводитись окремою особою, групою осіб чи державою. Держави можуть націлюватися на важливі критичні об'єкти інфраструктури, які вважаються життєво необхідними для функціонування суспільства. Наприклад, Країна А пережила серію DDoS-атак, скоєних

Країною Б проти її фінансового сектора. Внаслідок цих кібератак громадяни країни А були позбавлені доступу до Інтернет-банкінгу, а банкомати в цій країні працювали з перебоями.

DDoS-атаки можуть здійснюватися з використанням цифрових пристроїв, заражених шкідливим програмним забезпеченням (або шкідливою програмою), для створення можливості дистанційного керування цими пристроями та використання їх для здійснення кібератак. Бот-мережа (тобто мережа заражених цифрових пристроїв, іменованих зомбі) може використовуватися для скоєння інших кіберзлочинів, таких як криптоджекінг.

Криптоджекінг – це спосіб, за допомогою якого обчислювальна потужність заражених комп'ютерів використовується для видобутку криптовалюти (тобто зашифрованої цифрової валюти) для отримання фінансової вигоди особою (особами), що контролює заражені цифрові пристрої (тобто «господарем» бот-мережі) та/або особами, які найняли «господарів» бот-мереж.

Кіберзлочинці можуть також виробляти, мати та/або розповсюджувати засоби неправомірного використання комп'ютерів, включаючи технічні пристрої, шкідливе програмне забезпечення (або шкідливу програму), а також паролі, коди доступу та інші дані, які дозволяють особам отримувати незаконний доступ, перехоплювати повідомлення чи іншим чином заподіювати шкоду.

Шкідлива програма (або шкідливе програмне забезпечення) використовується для зараження цільових систем з метою їх моніторингу, збору даних, отримання контролю над системою, зміни роботи системи та/або даних, а також пошкодження системи та/або даних.

Існує кілька видів шкідливих програм, які можуть використовуватись для зараження систем:

«Черв'як». Автономна шкідлива програма, яка розповсюджується без участі користувача.

Вірус. Шкідлива програма, для поширення якої потрібна участь користувача (наприклад, файл, що виконується з вірусом, поширюється при його відкритті користувачем).

Троянський кінь. Шкідлива програма, що маскується під легітимне програмне забезпечення, щоб обманом змусити користувача завантажити програму, яка заражає систему користувачів з метою шпигунства, крадіжки та/або заподіяння шкоди.

Шпигунська програма. Шкідливе програмне забезпечення, призначене для таємного моніторингу заражених систем, а також збору та передачі інформації творцю та/або користувачеві шпигунської програми.

Вірус-вимагач. Шкідлива програма, призначена для взяття систем, файлів та/або даних користувачів у заручники та повернення контролю користувачам лише після виплати викупу.

Криптовимгач (різновид вірусу-вимагача) є шкідливою програмою, яка заражає цифровий пристрій користувача, шифрує документи користувача і загрожує видалити файли і дані, якщо жертва не заплатить викуп.

Програма doxware (шифрувальник-вимагач) – це різновид криптовимагача, який зловмисники використовують проти жертв, загрожуючи розголошенням даних користувача (тобто їх публікацією), якщо не буде виплачено викуп за надання коду для розшифрування файлів та даних.

2.2. Правопорушення, пов'язані з використанням комп'ютерних засобів.

Правопорушення, пов'язані з використанням комп'ютерних засобів, включають злочини, скоєні за допомогою кібертехнологій, «з метою отримання особистого або фінансового прибутку або заподіяння особистої або фінансової шкоди». До цієї категорії віднесено кіберзлочини, «у разі яких використання комп'ютерної системи (або цифрового пристрою) є частиною способу скоєння злочину». У Проєкті доповіді Управління ООН

з наркотиків та злочинності «Всебічне дослідження проблеми кіберзлочинності» (2013) до цієї широкої категорії віднесено такі кіберзлочини.

Комп'ютерне шахрайство або підробку (комп'ютерне підроблення визначається як «навмисне та протиправне введення, зміна, видалення або блокування комп'ютерних даних, що тягнуть за собою порушення автентичності 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»).).

Комп'ютерні злочини, пов'язані з використанням персональних даних.

Розповсюдження або контроль розповсюдження спаму.

Комп'ютерні злочини щодо авторських прав або товарних знаків.

Діяння, які передбачають використання комп'ютера з метою заподіяння особистої шкоди.

Діяння, що передбачають використання комп'ютера з метою залучення дітей та грумінгу (термін «грумінг» означає поведінку злочинців, коли вони завойовують довіру неповнолітніх з метою зустрітися або примусити до онлайн-обміну сексуальним контентом).

Приклад. Американська компанія з виробництва іграшок Mattel стала жертвою вейлінг-шахрайства. Кіберзлочинці, які стояли за цією атакою, таємно контролювали комп'ютерні мережі та комунікації компанії протягом кількох місяців до інциденту. Після того, як у компанії було оголошено про призначення нового генерального директора, кіберзлочинці використовували особу нового генерального директора Крістофера Сінклера для здійснення атаки. Зокрема, кіберзлочинці відправили електронного листа від імені Крістофера Сінклера, в якому просили одержувача схвалити переказ на суму три мільйони доларів до банку Веньчжоу в Китаї на рахунок китайського постачальника. Оскільки прохання надійшло від генерального директора, співробітниця компанії

перевела гроші, але пізніше зв'язалася з ним із цього приводу. Генеральний директор сказав, що не давав жодних вказівок щодо переказу грошей. Після цього компанія Mattel зв'язалася з правоохоронними органами США, Федеральним бюро розслідувань США, своїм банком та правоохоронними органами Китаю. Час інциденту (гроші було переведено напередодні свята) дозволив китайській владі вчасно заморозити рахунки до відкриття банків і компанія Mattel змогла повернути свої гроші.

Стаття 8 Конвенції Ради Європи про кіберзлочинність визначає комп'ютерне шахрайство як «навмисне та протиправне позбавлення іншої особи її власності шляхом будь-якого введення, зміни, видалення чи блокування комп'ютерних даних; та/або будь-якого втручання у функціонування комп'ютерної системи з шахрайським чи безчесним наміром неправомірного отримання економічної вигоди для себе чи іншої особи». Цей кіберзлочин також заборонено статтею 11 Конвенції Ліги арабських держав про боротьбу зі злочинами в галузі інформаційних технологій.

Види комп'ютерного шахрайства включають різні афери в Інтернеті, які припускають дачу помилкових даних або вводять в оману обіцянок любові і дружби (кетфішинг), майна (за допомогою афери зі спадщиною), а також грошей і багатства (шляхом шахрайства з лотереями, афер зі спадщиною тощо). Кінцева мета таких шахраїв полягає в тому, щоб змусити жертву розкрити або іншим чином надати особисту інформацію та/або засоби зловмиснику (це один із різновидів шахрайства методом соціальної інженерії). Цей прийом, як випливає з назви, заснований на використанні соціальної інженерії (цей термін був популяризований американським хакером Кевіном Мітником (Kevin Mitnick)), практиці «примусу людей – шляхом маніпулювання, введення в оману, впливу чи обману – до розкриття конфіденційної інформації або вчиненню дій, які принесуть певну користь соціальному інженеру».

Найбільш відомим видом комп'ютерного шахрайства є листи з проханням зробити авансовий платіж для завершення операції з переказу грошей, депонування або іншої транзакції в обмін на більшу суму грошей (Шахрайство з авансовим платежем, також відоме під назвою «афера 419». Це вид шахрайства, коли жертву переконують заплатити, щоб усунути перешкоди на шляху отримання більшої суми в майбутньому. Запити на відносно невелике «вкладення» в обмін на великий грошовий переказ після «розблокування рахунку» можна було отримати у звичайному листі факсом, по телефону і, з появою інтернету, електронною поштою. Назва Афера 419 походить від статті Кримінального кодексу (КК) Нігерії, на яку посилалися в перших «листах». Хоча історія, яку розповідають зловмисники, постійно змінюється (вони видають себе за урядовців, банківських службовців, юристів тощо), вони використовують ту саму тактику – просять перевести невелику суму грошей в обмін на більшу суму.

2.3. Комп'ютерні злочини, пов'язані з використанням персональних даних, і спам

На додаток до онлайн-схем, в мережі Інтернет також здійснюються деякі види фінансового (або економічного) шахрайства, такі як банківське шахрайство, шахрайство з електронною поштою та шахрайство з кредитними та дебетовими картками. Наприклад, дані дебетових та кредитних карток, отримані злочинцями незаконним шляхом, продаються ними, передаються одна одній та використовуються в Інтернеті. В результаті проведеної в 2018 році міжнародної операції по боротьбі з кіберзлочинністю було закрито один із найвідоміших онлайн кардинг-форумів Infraud, на якому злочинці продавали дані кредитних та дебетових карток та банківську інформацію та обмінювалися ними.

Персональна, медична та фінансова інформація, що купується, продається та обмінюється в Інтернеті, може використовуватися для

скоєння інших злочинів, таких як злочини, пов'язані з використанням персональних даних, коли злочинець неправомірно видає себе за іншу людину та/або незаконно присвоює собі ідентифікаційні дані жертви та/або використовує ці ідентифікаційні та/або особисті дані з незаконною метою.

Дані, які є метою злочинців, включають особисті дані, такі як ідентифікаційні номери (наприклад, номери соціального страхування в США), документи, що засвідчують особу (наприклад, паспорти, національні ідентифікаційні номери, посвідчення водія та свідоцтва про народження), а також облікові дані в Інтернеті (тобто імена користувачів та паролі). Злочин, пов'язаний із використанням персональних даних, може бути фінансово-мотивованим або не бути таким. Наприклад, підроблені посвідчення особи (наприклад, паспорти) можуть бути придбані в Інтернеті для використання під час здійснення поїздок. Такі види злочинів, а також економічне шахрайство здійснюються через Інтернет за допомогою розсилки непотрібних електронних листів (спаму), інформаційних бюлетенів та повідомлень з посиланнями на веб-сайти, які створені для того, щоб вводити користувачів в оману та обманом змусити їх відкривати електронні листи та ін. бюлетені або натискати на посилання в електронних листах, які можуть містити шкідливі програми або надсилати користувачів на фальшиві веб-сайти.

2.4. Комп'ютерні злочини, що порушують авторські права або товарні знаки

Стаття 10 Конвенції Ради Європи про кіберзлочинність передбачає кримінальну відповідальність за правопорушення, пов'язані з порушенням авторського права та суміжних прав. Так само стаття 17 Конвенція Ліги арабських держав про боротьбу зі злочинами в галузі інформаційних технологій забороняє «правопорушення, пов'язані з авторським правом та суміжними правами». До галузі авторського права «належать художні твори, наприклад книги, музика, картини та скульптури, фільми та твори,

створені на основі технологій, включаючи комп'ютерні програми та електронні бази даних».

Існує кілька міжнародних договорів, що стосуються захисту авторських прав, включаючи Бернську конвенцію з охорони літературних та художніх творів 1886 року, Угоду з торгових аспектів прав інтелектуальної власності Всесвітньої організації інтелектуальної власності (ВОІВ) 1994 року та Договір ВОІВ з авторського права. Крім того, існують регіональні закони щодо захисту інтелектуальної власності. Одним із яскравих прикладів порушення авторських прав є цифрове піратство (наприклад, несанкціоноване копіювання, розмноження чи розповсюдження фільму, захищеного авторським правом).

Роботи, захищені авторським правом, вважаються однією з форм інтелектуальної власності, що визначається ВОІВ як «результати творення людського розуму, такі як винаходи, літературні та художні твори, символіка, назви та зображення, що використовуються в комерційних цілях». Стаття 2 Конвенції, що засновує Всесвітню організацію інтелектуальної власності (ВОІВ) 1967 року, свідчить: інтелектуальна власність включає права, що належать до: літературних, художніх і наукових творів, виконавчої діяльності артистів, звукозапису, радіо та телевізійних передач, винаходів у всіх науках відкриттям, промисловим зразкам, товарним знакам, знакам обслуговування, фірмовим найменуванням та комерційним позначенням, захисту проти недобросовісної конкуренції, а також всі інші права, що стосуються інтелектуальної діяльності у виробничій, науковій, літературній та художній галузях.

Таким чином, інтелектуальна власність включає не тільки авторські права (наприклад, книги, музику, фільми, програмне забезпечення і т.д.), але і товарні знаки (тобто назви, символи або логотипи, що належать бренду, послугі або товару), патенти (тобто нові та унікальні твори, інновації та винаходи) та комерційні секрети (тобто цінна інформація про

бізнес-процеси та практики, які є секретними та захищають конкурентну перевагу компанії).

2.5. Дії, що використовують експлуатацію комп'ютера з метою заподіяти шкоди

Згідно з Проектом доповіді УНЗ ООН «Всебічне дослідження проблеми кіберзлочинності» за 2013 рік, «діяння, що передбачають використання комп'ютера з метою заподіяння особистої шкоди», включають «використання комп'ютерної системи з метою домагання, переслідування, залякування чи загроз людині». Прикладами таких видів кіберзлочинів є кіберпереслідування, кібердомагання та кібертравля.

Ці кіберзлочини не включені до багатосторонніх та регіональних договорів про кіберзлочинність (наприклад, Конвенцію Ради Європи про кіберзлочинність; Конвенцію Африканського союзу про кібербезпеку та захист особистих даних; та Конвенцію Ліги арабських держав про боротьбу зі злочинами в галузі інформаційних технологій).

Терміни кіберпереслідування, кібердомагання та кібертравля використовуються взаємозамінно. У деяких країнах будь-яка дія, яка вчиняється за участю дитини, яка виступає як жертва, або правопорушник, називається кібертравлею (наприклад, в Австралії та Новій Зеландії), у той час як у деяких штатах США термін «кібертравля» використовується для позначення дій, скоєних дітьми та проти дітей. Деякі країни не використовують термін «кібертравля» і використовують замість нього термін «кібердомагання» або «кіберпереслідування», або інші терміни, такі як кібермобінг (в Австрії та Німеччині), для позначення кібертравлі (European Parliament, Citizens' Rights and Constitutional Affairs, 2016), тоді як інші країни не використовують жодного з цих термінів. До таких країн належить, наприклад, Ямайка, яка забороняє «зловмисні та/або образливі повідомлення» відповідно до статті 9 (1) Закону про кіберзлочини 2015 року, яка передбачає, що особа вчиняє злочин, якщо вона «(а)... використовує комп'ютер для відправки іншій особі будь-яких даних (чи то

у формі повідомлення або іншим чином), які є непристойними, становлять загрозу або мають загрозовий характер; та (b) шляхом надсилання таких даних навмисно або з необережності завдає роздратування, незручність, занепокоєння чи хвилювання цій особі або будь-якій іншій особі».

Приклад. У 2017 році правозахисницю Латою Нугент (Latoya Nugent) було взято під варту після пред'явлення звинувачень на підставі статті 9 Закону Ямайки про кіберзлочини 2015 року за розміщення в соціальних мережах імен осіб, які вчинили сексуальне насильство. Звинувачення проти неї було згодом знято. Ця стаття закону, яка забороняє розповсюдження зловмисних повідомлень в Інтернеті, розкритикувалася за необґрунтоване обмеження свободи вираження думок. Стаття кенійського закону зі схожим формулюванням (стаття 29 Закону Кенії про інформацію та комунікацію) була скасована, оскільки була визнана національним судом конституції, що суперечить, через її розпливчате і неточне формулювання та відсутність ясності щодо типів виразів (або висловлювань), які можуть вважатися незаконними відповідно до цього закону.

Кіберпереслідування. Використання інформаційно-комунікаційних технологій (ІКТ) для здійснення неодноразових дій протягом певного періоду часу з метою домагання, занепокоєння, нападок, погроз, залякування та/або словесної образи особи (або осіб).

Кібердомагання. Використання ІКТ для навмисних дій з метою приниження, роздратування, нападок, погроз, залякування, завдання образи особи (або осіб).

Кібертравля. Використання ІКТ дітьми з метою досадження, приниження, завдання образи, домагання, залякування, переслідування, жорстокого поводження або інших нападок щодо інших дітей.

Відмінності між цими видами кіберзлочинів полягають у віці злочинців (наприклад, тільки діти здійснюють кібертравлю і є її жертвами), а також в інтенсивності та частоті випадків скоєння

кіберзлочину (кіберпереслідування передбачає серію інцидентів протягом певного часу, у той час як кібердомагання може включати в себе один чи кілька інцидентів).

2.6. Залучення дітей або «грумінг»

Інформаційно-комунікаційні технології використовуються для сприяння у вчиненні «грумінгу» щодо дітей. «Грумінг» дітей – це процес встановлення взаєморозуміння та довіри через розвиток емоційних стосунків із жертвою. Процес «грумінгу» варіює у значних межах з погляду стилю, тривалості та інтенсивності, що часто залежить від особистих якостей та поведінки злочинця. Злочинець може маніпулювати жертвою, використовуючи різні силові методи та методи контролю, включаючи (зокрема): лестощі, подарунки, ізоляцію, залякування, погрози та/або насильство, а також симулювання спільних інтересів або завоювання довіри шляхом імітації почуття самотності дитини. «Грумінг» дітей може відбуватися на платформах соціальних мереж, електронною поштою, у чатах, через служби обміну миттєвими повідомленнями, додатки тощо. Дослідження, проведене британською мовною корпорацією BBC у 2017 році, показало, що додаток Periscope, який дозволяє вести пряму трансляцію в будь-якій точці світу, використовувався зловмисниками для «грумінгу» дітей. Зловмисники, які зв'язувалися з дітьми, що брали участь у прямих трансляціях, висловлювали сексуалізовані коментарі про дітей, а деякі навіть просили дітей зняти свій одяг (BBC, 2017).

2.7. Правопорушення, пов'язані зі змістом комп'ютерних даних.

Як видно із заголовка, кіберзлочини, включені до цього розділу, пов'язані з незаконним контентом. Показовим прикладом незаконного контенту є матеріали із зображенням сексуального насильства над дітьми. Термін «матеріали із зображенням сексуального насильства над дітьми» слід використовувати замість «дитячої порнографії», оскільки термін «дитяча порнографія» мінімізує серйозність злочину. Тим не менш, у

міжнародних, регіональних та національних законах використовується термін «дитяча порнографія» замість терміна «матеріали із зображенням сексуального насильства над дітьми».

Стаття 9 Конвенції Ради Європи про кіберзлочинність передбачає кримінальну відповідальність за правопорушення, пов'язані з дитячою порнографією, причому концепція дитячої порнографії включає візуальні зображення «участі неповнолітньої особи у відвертих сексуальних діях, участі особи, яка здається неповнолітньою, зображення неповнолітньої особи, яка бере участь у відвертих сексуальних діях». Ця концепція дитячої порнографії перестала бути загальноприйнятою; деякі держави передбачають кримінальну відповідальність за поширення нереалістичних зображень дитячої порнографії, таких як мультфільми та малюнки (наприклад, Бразилія, Коста-Ріка, Домініканська Республіка, Гватемала, Мексика, Нікарагуа, Панама та Уругвай), тоді як інші держави передбачають кримінальну відповідальність за поширення зображень за участю реальних дітей (наприклад, Аргентина, Болівія, Чилі, Колумбія, Еквадор, Сальвадор, Гондурас, Парагвай, Перу та Венесуела).

Відповідно до статті 9 Конвенції Ради Європи про кіберзлочинність особа вважається такою, що вчинила злочин у разі навмисного та протиправного вчинення нею таких діянь: «виробництво дитячої порнографічної продукції з метою розповсюдження через комп'ютерну систему; пропозиція чи надання у користування дитячої порнографії через комп'ютерну систему; поширення чи передача дитячої порнографії через комп'ютерну систему; придбання дитячої порнографії через комп'ютерну систему для себе чи іншої особи; володіння дитячою порнографією, що зберігається у комп'ютерній системі чи на носіях комп'ютерних даних».

Стаття 29(3)(a-d) Конвенції Африканського союзу про кібербезпеку та захист особистих даних також забороняє виробництво, придбання, зберігання дитячої порнографії та сприяння її створенню та розповсюдженню.

Скандально відомому педофілу (тобто людині, яка відчуває сексуальний потяг до дитини) Метью Фолдеру, британському вченому, доктору наук Кембриджського університету, в 2017 році було пред'явлено звинувачення в скоєнні більш ніж 137 злочинів по відношенню до 46 осіб, у тому числі вчинення статевого акту з неповнолітнім членом сім'ї, підбурювання до сексуальної експлуатації дітей, зберігання та розповсюдження дитячої порнографії та скоєння інших злочинів. Він шантажував своїх жертв, змушуючи їх робити образливі, огидні, принизливі та непристойні дії проти самих себе та проти інших осіб, і знімав ці дії на фото та відео. Потім він ділився фотографіями та відеозаписами на основних сайтах на тему hurtcore («завдавати біль») (таких як Hurt2theCore, який вже припинив існування), що спеціалізувалися на розміщенні матеріалів з зображень актів зґвалтування, вбивства, садизму, тортур і педофілії.

Комерційна сексуальна експлуатація дітей – це термін, який використовується для опису деяких видів діяльності та злочинів, пов'язаних із сексуальним насильством над дітьми в обмін на будь-яку грошову чи негрошову винагороду (наприклад, притулок, їжа). Прикладом комерційної сексуальної експлуатації дітей є пряма трансляція сексуального насильства над дітьми, яка передбачає передачу та мовлення в режимі реального часу сцен сексуального насильства над дітьми, коли глядачі можуть бути пасивними чи активними (тобто вони можуть спостерігати та/або взаємодіяти з жертвою, просити саму дитину про вчинення певних дій або просити дорослих про вчинення певних дій щодо дитини).

Крім матеріалів із зображенням сексуального насильства над дітьми та прямої трансляції сцен сексуального насильства над дітьми, інші матеріали, включені до цієї категорії, не у всіх країнах визнаються незаконними, наприклад, «расистські та ксенофобські матеріали», які означають «будь-які письмові матеріали, будь-яке зображення або будь-

яке інше уявлення ідей чи теорій, які пропагують, сприяють чи підбурюють до ненависті, дискримінації чи насильства проти будь-якої особи чи групи осіб, якщо як привід до цього використовуються фактори, засновані на расі, кольорі шкіри, національному чи етнічному походженні, а також релігії», і які заборонені статтею 2(1) Додаткового протоколу до Конвенції Ради Європи про кіберзлочинність, що стосується кримінальної відповідальності за акти расистського та ксенофобського характеру, які здійснюються через комп'ютерні системи (2003 р). Тим не менш, такі матеріали заборонені регіональними та міжнародними договорами, наприклад, статтею 29(3)(e-f) Конвенції Африканського союзу про кібербезпеку та захист особистих даних та статтею 20(2) Міжнародного пакту про цивільні та політичні права 1966 року, який забороняє « будь-який виступ на користь національної, расової чи релігійної ненависті, що є підбурюванням до дискримінації, ворожнечі чи насильства».

У деяких країнах публікація неправдивої інформації також вважається злочином. У Танзанії стаття 16 Закону про кіберзлочини 2015 року забороняє публікацію «інформації або даних, представлених у вигляді зображення, тексту, символу або в будь-якій іншій формі, у комп'ютерній системі, якщо особа, яка публікує ці дані та інформацію, свідомо знає, що вони є хибними, невірними, які вводять в оману або неточними і публікуються з метою компрометації, загрози, образи, або введення в оману громадськості іншим чином, або з метою пособництва у скоєнні злочину у вигляді дачі порад». Закон Кенії про неправомірне використання комп'ютерних технологій та кіберзлочини 2018 року також передбачає кримінальну відповідальність за «відоме оприлюднення неправдивої інформації в друкованих та мовних засобах масової інформації або через комп'ютерну систему, яка тягне за собою паніку, хаос чи насильство серед громадян республіки або розрахована на поширення паніки, хаосу чи насильства, чи може призвести до дискредитації репутації особи» (стаття 23). Проте, згідно з Проектом доповіді УНЗ ООН «Всебічне дослідження

проблеми кіберзлочинності» (2013), «країни повідомляють про різний рівень обмеження свободи вираження поглядів, у тому числі щодо дифамації (розповсюдження ганебних відомостей), неповаги, загроз, підбурювання до ненависті, образи релігійних почуттів, непристойних матеріалів та підризу державних засад» (УНЗ ООН, 2013). У ряді випадків видалення урядовими структурами Інтернет-контенту, що відноситься до таких форм вираження поглядів, викликало занепокоєння в контексті дотримання прав людини (УНЗ ООН, 2013, с. 28).

У 2005 році Рада безпеки ООН прийняла резолюцію 1624, яка (в числі іншого) закликає всі держави «вжити таких заходів, які можуть бути необхідні та доречні та відповідатимуть їхнім зобов'язанням з міжнародного права, щоб: законодавчо заборонити підбурювання до вчинення терористичного акту чи актів і запобігати такій поведінці» (UNSCR 1624 (2005)). Заходи, які держави-учасниці можуть вжити з метою досягнення цієї мети, включають криміналізацію підбурювання до тероризму.

Інші міжнародні органи також закликають держави вжити заходів щодо боротьби з підбурюванням до тероризму в рамках своїх національних правових систем. Наприклад, стаття 3 Рамкового рішення Ради Європейського Союзу 2008/919/JHA від 28 листопада 2008 року про внесення поправок до Рамкового рішення 2002/475/JHA про боротьбу з тероризмом та стаття 5 Конвенції Ради Європи про запобігання тероризму зобов'язують держави-учасниці запровадити кримінальну відповідальність за дії чи заяви, які є підбурюванням до здійснення терористичних актів. Крім того, Конвенція Ради Європи про запобігання тероризму накладає на держави-учасниці зобов'язання щодо криміналізації «публічного підбурювання до скоєння терористичних злочинів», а також вербування та підготовки терористів (UNODC, 2012, pp. 39-40).

Хоча нині у міжнародному праві немає універсального зобов'язання, що має юридичну силу для всіх держав, з криміналізації дій, пов'язаних з

підбурюванням до тероризму, багато держав використовують правові і кримінально-правові підходи боротьби з такими діям і актами. Прикладами підходів, що використовуються в деяких країнах, є використання Сполученими Штатами параграфу 373 (а) титулу 18 Зводу законів США, який забороняє підбурювання та змову для успішного переслідування винних у скоєнні дій, пов'язаних із підбурюванням до тероризму (наприклад, справа United States of America Emerson Winfield Begolly, UNODC, 2012, pp.39-41), а також використання владою Великобританії статті 1 Закону про тероризм 2006 року, який передбачає кримінальну відповідальність за «заохочення тероризму» наступним чином.

Особа вчиняє злочин, якщо:

(а) вона публікує заяву, на яку поширюється дія цієї статті, або спонукає іншу особу до публікації такої заяви;

(b) у момент, коли вона публікує цю заяву або спонукає іншу особу до її публікації, вона:

має на меті, щоб ця заява була зрозуміла представниками громадськості як пряме чи опосередковане заохочення або інше спонукання до вчинення, підготовки чи підбурювання до актів тероризму чи злочинів, передбачених Конвенцією;

байдуже ставиться до того, чи буде ця заява зрозуміла представникам громадськості як пряме чи опосередковане заохочення чи інше спонукання до скоєння, підготовки чи підбурювання до актів тероризму чи злочинів.

Влада Великобританії вже має успішний досвід кримінального переслідування діянь, пов'язаних із підбурюванням до тероризму, відповідно до Закону про тероризм 2000 року. Див. справу Юніса Тсулі (Younes Tsouli) та інших осіб, які були засуджені на підставі цього закону за підбурювання до тероризму за кордоном шляхом розміщення матеріалів

на веб-сайтах та в чатах, які вони створили, адміністрували та контролювали.

Незважаючи на відсутність у міжнародному праві будь-якого універсального юридично зобов'язання держав здійснювати заходи щодо боротьби з підбурюванням до тероризму, багато держав вжили таких заходів на національному рівні. Однак деякі фактори продовжують створювати труднощі для прийняття узгодженого на міжнародному рівні підходу до вирішення цієї проблеми, включаючи відсутність загальноприйнятого визначення тероризму та відмінності в національних конституційних та правових підходах до основних прав людини, таких як право на вільне вираження думок та свободу об'єднань, конфіденційність тощо. Тому перед законодавцями, правоохоронними органами та органами кримінального правосуддя всіх держав, як і раніше, стоїть важке завдання прийняття та впровадження національних підходів, які націлені на інформаційні матеріали в Інтернеті, що підбурюють до насильницьких актів тероризму, і не надають при цьому «обмежувального впливу» на легітимне законне право на вираження певних політичних чи ідеологічних поглядів.

Висновок

Приватні особи, групи та держави можуть займатися (і займаються) діяльністю, пов'язаною з незаконним доступом до систем, мереж та даних, перехопленням повідомлень та втручанням у функціонування систем та мереж або дані (наприклад, шляхом проведення хакерських атак, DoS та DDoS-атак і поширення шкідливих програм). ІКТ є мішенню кіберзлочинців і використовуються для сприяння вчиненню кіберзлочинів. Так само, як немає універсального визначення кіберзлочинності, немає і загальноприйнятих визначень різних видів кіберзлочинів і загальних категорій кіберзлочинності.

Вправа № 1. Який це тип кіберзлочинності?

Корпоративний контролер трейдера товарів нібито отримав електронні листи від генерального директора компанії та аудиторської фірми з Києва, яка працює з компанією, із запитом на три банківські перекази до кіпрського банку на загальну суму приблизно 17 мільйонів доларів. У електронних листах містилося прохання до контролера не баритися, оскільки гроші йшли на придбання кіпрської компанії. Контролер задовольнив запити, припускаючи, що генеральний директор керував ними, хоча використана електронна адреса не була офіційною електронною адресою компанії.

Вправа № 2 – Справи про кіберзлочини

Розподілити студентів випадковим чином у групи перед заняттям, щоб дати їм змогу виконати завдання до того, як клас зустрінеться. Кожній групі слід випадковим чином розподілити одну з наступних категорій:

Злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем

Злочини, пов'язані з комп'ютером

Правопорушення, пов'язані зі змістом

Студенти повинні провести дослідження та знайти справу про кіберзлочин, а також підготуватися до обговорення справи в класі. Студенти можуть шукати справу про кіберзлочин за допомогою бази даних прецедентного права UNODC SHERLOC.

Питання для самоперевірки

1. Які загальні категорії кіберзлочинності?
2. Які кіберзлочини підпадають під ці категорії?
3. Чи є злочини, які підпадають під більш ніж одну категорію?

Якщо так, то які?

4. Визначте кіберзлочин. Як скоюється цей кіберзлочин? Будь ласка, опишіть детально процес.

Лекція 3. Правова база. Роль законодавства про кіберзлочинність у цифровій криміналістиці.

3.1. Законодавство про кіберзлочинність

3.2. Уніфікація законодавства.

3.3. Міжнародні та регіональні правові документи.

3.4. Міжнародне право в галузі прав людини та законодавство про кіберзлочинність

3.1. Законодавство про кіберзлочинність

Законодавство про кіберзлочинність визначає стандарти прийнятної поведінки для користувачів інформаційно-комунікаційних технологій (ІКТ); встановлює соціально-правові санкції за кіберзлочини; захищає користувачів ІКТ загалом і пом'якшує та/або запобігає шкоді, заподіяній людям, даним, системам, сервісам та інфраструктурі зокрема; захищає права людини; забезпечує можливість для проведення розслідувань та здійснення кримінального переслідування щодо злочинів, що скоюються в мережі Інтернет (поза межами реального світу); та сприяє співпраці між країнами у справах, пов'язаних із кіберзлочинами. Законодавство в галузі кіберзлочинності передбачає правила та стандарти поведінки при використанні Інтернету, комп'ютерів та пов'язаних з ними цифрових технологій та дії публічних, державних та приватних організацій; норми доказового права, правила здійснення кримінального судочинства та інші питання кримінального права, пов'язані з кіберпростором; положення про зниження ризику та/або пом'якшення шкоди, заподіяної фізичним особам, організаціям та інфраструктурі у разі скоєння кіберзлочину. Отже, законодавство у сфері кіберзлочинності включає в себе матеріальне, процесуальне і превентивне право.

Матеріальне право

Незаконне діяння має бути чітко прописане в законі та заборонено законом. Відповідно до морального принципу «*nullum crimen sine lege*»

(лат. «немає злочину без закону, що його передбачає»), особа не може бути піддана покаранню за діяння, яке не було прописано в законі на момент вчинення особою цього діяння (УНЗ ООН, 2013 , Стор. 59).

Матеріальне право визначає права та обов'язки суб'єктів права, до яких належать фізичні особи, організації та держави.

Джерелами матеріального права є нормативно-правові акти та розпорядження, що приймаються місцевими та центральними законодавчими органами (статутне право), федеральні конституції та конституції федеральних одиниць, а також судові рішення (у системах загального права).

Деякі країни, замість розробки нових спеціальних законів боротьби з кіберзлочинністю, внесли поправки до свого національного законодавства чи кодексів, доповнивши їх окремими положеннями, що стосуються кіберзлочинів. Ця практика мала цікаві наслідки, що заслуговують на увагу, які полягали в тому, що деякі країни вирішили окремо криміналізувати діяння, пов'язане з незаконним використанням інформаційно-комунікаційних технологій для скоєння злочину. Таким чином, якби злочинець використав незаконний доступ для скоєння підробки чи шахрайства, таке діяння утворило б одночасно два злочини.

Матеріальне законодавство в галузі кіберзлочинності включає закони, які забороняють конкретні види кіберзлочинів, і передбачає покарання за недотримання цих законів. До кіберзлочинів належать традиційні злочини в реальному світі (поза мережею Інтернет) (наприклад, шахрайство, фальсифікація, організована злочинність, відмивання грошей і крадіжка), що скоюються в кіберпросторі, які є «гібридними» злочинами або «злочинами з використанням кібермереж», а також «новими» або «кіберзалежними» злочинами, які стали можливими з винаходом Інтернету та цифрових технологій, що функціонують через Інтернет. Тому багато країн розробили закони, які безпосередньо призначені для протидії кіберзлочинності. Наприклад, Німеччина, Японія та Китай внесли

поправки до відповідних положень своїх кримінальних кодексів з метою боротьби з кіберзлочинами. Деякі країни також використовували чинні закони, які були розроблені для боротьби зі злочинністю в реальному світі (поза мережею Інтернет), щоб охопити певні види кіберзлочинності та кіберзлочинців. Як ще один приклад можна навести Ірак, де чинні цивільний кодекс (Цивільний кодекс Іраку №.40 від 1951 року) та кримінальний кодекс (Кримінальний кодекс Іраку №.111 від 1969 року) використовуються для судового переслідування за злочини, які скоюються в реальному світі (наприклад, шахрайство, шантаж, розкрадання персональних даних) з використанням Інтернету та цифрових технологій.

Правові системи

Кожна держава має власну правову систему, яка впливає створення матеріального кримінального права у сфері кіберзлочинності. Ці системи включають:

1) Загальне право. Країни із системою загального права створюють закони на основі судових прецедентів (тобто рішення, винесене у справі, є обов'язковим для суду та нижчих судів) та усталеної практики. Ці закони існують у вигляді окремих законів та прецедентного права (тобто права, яке формується на основі рішень судів чи судових прецедентів).

2) Цивільне право. Країни з такою системою права мають кодифіковані, консолідовані та всеосяжні правові норми та закономірності, які встановлюють межі основних прав, зобов'язань, обов'язків та очікувань щодо поведінки. Ці системи засновані переважно на законодавстві та конституціях.

3) Звичайне право. Ці правові системи включають укорінені та загальноприйняті моделі поведінки в рамках культури, які сприймаються носіями цієї культури як закон (*opinio juris* – переконаність у правомірності). У міжнародному праві звичайне право регулює взаємовідносини і практику між державами і вважається обов'язковим всім державам.

4) Релігійне право. У системах релігійного права як джерело права використовуються правила, що ґрунтуються на релігійних навчаннях або релігійній літературі.

5) Правовий плюралізм. У правовій системі такого типу можливе співіснування двох або більше вищезгаданих правових систем (тобто загального, громадянського, звичайного чи релігійного права).

Матеріальне право зосереджено на суті злочину, наприклад, елементах складу злочину, які включають заборонене діяння (*actus reus* – «винна дія») та суб'єктивну сторону (*mens rea* – «злочинний намір»). Різні країни можуть надавати перевагу криміналізації різних діянь з урахуванням різних елементів, які утворюють склад злочину. В якості альтернативи країни можуть криміналізувати ті ж дії, проте закони можуть відрізнятися з точки зору того, яка «суб'єктивна сторона» робить осіб винними за таке діяння (тобто з точки зору ступеня кримінально-правової вини). У зв'язку з цим закони, які кримінализують, наприклад, несанкціонований доступ до комп'ютерних систем та даних, відрізняються в різних країнах залежно від ступеня наміру злочинця (див. «Рівні кримінально-правової провини» у вставці нижче).

Рівні (форми) кримінально-правової провини

Існують різні рівні кримінально-правової провини (або кримінальної відповідальності) залежно від ступеня, в якому незаконна дія була навмисною (досконалою свідомо або навмисне) або ненавмисною (досконалою з необачності або необережності), яка в різних правових системах тлумачиться по-різному.

Свідомо. Особа свідомо вчиняє злочин, коли вона діє з метою заподіяння шкоди (тобто особа має намір заподіяти шкоду). Як приклад можна навести Закон Сполученого Королівства про неправомірне використання комп'ютерних технологій 1990 року, який криміналізує, серед іншого, несанкціонований доступ до систем та даних з наміром

викликати зміни та/або пошкодження, порушення нормальної роботи систем та сервісів та модифікації системних даних та програм.

Навмисне. Особа навмисне вчиняє злочин, коли йому відомо про те, що його дія завдасть шкоди, але вона, проте, робить таку дію та завдає шкоди. Відповідно до Закону про комп'ютерне шахрайство та зловживання 1986 року, зокрема, параграфом 1030(a)(1) розділу 18 Зводу законів США, особі можуть бути пред'явлені звинувачення, якщо вона: свідомо проникнувши в комп'ютер без необхідних на те санкцій або переступивши межі санкціонованого доступу і за допомогою цієї дії отримавши інформацію, яка була визначена Урядом Сполучених Штатів згідно з указом або актом виконавчої влади, яка потребує захисту від несанкціонованого розкриття з міркувань національної оборони чи міжнародних відносин, або отримавши якусь будь-яку закриту інформацію, як це визначено в параграфі «у» статті 11 Закону про атомну енергію від 1954 року, за наявності підстав вважати, що отримана таким чином інформація може використовуватися з метою заподіяння шкоди Сполученим Штатам або на користь будь-якої іноземної держави, навмисне повідомляє, спрямовує, передає або вживає заходів для повідомлення, направлення або передачі, або намагається повідомити, направити, передати або вжити заходів для повідомлення, направлення або передачі такої інформації будь-якій особі, яка не має права отримувати її, або навмисне зберігає цю інформацію не передає її посадовцю або службовцю Сполучених Штатів, яка має право на її отримання.

По необачності (або легковажності). Особа вчиняє злочин через необачність, коли вона вчиняє акт, навіть незважаючи на те, що вона усвідомлює суттєвий і не виправданий ризик заподіяння шкоди іншим особам, проте демонструє зневагу або байдужість до такого ризику заподіяння шкоди. В Австралії особі можуть бути пред'явлені звинувачення на підставі положень розділу 477.2(1)(c) Закону про

кіберзлочинність 2001 р. (№.161, 2001), якщо «обличчя необачно не усвідомлює того, що несанкціонована зміна даних порушує: (i) доступ до цих або будь-яких інших даних, що зберігаються на будь-якому комп'ютері; або (ii) достовірність, безпека або застосовність будь-яких таких даних».

З необережності. Необережність є найнижчим ступенем винності. Особи, які роблять якісь дії з необережності, не усвідомлюють негативних наслідків своєї поведінки. У Сенегалі «будь-яка особа, яка навіть за необережністю обробляє або організує обробку персональних даних без дотримання формальних вимог, викладених у Законі про персональні дані, до використання таких даних, підлягає покаранню» (стаття 431-17, Закон №.2008-11) про кіберзлочинність).

Тут важливо відзначити два моменти. По-перше, місцеве застосування закону (кримінальне переслідування) можливе лише в тому випадку, коли кримінальне переслідування відповідає інтересам суспільства, при цьому велика кількість масових кіберзлочинів, таких як шахрайство через Інтернет, належать до малозначних відповідно до принципу *de minimis non-curat lex*. (Лат. Закон не дбає про дрібниці), в тому сенсі, що окремо вони вважаються занадто незначними за своїми наслідками, щоб виправдати розслідування поліцією або кримінальне переслідування. Тим не менш, вони можуть спричинити значні сукупні наслідки в міжнародному масштабі, тому вони мають підпадати під дію міжнародного права. По-друге, «за відсутності надійного обґрунтування криміналізації певних діянь виникає ризик надмірної криміналізації. У цьому плані міжнародне право в галузі прав людини є одним із важливих інструментів, необхідних для оцінки кримінального права відповідно до зовнішніх, міжнародних стандартів» (УНЦ ООН, 2013, стор. 60).

Процесуальне право

Процесуальне право визначає межі процесів і процедур, які необхідно дотримуватись при застосуванні норм матеріального права, а також правила, що забезпечують можливість застосування матеріального права. Важливою частиною процесуального законодавства є кримінально-процесуальне право, яке включає вичерпні правила та керівні принципи щодо того, як повинні поводитися з підозрюваними, обвинуваченими та засудженими особами система кримінального правосуддя та її співробітники. Нарешті, процесуальне законодавство в галузі кіберзлочинності включає положення про юрисдикцію та слідчі повноваження, норми доказового права та правила здійснення кримінального судочинства, які відносяться до процедур збору даних, перехоплення повідомлень, обшуку та виїмки, збереження та зберігання даних. Кіберзлочинність створює деякі унікальні складнощі щодо процедур, особливо тих, які пов'язані з юрисдикцією, розслідуваннями та цифровими доказами.

Юрисдикція. Правоохоронні органи мають право здійснювати розслідування кіберзлочинів, а національні суди мають право виносити рішення у справах про кіберзлочини лише в тих випадках, якщо зацікавлена держава має відповідну юрисдикцію. Під юрисдикцією розуміється право та повноваження держави застосовувати закони та призначати покарання за недотримання законів. Питання юрисдикції тісно пов'язані з державним суверенітетом, тобто з правом держави здійснювати повноваження на власній території (УНЦ ООН, 2013, стор. 61). Юрисдикція зазвичай пов'язана з географічною територією або *locus commissi delicti* (місце скоєння злочину), коли держава заявляє про свою юрисдикцію щодо злочинів, скоєних на її території та здійснює переслідування винних у їх скоєнні (принцип територіальності). Враховуючи відсутність географічних кордонів та територій у кіберпросторі, місцезнаходження не може використовуватись для визначення юрисдикції. Тому держави використовують цілий ряд

факторів, щоб визначити юрисдикцію. Одним із таких факторів є громадянство правопорушника (принцип державної власності; принцип активної правосуб'єктності). Цей принцип визнає право держав здійснювати переслідування своїх громадян, навіть якщо ці громадяни перебувають за межами їхньої території. У меншій мірі (з точки зору застосування) для встановлення юрисдикції щодо злочину може використовуватися громадянство потерпілого (принцип державної приналежності; принцип пасивної правосуб'єктності). Держава може також встановлювати юрисдикцію в тому випадку, коли злочин, скоєний в іншій державі (наприклад, державна зрада або шпигунство), завдав шкоди інтересам та безпеці держави, яка домагається здійснення юрисдикції щодо цього злочину (принцип захисту). Нарешті, будь-яка держава може встановити юрисдикцію щодо певних транснаціональних злочинів, таких як масові злочини (наприклад, геноцид), які розглядаються як злочини, які торкаються всіх людей, незалежно від географічного розташування, коли держава, на території якої було скоєно злочин, не бажає або неспроможна здійснювати переслідування винних осіб (принцип універсальності).

Слідчі дії та повноваження. Цифрові докази кіберзлочинів пов'язані з особливими труднощами – як у плані поводження з ними, так і з точки зору їх використання в судовому провадженні. Як зазначалося в проєкті доповіді УНЦ ООН «Всебічне дослідження проблеми кіберзлочинності» у 2013 році, «в той час, як деякі такі слідчі дії можуть бути здійснені на підставі традиційних повноважень, багато процесуальних положень, в основі яких лежить просторовий, об'єктно-орієнтований підхід, важко застосовувати в ситуаціях, пов'язаних із зберіганням цифрових даних та потоками даних у режимі реального часу» (стор. 137), тому для проведення розслідування необхідні спеціальні повноваження (УНЦ ООН, 2013, стор. 60). Такі спеціальні повноваження передбачаються законом і не тільки поширюються на доступ до необхідної інформації, але й включають гарантії для забезпечення того, щоб дані були отримані відповідно до

належних законних розпоряджень і були доступні тільки в тій мірі, в якій це необхідно і дозволено законом. Закон США про збережені повідомлення (титул 18 Зводу законів США, § 2701-2712), що є титулом II Закону про конфіденційність електронних повідомлень 1986 року, передбачає такі гарантії. Наприклад, згідно з параграфом 2703(a) титулу 18 Зводу законів США: державна установа має право вимагати від провайдера послуг електронних комунікацій розкриття змісту провідних або електронних повідомлень, що зберігаються в електронному сховищі системи електронних комунікацій протягом не більше ста вісімдесяти днів, лише на підставі ордера, виданого відповідно до процедур, описаних у Федеральних правилах кримінального провадження (або, у разі суду штату, виданого відповідно до порядку видачі судових ордерів, який діє у цьому штаті), судом компетентної юрисдикції.

Проте ці гарантії (тобто вимога законного розпорядження) потрібні не в усіх країнах. У 2014 році Туреччина внесла поправки до Закону про Інтернет №5651, щоб вимагати від інтернет-провайдерів збереження даних користувачів та надавати їх владі на першу вимогу без необхідності отримання законного розпорядження (наприклад, рішення суду або ордера на обшук) для отримання цих даних. Такі слідчі повноваження виходять за рамки звичайного збору доказів та передбачають отримання сприяння та взаємодію з іншими представниками системи кримінального правосуддя у справах, пов'язаних із кіберзлочинністю. Така сама ситуація склалася в Танзанії, де Закон про кіберзлочинність 2015 року наділив поліцію надмірними, необмеженими слідчими повноваженнями щодо кіберзлочинів. Зокрема, санкція поліції є єдиною вимогою для обшуку та вилучення доказів і примусу до розкриття даних. Відповідно, обшук та виїмка, а також інші слідчі дії можуть проводитись без наявності належних законних розпоряджень. Крім того, існує небезпека «розмивання (відхилення від основного) мандата» або «розмивання функцій» (ці терміни використовуються для опису випадків поширення законів та/або

інших заходів на області, що знаходяться за межами їхньої початкової сфери дії), коли закони та слідчі повноваження, спрямовані на один вид кіберзлочинності, згодом поширюються на інші, менш тяжкі види кіберзлочинів. Зрештою, повноваження та процедури, які використовуються для розслідування кіберзлочинів та судових розглядів, повинні відповідати принципам верховенства закону та стандартам у галузі прав людини (див., наприклад, статтю 15 Конвенції Ради Європи про кіберзлочинність 2001 року).

Ідентифікація, збирання, обмін, використання та допустимість цифрових доказів. Процесуальне законодавство у сфері кіберзлочинності охоплює аспекти ідентифікації, збирання, зберігання, аналізу та обміну цифрових доказів. До цифрових доказів (або електронних доказів) відноситься «інформація будь-якого типу, яку можна витягти з комп'ютерних систем або інших цифрових пристроїв, і яка може використовуватись для доказу чи спростування факту правопорушення». Цифрові докази можуть підтвердити або спростувати свідчення потерпілого, свідка та підозрюваного, підтвердити або спростувати правдивість твердження про факт, визначити мотив, намір і місце правопорушника (дії та поведінка в минулому) та встановити ступінь кримінально-правової провини.

Норми доказового права та правила кримінального судочинства включають критерії, що використовуються для визначення допустимості цифрових доказів у суді. Вони описуються процедури документування, збору, збереження, передачі, аналізу, зберігання та захисту цифрових доказів з метою забезпечення їх допустимості в національних судах. Для того щоб цифрові докази були допустимими в суді, проводиться їхня автентифікація та встановлюється їхня цілісність. Процедури автентифікації включають визначення джерела/автора цифрових доказів (наприклад, ідентифікаційної інформації про джерело) та перевірку цілісності доказів (наприклад, щодо того, що вони не були якимось чином

змінені, підтасовані або пошкоджені). Найважливішим значенням для забезпечення допустимості цифрових доказів у більшості судів є система охорони доказів, яка включає докладний облік доказів, їх стану, процесів збору, зберігання, отримання доступу та передачі, а також причин отримання доступу та передачі. У різних країнах діють різні стандарти норм доказового права та правил кримінального судочинства. Для боротьби з кіберзлочинністю необхідні подібні норми доказового права та кримінального судочинства, оскільки злочини такого типу не знають кордонів і впливають на цифрові докази та системи у будь-якій точці світу через підключення до мережі Інтернет.

Превентивне право

Превентивне право ґрунтується на регулюванні та зниженні ризиків правопорушень. У контексті кіберзлочинності мета превентивного законодавства полягає або у запобіганні кіберзлочинам, або, як мінімум, у пом'якшенні збитків, які завдають скоєння кіберзлочинів (УНЗ ООН, 2013, стор. 61). Закони про захист даних (наприклад, Загальні положення про захист даних ЄС 2016 року та Конвенція Африканського союзу про кібербезпеку та захист персональних даних 2014 року) та Закон України «Про основні засади забезпечення кібербезпеки України» 2017 року прийнято з метою зниження матеріальних збитків внаслідок кіберзлочинів, пов'язаних із витоком особистих даних, та/або мінімізації вразливості громадян до кіберзлочинів. Інші закони дозволяють співробітникам системи кримінального правосуддя виявляти та розслідувати кіберзлочини та здійснювати кримінальне переслідування винних шляхом забезпечення можливості для використання необхідних засобів, заходів та процедур, що полегшують здійснення таких дій (наприклад, інфраструктури постачальників телекомунікаційних послуг та послуг електронного зв'язку, що дає їм можливість перехоплення повідомлень та збереження даних).

У Сполучених Штатах Америки Закон про сприяння правоохоронним органам у галузі комунікацій (CALEA) 1994 року

зобов'язує провайдерів телефонного зв'язку та виробників обладнання вживати заходів для того, щоб їх сервіси та продукти забезпечували влади, які мають законний дозвіл (наприклад, належний судовий ордер), можливість отримання доступу до ліній зв'язку.

3.2. Уніфікація законодавства.

Очевидна більшість країн світу мають національні закони, які охоплюють кіберзлочинність або деякі аспекти кіберзлочинності (УНЗ ООН, 2015). У країнах, які не ухвалили закони про кіберзлочинність, створюються безпечні притулки для кіберзлочинців, оскільки особа не може бути притягнута до відповідальності за кіберзлочин, якщо тільки вона не розглядається як незаконна діяльність, яка переслідується згідно із законом. Прикладом є випадок із творцем та розповсюджувачем комп'ютерного вірусу «LOVE BUG», громадянином Філіппін, якого неможливо було притягнути до кримінальної відповідальності (навіть попри те, що цей вірус спричинив несприятливі економічні наслідки для багатьох країн по всьому світу), оскільки на Філіппінах був відсутній закон про кіберзлочинності на момент скоєння діяння. Такі безпечні притулки для кіберзлочинців можуть також створюватися в тому випадку, якщо закони про кіберзлочинність не дотримуються належним чином, та/або якщо існують розбіжності в законодавстві різних країн у галузі кіберзлочинності (УНЗ ООН, 2013, с. 61-65).

Уніфікація основних положень законодавства в галузі кіберзлочинності не лише дозволить запобігти створенню безпечних притулків для кіберзлочинців, а й виключить можливість уникнення серйозного покарання за скоєння кіберзлочинів (УНЗ ООН, 2013, с. 66-69). Ці безпечні притулки створюються тому, що лише ті дії, які перевищують «поріг тяжких злочинів, – який, як правило, виражається у формі можливого покарання, яке може спричинити відповідне діяння, – виправдовують вкладення, необхідні для здійснення міжнародного співробітництва між державами (УНЦ ООН, 2013, с. 67). Таким чином,

уніфікація основних положень законів про кіберзлочинність сприятиме розвитку міжнародного співробітництва.

Уніфікація процесуальних норм законодавства в галузі кіберзлочинності сприятиме створенню умов для збирання доказів у будь-яких країнах світу та обміну доказами в рамках міжнародного співробітництва (УНЗ ООН, 2013, с. 66-69). Всеосяжні та точні процесуальні норми та протоколи, що стосуються цифрових доказів та судової експертизи, і уніфікація цих норм та протоколів могли б забезпечити, щоб цифрові докази, що обробляються в одній країні, були допустимими в іншій країні (або інших країнах).

Національні закони містять положення, які полегшують міжнародне співробітництво. Наприклад, на Ямайці у 2015 році було прийнято Закон про боротьбу з кіберзлочинами з метою уніфікації законодавства та виконання багатьох суттєвих та процесуальних положень Конвенції про кіберзлочинність. У Нігерії Закон про (заборону, запобігання тощо) кіберзлочинів 2015 року закликає до створення Консультативної ради з кіберзлочинності для сприяння здійсненню міжнародного співробітництва у справах, пов'язаних із кіберзлочинністю. У Катарі Закон №.14 від 2014 року про набуття чинності Законом про профілактику кіберзлочинності передбачає слідчі повноваження, норми доказового права та правила судочинства, міжнародне співробітництво, взаємну правову допомогу, екстрадицію та зобов'язання постачальників послуг, пов'язані з кіберзлочином. Існування національних, регіональних та міжнародних законів у галузі кіберзлочинності та уніфікація законодавства держав сприяють міжнародному співробітництву (УНЦ ООН, 2013, с. 61). Уніфікація та застосування національних, регіональних та міжнародних законів також сприяють ліквідації безпечних притулків для кіберзлочинців (Maras, 2016).

3.3. Міжнародні та регіональні правові документи

Існують міжнародні та регіональні договори у сфері боротьби з кіберзлочинністю. Одним із прикладів є Конвенція Ради Європи про кіберзлочинність 2001 року. Мета цієї конвенції полягає в уніфікації національних законодавств, вдосконаленні методів розслідування кіберзлочинів та розширенні міжнародного співробітництва. Вона також містить рекомендації для держав-учасниць конвенції щодо заходів, які необхідно вжити на національному рівні для боротьби з кіберзлочинністю, включаючи внесення поправок та доповнень до норм матеріального права (наприклад, введення відповідальності за правопорушення, пов'язані з кіберзлочинністю, до кримінального законодавства) та кримінально-процесуальне право (наприклад, визначення порядку здійснення кримінального розслідування та судового переслідування). Конвенція також містить рекомендації для держав-учасниць щодо взаємної допомоги та служить як договір про надання взаємної правової допомоги (тобто угоди між країнами про співпрацю у розслідуванні та кримінальному переслідуванні щодо деяких та/або всіх правопорушень, визнаних такими у національних законодавствах обох сторін, для країн, які не мають подібного договору з країною, яка запитує допомогу).

Чи знаєте ви?

У той час, як низка країн активно виступають за ухвалення глобальної конвенції під егідою Організації Об'єднаних Націй, на сьогоднішній день у міжнародному співтоваристві поки що не досягнуто достатнього консенсусу щодо прийняття такої глобальної конвенції в рамках Організації Об'єднаних Націй.

Існує кілька договорів у сфері боротьби з кіберзлочинністю, що мають регіональний характер:

Угода про співпрацю у боротьбі зі злочинами у сфері комп'ютерної інформації, підписана країнами-членами Співдружності Незалежних Держав у 2001 році. Ця угода закликає держави ухвалити національні

закони для виконання положень угоди та уніфікації національних законодавств у сфері боротьби з кіберзлочинністю.

Конвенція Ліги арабських держав про боротьбу зі злочинами в галузі інформаційних технологій, ухвалена Лігою арабських держав у 2010 році. Основна мета цієї конвенції полягає у зміцненні співробітництва між державами для забезпечення ним можливості захисту свого майна, населення та інтересів від кіберзлочинності.

Угода про співробітництво у сфері забезпечення міжнародної інформаційної безпеки, ухвалена Шанхайською організацією співробітництва у 2010 році. Дія цієї угоди виходить за межі кіберзлочинності та кібербезпеки і включає заходи забезпечення інформаційної безпеки держав-учасниць як одну з головних цілей угоди, а також заходи з національного контролю за інформаційними системами та їх контентом.

Проект Конвенції Африканського союзу про створення юридичних основ кібербезпеки в Африці (проект Конвенції Африканського союзу) 2012 року. Ця конвенція сприяє забезпеченню та підтримці людських, фінансових та технічних ресурсів, необхідних для сприяння здійсненню розслідувань кіберзлочинів.

Конвенція Африканського союзу про кібербезпеку та захист персональних даних 2014 року. Ця конвенція містить, серед інших положень, заклик до держав Африканського союзу приймати національні закони та/або вносити поправки до чинних національних законів з метою ефективної боротьби з кіберзлочинністю, уніфікувати національні законодавства, укласти договори про взаємну правову допомогу (ДВПД), якщо вони ще не укладені, сприяти обміну інформацією між державами, сприяти регіональному, міжурядовому та міжнародному співробітництву та використовувати наявні кошти для співпраці з іншими державами та навіть приватним сектором.

Регіональними організаціями та/або регіональними міжурядовими організаціями були також розроблені та імplementовані закони та директиви у сфері боротьби з кіберзлочинністю. Наприклад:

Типовий закон про комп'ютерні злочини та кіберзлочинність Співтовариства розвитку Півдня Африки (СРПА) 2012 року. Цей закон є керівництвом для держав-учасниць СРПА для розробки норм матеріального та процесуального права у сфері боротьби з кіберзлочинністю. Оскільки цей закон є типовим, він не накладає на держави жодних юридичних зобов'язань щодо здійснення співробітництва. Держави, які не мають та/або не розробляють закони про кіберзлочинність, можуть використовувати Протокол СРПА про взаємну правову допомогу у кримінальних справах та Протокол СРПА про видачу для сприяння співпраці та координації при здійсненні міжнародних розслідувань кіберзлочинів.

Директива щодо боротьби з кіберзлочинністю Економічного співтовариства західноафриканських держав (ЕСЗД) 2011 року. Ця директива вимагає від держав-учасниць криміналізації кіберзлочинності у національному законодавстві та сприяє взаємній правовій допомозі, співпраці та видачі злочинців у справах, пов'язаних із кіберзлочинністю та кібербезпекою. ЕСЗД ухвалив Конвенцію про взаємну правову допомогу у кримінальних справах та Конвенцію про видачу з метою сприяння співпраці у розслідуванні кіберзлочинів та видачі кіберзлочинців.

3.4. Міжнародне право в галузі прав людини та законодавство про кіберзлочинність

Основні положення деяких законів про боротьбу з кіберзлочинами, особливо тими, що пов'язані з контентом в Інтернеті, такі як неповага до влади, образа, дифамація глави держави, непристойність чи порнографічні матеріали можуть надмірно обмежувати можливість здійснення певних прав людини (УНЦ ООН, 2013, стор. xxii та 119-120). Процесуальні норми законів про кіберзлочинність, які забезпечують можливість використання

при розслідуванні кіберзлочинів засобів і методів, що дозволяють перехоплювати повідомлення та здійснювати електронне спостереження, також можуть призвести до не виправданого обмеження можливостей здійснення прав людини, таких як право на недоторканність приватного життя (УНЦ ООН, 2013, стор. 136). Необхідно дотримуватися балансу між боротьбою з кіберзлочинністю та дотриманням прав людини.

Міжнародне законодавство в галузі прав людини дозволяє вводити обмеження на здійснення певних прав людини, які можуть обмежуватися на законних підставах у особливих умовах (деякі права не можуть бути обмежені). Ці обмеження є допустимими, коли вони переслідують законну мету, відповідають чинному законодавству і є необхідними та пропорційними до загрози, яка виправдовує їх застосування. Конкретне охоплення законних цілей залежить від застосовних прав людини і може включати інтереси громадської безпеки, національної безпеки, економічної безпеки, охорони здоров'я, захисту моральності та захисту прав інших осіб. На додаток до необхідності запровадження обмежень для досягнення однієї з вищезазначених законних цілей, обмеження має вводитися на підставі національного закону. Цей закон має бути доступним громадянам, щоб вони могли належним чином стежити за своєю поведінкою, знати про повноваження влади при застосуванні цього закону, а також про наслідки його недотримання. Закон має бути чітко сформульований і не повинен допускати надання державним органам влади необмеженої свободи дій у разі застосування обмежень (див. Зауваження загального порядку №34 Комітету з прав людини: (2011)). Розпливчасті та надмірно широкі виправдання, такі як неконкретні посилення на «національну безпеку», «екстремізм» чи «тероризм», не підходять для визначення чітко сформульованих законів. Слово «необхідне» означає, що обмеження має бути чимось більшим, ніж «доцільне», «розумне» чи «бажане» (Справа «Санді Таймс» (The Sunday Times) проти Сполученого Королівства, ухвала суду від 26 квітня 1979 року, пункт 59). Крім того, має існувати

відповідний зв'язок між законною метою, яку переслідує держава, та діями держави щодо досягнення цієї законної мети. Іншими словами, дії повинні бути пропорційні інтересам, що захищаються. З цього випливає, що обмеження є найменш інтрузивним заходом у порівнянні з іншими заходами, за допомогою яких можна забезпечити досягнення бажаного результату. Держави користуються деякою свободою дій у виконанні своїх зобов'язань, прийнятих у межах міжнародного законодавства у сфері правами людини (свобода розсуду).

Свобода розсуду

Свобода розсуду є складною та важкою для розуміння доктриною. Для ознайомлення з докладним аналізом цієї доктрини та її значенням див: Council of Europe.

Більш того, навіть деякі права можуть перешкоджати здійсненню права на свободу слова або свободу вираження думок, такі як право на свободу від катувань та інших видів жорстокого, нелюдського або принижуючого гідність поводження, право на недоторканність приватного життя (докладно розглядається в модулі 10 серії модулів з кіберзлочинності: «Конфіденційність та захист даних»), право на свободу від дискримінації та право дітей на особливий захист.

Свобода вираження думок (або свобода слова)

- Стаття 19 Загальної декларації з прав людини 1948 року
- Стаття 10 Європейської конвенції з прав людини 1950 року
- Стаття 19 Міжнародного пакту про громадянські та політичні права 1966 року
- Стаття 13 Американської конвенції з прав людини 1969 року
- Стаття 9(2) Африканської хартії прав людини та народів 1981 року

Заборона на застосування тортур та інших видів жорстокого,

нелюдського та принижуючого гідність поводження та покарання

- Стаття 5 Загальної декларації з прав людини 1948 року
- Стаття 3 Європейської конвенції з прав людини 1950 року
- Стаття 7 Міжнародного пакту про громадянські та політичні права

1966 року

- Стаття 5(2) Американської конвенції з прав людини 1969 року
- Стаття 5 Африканської хартії прав людини та народів 1981 року

Право на недоторканність приватного життя

- Стаття 12 Загальної декларації з прав людини 1948 року
- Стаття 8 Європейської конвенції з прав людини 1950 року
- Стаття 17 Міжнародного пакту про громадянські та політичні права

1966 року

- Стаття 11 Американської конвенції з прав людини 1969 року

Право на свободу від дискримінації

- Статті 2 та 7 Загальної декларації прав людини 1948 року
- Стаття 14 Європейської конвенції з прав людини 1950 року
- Статті 2(1) та 26 Міжнародного пакту про громадянські та

політичні права 1966 року

- Стаття 2(2) Міжнародного пакту про економічні, соціальні та культурні права 1966 року

- Статті 1 та 24 Американської конвенції з прав людини 1969 року
- Статті 2 та 18(3) Африканської хартії прав людини та народів 1981

року

- Стаття 5 Конвенції Організації Об'єднаних Націй про права інвалідів 2006 року

Такі права на свободу від дискримінації та можливість здійснення цих прав будь-якою особою у прямій формі передбачені у Міжнародній

конвенції Організації Об'єднаних Націй про ліквідацію всіх форм расової дискримінації 1966 року та Декларацію Організації Об'єднаних Націй про ліквідацію всіх форм расової дискримінації 1963 року.

Право дітей на особливий захист

- Стаття 24 Міжнародного пакту про громадянські та політичні права 1966 року

- Стаття 10(3) Міжнародного пакту про економічні, соціальні та культурні права 1966 року

- Стаття 19 Американської конвенції з прав людини 1969 року

- Стаття 3 Конвенції Організації Об'єднаних Націй про права дитини 1989 року

Європейський суд з прав людини поширив сферу дії цього позитивного зобов'язання щодо захисту на вразливих осіб (а саме дітей) в мережі Інтернет, заявивши, що країни зобов'язані вживати заходів для захисту дітей від шкідливого впливу шляхом ухвалення відповідного законодавства (наприклад, див. *Mouvement raelien Suisse v. Switzerland*, 2012; *M.C. v. Bulgaria*, 2003; *Perrin v. United Kingdom*, 2003; *K.U. v. Finland*, 2008).

Рада з прав людини Організації Об'єднаних Націй неодноразово підтверджувала, що «ті ж права, які людина має в офлайновому середовищі, повинні також захищатися і в онлайновому середовищі, зокрема право на свободу вираження думок, яке здійснюється незалежно від державних кордонів та будь-якими засобами за власним вибору» (наприклад, A/HRC/RES/20/8; A/HRC/RES/38/7; див. також резолюцію Генеральної асамблеї A/RES/68/167, в якій міститься таке ж підтвердження права на недоторканність приватного життя). Свобода вираження поглядів розглядається як право, що сприяє здійсненню інших основних економічних, соціальних, культурних, громадянських та політичних прав,

включаючи право на свободу мирних зборів та свободу об'єднань, право на освіту та право на участь у культурному житті. Генеральна асамблея Організації Об'єднаних Націй також визнає, що «здійснення права на недоторканність особистого життя також має важливе значення для реалізації права вільно висловлювати свої думки та безперешкодно дотримуватись їх і є однією з основ демократичного суспільства» (резолюція Генеральної асамблеї A/RES/68 /167).

Свобода зборів та об'єднань

- Стаття 20 Загальної декларації з прав людини 1948 року
- Стаття 11 Європейської конвенції з прав людини 1950 року
- Статті 21 та 22 Міжнародного пакту про громадянські та політичні права 1966 року
- Стаття 15 Американської конвенції з прав людини 1969 року
- Статті 10(1) та 11 Африканської хартії прав людини та народів 1981 року

Право на освіту

- Стаття 26 Загальної Декларації прав людини 1948 року
- Стаття 2 Протоколу №1 до Європейської конвенції з прав людини 1950 року
- Стаття 13 Міжнародного пакту про економічні, соціальні та культурні права 1966 року
- Статті 23 та 28 Конвенції Організації Об'єднаних Націй про права дитини 1989 року
- Стаття 14 Хартія основних прав Європейського Союзу 2000 року

*Право на освіту також визнається у Конвенції Організації Об'єднаних Націй з питань освіти, науки та культури (ЮНЕСКО) про боротьбу з дискримінацією в галузі освіти 1960 року. Це право підтверджено у міжнародних договорах, що охоплюють права окремих

груп (жінок, дітей, інвалідів, біженців, мігрантів та корінних народів), таких як Конвенція Генеральної асамблеї Організації Об'єднаних Націй про ліквідацію всіх форм дискримінації щодо жінок 1979 року; Конвенція Організації Об'єднаних Націй про права дитини; Конвенція Організації Об'єднаних Націй про статус біженців 1951; Конвенція Організації Об'єднаних Націй про захист прав усіх трудящих-мігрантів та членів їх сімей 1990 року; Декларація Організації Об'єднаних Націй з прав корінних народів 1970 року.

Право на участь у культурному житті

- Стаття 27 Загальної декларації з прав людини 1948 року
- Стаття 15(1) (а) Міжнародного пакту про економічні, соціальні та культурні права 1966 року

Примітка: право на недоторканність приватного життя докладно розглядається в модулі 10 серії модулів з кіберзлочинності «Конфіденційність та захист даних».

Крім того, у 2016 році Рада з прав людини Організації Об'єднаних Націй ухвалила резолюцію, яка засуджує практику недопущення та/або порушення доступу до Інтернету (A/HRC/RES/32/13). Хоча загальний доступ до Інтернету не визнається одним з прав людини в міжнародному праві в галузі прав людини, існують зобов'язання держав щодо заохочення підключення до Інтернету, які можуть бути пов'язані з деякими правами людини, такими як право на свободу вираження поглядів (A/ HRC/17/27). Доступ до Інтернету є також необхідним для реалізації багатьох інших прав, включаючи право на свободу об'єднань, право на свободу зборів, право на освіту та охорону здоров'я, право на повну участь у соціальному, культурному та політичному житті, право на соціальний та економічний розвиток (A /HRC/17/27). Ці зобов'язання включають прийняття «ефективних і конкретних стратегій і заходів політики, розроблених на основі консультацій з представниками всіх верств суспільства, включаючи

приватний сектор, а також з відповідними державними відомствами, щоб дозволити всім на практиці активно і недорого користуватися Інтернетом» (A/HRC/17/27, параграф 66). Крім того, «слід застосовувати правозахисний підхід при забезпеченні та розширенні доступу до Інтернету, і ... держави мають докладати всіх зусиль для подолання численних форм цифрових розривів» (A/HRC/32/L.20, пункт 5). Зокрема, Комітет з прав людини Організації Об'єднаних Націй заявляє, що «Державам-учасницям слід враховувати масштаби змін в інформаційних та комунікаційних технологіях, таких як електронні системи розповсюдження інформації на базі Інтернету та мобільного зв'язку, які суттєво змінили методи спілкування у всьому світі. Сьогодні створено нову глобальну мережу для обміну ідеями та думками, яка не обов'язково спирається на традиційні засоби масової інформації. Державам-учасницям слід вжити всіх необхідних заходів для зміцнення незалежності цих нових ЗМІ та забезпечити доступ до них для населення» (Зауваження загального порядку №.34, пункт 15). Це зобов'язання закріплено у національному законодавстві деяких страх, таких як Греція, яка внесла такі поправки до своєї конституції: «кожен має право на участь в інформаційному суспільстві. Сприяння доступу до інформації в електронній формі, а також до її виробництва, обміну та поширення є обов'язком держави».

Важлива примітка: проблема нерівності ще більше ускладнюється внаслідок обмеження якості та стійкості доступу до Інтернету.

Крім того, доступ до онлайн-контенту може бути обмежений (і обмежується) для захисту прав інших осіб. На думку «Спеціального доповідача Організації Об'єднаних Націй з питання про заохочення та захист права на свободу думок та їх вільне вираження», певні «форми вираження думок... повинні бути заборонені відповідно до міжнародного права», включаючи «виступ на користь національної, расової чи релігійної. ненависті, що є підбурюванням до дискримінації, ворожнечі або насильства», і «пряме і публічне підбурювання до геноциду» (УНЦ

ООН, 2013, стор. 124). Така заборона також закріплена у статті 20 (2) Міжнародного пакту про громадянські та політичні права 1966 року, яка забороняє «у будь-який виступ на користь національної, расової чи релігійної ненависті, що є підбурюванням до дискримінації, ворожнечі чи насильства», та статті III(с) Конвенції про запобігання злочину геноциду та покарання за нього 1948 року, яка забороняє пряме та публічне підбурювання до вчинення геноциду. У «Рабатському плані дій щодо заборони пропаганди національної, расової чи релігійної ненависті, що є підбурюванням до дискримінації, ворожнечі чи насильства» (A/HRC/22/17/Add. 4) проводиться чітка різниця між різними типами висловлювань: «висловлювання, яке є кримінальним злочином; висловлювання, яке не є кримінальним, але може підлягати цивільному позову або адміністративним санкціям; висловлювання, яке не підлягає кримінальним, цивільним чи адміністративним санкціям, проте викликає занепокоєння з точки зору толерантності, коректності та поваги прав інших людей» (пункт 20).

Держави можуть обмежувати (і вже обмежили) ксенофобські та расистські висловлювання з метою збереження громадського порядку та захисту прав осіб, до яких звернено такі висловлювання. У Танзанії Закон про кіберзлочини 2015 року забороняє провадження, пропозицію, надання та розповсюдження расистських та ксенофобських матеріалів (стаття 17) та образи на ґрунті расизму та ксенофобії (стаття 18) (для ознайомлення з критичним оглядом Закону Танзанії про кіберзлочини його положень, які забороняють расистські та ксенофобські матеріали, див. звіт британської правозахисної організації «Article 19»). Європейський суд з прав людини (ЄСПЛ) ухвалив, що висловлювання, в яких заявляється, що всі мусульмани є терористами, і заперечується Голокост (Norwood v. the United Kingdom, 2003); Garaudy v. France, 2003) не підпадають під захист статті 10 Європейської конвенції з прав людини. У Сполученому Королівстві Великобританії Закон про расову та релігійну ненависть 2006

року передбачає кримінальну відповідальність за висловлювання, які розпалюють расову та/або релігійну ненависть.

Стаття 17 Європейської конвенції з прав людини (ЄКПЛ) забороняє зловживання правами. Згідно зі статтею 17 ЄКПЛ, «ніщо в цій Конвенції не може тлумачитися як таке, що будь-яка Держава, якась група осіб або якась особа має право займатися будь-якою діяльністю або вчиняти будь-які дії, спрямовані на скасування прав і свобод, визнаних у цій Конвенції, або на їхнє обмеження більшою мірою, ніж це передбачається у Конвенції».

Пропаганда ненависті спрямована на те, щоб очорнити цільову групу інших людей та розділити членів суспільства не тих, хто підтримує пропаганду ненависті і дотримується схожих з нею ідеологій (тобто на групу «ми»), і тих, хто входить до цільової групи інших людей, толерантних до цієї групи, і тих, хто так чи інакше підтримує цільову групу. Мета цієї пропаганди полягає в відокремленні, а часом і дегуманізації цільової групи шляхом прирівнюючи їх до комах, тварин, хвороб і демонів. Пропаганда такого типу, поряд із підбурюванням до насильства та геноциду, спостерігалася, наприклад, під час геноциду в Руанді.

Під час геноциду в Руанді тутсі були прозвані тарганями (іньєнзі), а радіостанція «Вільне радіо та телебачення тисячі пагорбів» (RTLM) закликала до знищення «тарганів тутсі» (Gourevitch, 1998; Bhavnani, 2006). Журналістів радіо (і друкованих засобів масової інформації) у Руанді було притягнуто до кримінальної відповідальності та засуджено за поширення ненависницьких висловлювань та пропаганду ненависті, а також за підбурювання до насильства та геноциду. Наприклад, Жан-Боско Бараягвіза та Фердинанд Нахімана, засновники радіостанції «Вільне радіо та телебачення тисячі пагорбів» (RTLM), і Хассан Нгезе, засновник і редактор місцевої газети (Kanguara), були визнані винними, зокрема, у

прямому та публічному підбурюванні до геноциду (The Prosecutor v. Ferdinand Nahimana, Jean-Bosco Barayagwiza, Hassan Ngeze, 2003; Baisley, 2014, 39). Під час винесення вироку Фердинанду Нахімані у Міжнародному кримінальному трибуналі по Руанді суддя заявив: «Ви були повною мірою обізнані про силу слова, і ви використовували радіо – засіб комунікації з найширшим охопленням населення – для поширення ненависті та насильства. Без вогнепальної зброї, мачете або іншої фізичної зброї ви стали причиною загибелі тисяч ні в чому не винних цивільних осіб» (Організація Об'єднаних Націй, Міжнародний залишковий механізм для кримінальних трибуналів 2003; The Prosecutor v. Ferdinand Nahimana, Jean-Bosco Baraya Hassan Ngeze, 2003).

Крім радіо, для ненависницьких висловлювань та пропаганди ненависті, а також для підбурювання насильства та геноциду можуть використовуватися (і використовуються) онлайн-платформи. Розглянемо роль однієї із соціальних медіаплатформ у вчиненні передбачуваних актів геноциду у М'янмі. Як повідомляли засоби масової інформації, «понад 650.000 мусульман-рохінджа... тікали зі штату Ракхайн у М'янмі в Бангладеш, після того, як напади повстанців спричинили жорстокі заходи щодо забезпечення безпеки... у серпні 2017 року. Більшість постраждалих надали жахливі докази вбивств та зґвалтувань з боку сил безпеки М'янми» (Miles, 2018). За твердженням представника Незалежної міжнародної місії Організації Об'єднаних Націй зі встановлення фактів у М'янмі (Марзукі Дарусман), «Facebook» «відіграв визначальну роль» у М'янмі, «значною мірою сприявши підвищенню рівня люті, розбратів та конфліктів [з мусульманами-рохінджа]» у «М'янмі шляхом поширення пропаганди насильства». Зокрема, у заяві місії щодо встановлення фактів йшлося, що члени місії не мають жодних сумнівів у тому, що широка поширеність ненависницьких висловлювань у М'янмі значною мірою сприяла зростанню напруженості та створенню атмосфери, в якій окремі особи та групи людей могли стати більш сприйнятливими до підбурювання та

закликів до насильства. Це також стосується ненависницьких висловлювань у «Facebook». Ступінь, в якій розповсюдження повідомлень і чуток у «Facebook» посилює дискримінацію та насильство в М'янмі, має бути незалежно і ретельно досліджено, щоб можна було винести відповідні уроки та запобігти аналогічним сценаріям. Так само необхідно оцінити вплив недавніх заходів, вжитих «Facebook» для запобігання випадкам зловживань своєю платформою та виправлення положення (A/HRC/39/CRP.2, пункт 1354).

Ще один приклад пов'язаний із використанням іншої соціальної медіаплатформи, «YouTube», для поширення ненависницьких висловлювань та підбурювання до насильства. Фуад Белкасем, який був лідером та представником (колишньої) організації Sharia4Belgium (Шаріат для Бельгії), виклав відеоматеріали на YouTube, призначені для поширення ненависті і, зрештою, підбурювання до насильства; він називав немусульманське населення, зокрема тваринами і закликав «глядачів витіснити немусульманське населення, «дати йому урок» і... боротися з ним» (Belkacem v. Belgium, 2017; Voorhoof, 2017).

Права інтелектуальної власності (ІВ) можуть також бути виправданням для обмеження права на свободу вираження та доступу до інформації. Наприклад, при дотриманні певних вимог блокування веб-сайтів, які незаконно надають доступ до контенту, захищеного правом інтелектуальної власності, може бути виправданим. Європейський суд із прав людини ухвалив і визнав, що права авторів інтелектуальної власності повинні захищатися (Neij and Sunde Kolmisoppi v. Sweden, 2012). Проте, оскільки заходи блокування є дуже делікатними заходами, які можуть зачіпати права багатьох людей (зокрема, їхнє право на поширення, пошук та отримання інформації), слід приділяти більше уваги забезпеченню балансу між правами людини та вимогами щодо законних заходів блокування (див., наприклад, справи, що розглядалися в Суді Європейського союзу UPC Telekabel Wien GmbH v Constantin Film Verleih

GmbH та Wega Filmproduktionsgesellschaft mbH, 2014; Cengiz and Others v. Turkey, 2015; 19 Міжнародного пакту про громадянські та політичні права).

Доступ до Інтернету також блокувався через політичні хвилювання. Зокрема, уряди країн закривали громадянам доступ до Інтернету та соціальних мереж (повністю або частково) під час акцій протестів та інших подій національного значення (наприклад, у Камеруні, Єгипті та Уганді). Доступ блокувався для окремих осіб та/або окремого контенту, а в деяких випадках доступ до Інтернету блокувався на певний період для всього населення. В Індії в 2017 році доступ до 22 соціальних мереж (наприклад, Twitter, Facebook, Snapchat та YouTube) та додатків для обміну повідомленнями (наприклад, WhatsApp, Skype та WeChat) у Кашмирській долині було заблоковано через масові хвилювання. Можна навести ще багато випадків, коли масові заворушення призводили до блокування Інтернету та роботи мобільного та стаціонарного зв'язку в цьому та інших регіонах Індії.

Попередня цензура з боку держави (тобто обмеження щодо контенту до того, як він буде доступний для публічного чи приватного споживання) і практика блокування онлайн-контенту вступають у пряму суперечність із правом окремих осіб на доступ до інформації. У справі Ahmet Yildirim v. Turkey (2010) на приватному веб-сайті, створеному через хостинг «Сайти Google», публікувалися, серед іншого, праці його творця та власника. Його сайт був вважаний образою пам'яті та спадщини Мустафи Кемаля Ататюрка, що заборонено відповідно до турецького Закону №.5816 зокрема, який передбачає покарання за злочини проти Ататюрка, та відповідно до статті 301 Кримінального кодексу Туреччини загалом, яка забороняє образи Туреччини та її інститутів. У відповідь на розміщення контенту на його вебсайті, замість блокування доступу до цього сайту, турецька влада заблокувала всі сайти. Дії Туреччини вважаються порушенням вимог статті 10 Європейської конвенції з прав людини. У той

час як тимчасові або часткові заходи припинення або блокування можуть бути виправдані в особливих обставинах, призупинення роботи Інтернет-сервісів та блокування доступу до Інтернету для всього населення та його окремих груп не можуть бути виправдані з юридичної точки зору. У доповіді Спеціального доповідача Організації Об'єднаних Націй з питання про заохочення та захист права на свободу думок та їх вільне вираження йдеться, що: «блокування Інтернет-платформ та відключення систем телекомунікаційної інфраструктури є стійкою загрозою; навіть якщо підставою для таких заходів є інтереси державної безпеки або підтримки громадського порядку, їх застосування зазвичай призводить до блокування повідомлень мільйонів людей» (A/71/373 пункт 22). У доповіді також згадується, що у 2015 році «Організація Об'єднаних Націй та регіональні експерти у сфері свободи вираження поглядів у спільній заяві засудили незаконні блокування мережі Інтернет» (A/71/373 пункт 22).

Рада Організації Об'єднаних Націй з прав людини у своїй резолюції 32/13 «беззастережно засуджує також заходи щодо навмисного недопущення або порушення доступу до інформації або її поширення в режимі он-лайн на порушення норм міжнародного права прав людини і закликає всі держави утримуватися від таких заходів і припинити їх використання» (A/HRC/RES/32/13). Як справедливо зазначає Комітет з прав людини Організації Об'єднаних Націй (Зауваження загального порядку №.34, пункт 43, CCPR/C/GC/34), «будь-які обмеження на роботу вебсайтів, блогів та інших подібних систем поширення електронної та іншої інформації, заснованих на Інтернет-технологіях, у тому числі систем, що забезпечують роботу подібних засобів комунікації, таких як системи доступу до мережі Інтернет або пошукові системи, допустимі тією мірою, якою вони сумісні з пунктом 3 [статті 19 Міжнародного пакту про цивільні та політичні права] . Допустимі обмеження повинні ґрунтуватися головним чином на змісті конкретних матеріалів; загальні заборони на функціонування певних сайтів та систем несумісні з пунктом 3 [статті 19

Міжнародного пакту про громадянські та політичні права 1966 року]. Будь-які заходи блокування повинні бути вузькоспрямованими та індивідуальними, щоб торкатися лише тих веб-сторінок, які містять незаконний контент. Призупинення роботи Інтернет-сервісів та блокування доступу до Інтернету для всього населення та його окремих груп не може бути виправдано з юридичної точки зору».

Приклад обмеження права на свободу слова

Уряд країни К надсилає засобам масової інформації повідомлення, в якому він забороняє їм популяризувати «західний спосіб життя» та висміювати цінності країни К. Державний орган країни К закриває декілька онлайн-каналів новин за поширення інформації, яку уряд вважає невірною та/або незаконною, та /або за нездатність видаляти на своїх сайтах коментарі, що підтримують висловлювання, які уряд вважає недозволеними. Країна К вимагає, щоб приватні компанії у випереджувальному порядку відстежували свої сайти та видаляли цей некоректний та/або незаконний контент.

Висновок

Було укладено кілька міжнародних договорів, пов'язаних із кіберзлочинністю. Загалом існуючі багатосторонні та регіональні правові документи та національні закони відрізняються за своїм тематичним змістом та ступенем охоплення таких аспектів, як криміналізація, слідчі заходи та повноваження, збирання та використання цифрових доказів, регулювання та ризик, юрисдикція та міжнародне співробітництво. Ці договори також різняться за своїм географічним охопленням (тобто є регіональними або багатосторонніми) та сферою застосування. Такі відмінності створюють перешкоди для ефективної ідентифікації, розслідування та кримінального переслідування кіберзлочинців та запобігання кіберзлочинності.

Необхідні гарантії для того, щоб закони, що обмежують контент і доступ до Інтернету, застосовувалися в законних цілях і відповідали принципу верховенства закону та стандартам у галузі прав людини. Крім того, закони повинні містити гранично чіткі положення, які не допускають їх використання з метою заборони доступу до контенту з порушенням законодавства у галузі прав людини. Існує небезпека «розмивання (відхилення від основного) мандата» або «розмивання функцій» (ці терміни використовуються для опису випадків поширення законів та/або інших заходів на області, що знаходяться за межами їхньої початкової сфери дії), коли закони та слідчі повноваження, спочатку націлені на один вид кіберзлочинності, згодом націлюються інші, менш тяжкі види кіберзлочинів. Більше того, складнощі, пов'язані зі сферою дії та застосування законів про кіберзлочинність, виникають у тих випадках, «коли Інтернет-контент, що генерується та прийнятий в одній країні, стає доступним у третій країні», де такий контент вважається незаконним (УНЦ ООН, 2013, Стор. 128).

Питання для самоперевірки

1. Яким правам людини суперечить розділ 112 Кримінального кодексу Таїланду?
2. Чи є існуючі обмеження прав людини (про які згадано в попередньому питанні) відповідними законній меті, чинному законодавству, і чи є необхідними та пропорційними вчиненому злочину?

ЗМІСТОВИЙ МОДУЛЬ 2. Цифрові докази.

Стандарти та методи цифрової криміналістики.

Лекція 4. Основи цифрової криміналістики.

- 4.1. Цифрові докази.
- 4.2. Стандарти та передові практичні методи в області цифрової криміналістики.
- 4.3. Криміналістична експертиза Інтернету речей
- 4.4. Антикриміналістика

4.1. Цифрові докази

Цифрова криміналістика «ґрунтується на принципах криміналістики, таких як «принцип обміну Едмона Локара», який стверджує, що «коли об'єкти та поверхні вступають у контакт один з одним, відбувається перехресне перенесення матеріалів».

У контексті цифрової криміналістики люди після використання інформаційно-комунікаційних технологій (ІКТ) залишають цифрові сліди. Зокрема, особа, яка використовує ІКТ, може залишити *цифрові відбитки*, тобто дані, залишені користувачами ІКТ, які можуть розкрити відомості про них, включаючи інформацію про вік, статеву, расову та етнічну приналежність, громадянство, сексуальну орієнтацію, думки, уподобання, звички, хобі, історію хвороби та проблеми здоров'я, психологічні розлади, статус зайнятості, приналежності до будь-якої спільноти, відносин, геолокації, порядку дня та іншої активності. Такі цифрові відбитки можуть бути активними або пасивними.

Активний цифровий відбиток створюється даними, що надаються користувачем, такими як персональні дані, відео, зображення та коментарі, що розміщуються у додатках, на вебсайтах, електронних дошках оголошень, соціальних мережах та інших онлайн-форумах.

Пасивний цифровий відбиток – це дані, які ненавмисно залишають люди, які користуються Інтернетом та цифровими технологіями (наприклад, історія переглядів у браузері).

Дані, які є частиною активних і пасивних цифрових відбитків, можуть використовуватися як доказ скоєння злочину, у тому числі кіберзлочини (тобто *цифрові докази*). Такі дані можуть також використовуватись для доказу або спростування твердження про факт; підтвердження або спростування показань потерпілого, свідка та підозрюваного; та/або визначення причетності чи непричетності підозрюваного до скоєння злочину.

Дані зберігаються в цифрових пристроях (наприклад, комп'ютерах, смартфонах, планшетах, телефонах, принтерах, «розумних» телевізорах (Smart TV) та будь-яких інших пристроях, що мають цифрову пам'ять), зовнішніх накопичувачах (наприклад, зовнішніх жорстких дисках та USB-флеш-накопичувачах), мережевих компонентах та пристроях (наприклад, маршрутизаторах), серверах та хмарному сховищі даних (де дані зберігаються «у кількох центрах даних у різних географічних точках»; УНЦ ООН, 2013, стор. xxvi). Видобувані дані можуть являти собою дані, що відносяться до контенту (тобто слова в письмових повідомленнях або вимовлені слова в аудіофайлах; наприклад, відео, текст електронних листів, текстові повідомлення, миттєві повідомлення та зміст соціальних мереж), та дані, що не стосуються контенту, або мета-данні (тобто дані про зміст; наприклад, особистість і місцезнаходження користувачів та дані про операції, такі як інформація про відправників та одержувачів телекомунікаційних та електронних повідомлень).

Дані, отримані в режимі онлайн та/або вилучені з цифрових пристроїв, можуть містити велику кількість інформації про користувачів та події. Наприклад, ігрові приставки, які працюють як персональні комп'ютери, зберігають особисту інформацію про користувачів пристроїв (наприклад, імена та адреси електронної пошти), фінансову інформацію

(наприклад, дані кредитної картки), інформацію про історію відвідувань Інтернету (наприклад, про відвідувані веб-сайти), зображення, відео та інші дані. Дані, витягнуті з ігрових приставок, використовувалися при розслідуванні справ, пов'язаних із сексуальною експлуатацією дітей та розміщенням в Інтернеті матеріалів зі сценами сексуального насильства над дітьми. Ще одним цифровим пристроєм, що накопичує значний обсяг даних про його користувачів, є Amazon Echo (з голосовим помічником Alexa). Дані, що накопичуються цим пристроєм, можуть містити цінні відомості про користувачів/власників, такі як інформація про їх інтереси, переваги, запити, покупки та інші види активності, а також про їх місцезнаходження (щоб, наприклад, визначити, чи знаходяться вони вдома чи ні, шляхом перегляду міток часу та аудіозапису взаємодій з мовним помічником Alexa). Дані, витягнуті з Amazon Echo, використовувалися в Сполучених Штатах Америки при розслідуванні справи про вбивство. Хоча звинувачення проти підозрюваного було зрештою знято, ця справа наочно продемонструвала, що дані, які збираються з використанням нових цифрових технологій, неминуче будуть представлені в суді як доказ.

Дані можуть видобуватись та використовуватись з метою отримання оперативно-розшукових відомостей та/або можуть подаватися в суді як цифрові докази. У разі цифрові докази можуть бути *прямими доказами* шляхом «встановлення факту» чи *опосередкованими доказами* шляхом «виведення висновку про істинність цього факта». Розглянемо наступний гіпотетичний випадок: матеріал расистського змісту було опубліковано від імені облікового запису Twitter (Обліковий запис А). *Прямим доказом* є той факт, що Обліковий запис А був використаний для публікації расистського матеріалу. *Непрямим доказом* є те, що матеріал був розміщений власником облікового запису. Для того щоб довести, що власник облікового запису опублікував цей матеріал, необхідно отримати додаткові докази, що підкріплюють цю версію.

Перш ніж цифрові докази можуть бути представлені в суді як прямі або непрямі докази, їх необхідно автентифікувати (тобто необхідно показати, що докази відповідають передбачуваній меті). Для наочної демонстрації практики аутентифікації розглянемо такі загальні категорії цифрових доказів:

контент, що генерується однією чи кількома особами (наприклад, текст, електронний лист або миттєве повідомлення та документи текстового редактора, такого як Microsoft Word);

контент, що генерується комп'ютером або цифровим пристроєм без участі користувача (наприклад, журнали реєстрації даних), який вважається однією з форм *речового доказу*, наприклад, у Сполученому Королівстві;

контент, що генерується одночасно користувачем та пристроєм (наприклад, динамічні таблиці в таких програмах, як Microsoft Excel, які включають дані, що вводяться користувачем, і розрахунки, що здійснюються програмою).

Контент, що генерується користувачем, може вважатися допустимим доказом, якщо він є достовірним та правдоподібним (тобто можна встановити його належність до будь-якої особи). Контент, що генерується пристроєм, може вважатися допустимим доказом, якщо можна довести, що пристрій функціонувало належним чином у момент генерування даних, і якщо можна показати, що в момент генерування даних діяли механізми забезпечення захисту для запобігання зміні даних. У випадках, коли контент генерується одночасно пристроєм та користувачем, необхідно встановити достовірність та правдоподібність кожного з них.

У порівнянні з *традиційними доказами* (наприклад, паперовими документами, зброєю, контрольованими речовинами і т.д.), цифрові докази створюють унікальні складності при аутентифікації через обсяг доступних даних, їх швидкості (тобто швидкості, з якої вони створюються і передаються), нестійкості (тобто. вони можуть швидко зникнути під час

перезапису чи видалення) та вразливості (тобто їх легко можна обробити, змінити чи пошкодити). У той час як одні країни впровадили норми доказового права, що включають вимоги щодо аутентифікації, які конкретно ставляться до цифрових доказів, інші країни для *аутентифікації* традиційних доказів і цифрових доказів використовують схожі вимоги. У Франції, наприклад, як паперові, і електронні документи повинні аутентифікуватися шляхом перевірки особистості творця документів і цілісності документів. Перевірка цілісності документів означає як перевірку їх точності, а й можливості зберігати точність (тобто. *несуперечність*) з часом. Більше того, для того, щоб уніфікувати режими поводження з нецифровими та цифровими доказами, Сінгапур вніс поправки до норм доказового права, ухваливши Закон про докази (з поправками) 2012 року, щоб забезпечити однакову практику автентифікації для нецифрових та цифрових доказів.

На додаток до визначення справжності цифрових доказів, багато країн також проводять оцінку того, чи є отриманий доказ *найкращим доказом* (тобто справжнім доказом або точною копією справжнього доказу), та/або може бути допустимим відповідно до винятків вимог дотримання заборони свідчення з *чужих слів* (тобто заяв, зроблених поза судом). Як приклад можна навести Танзанію (Закон про докази 1967 року, Закон про письмові закони (з різними поправками) 2007 року та Закон про електронні операції 2015 року); Беліз (Закон про електронні докази 2011 року); Індонезію (Закон №.11 від 2008 року про електронну інформацію та операції та Постанову уряду №.82 від 2012 року); Малайзію (Закон про докази 1950); Індію (Закон про інформаційні технології 2000 року); Сінгапур (Закон про докази (з поправками) 2012 року) та інші країни.

Крім того, оцінка справжності цифрових доказів також передбачає вивчення процесів, методів та інструментів, використаних для збору, отримання, збереження та аналізу цифрових доказів, щоб переконатися, що

дані не були змінені будь-яким чином. Ці процеси, методи та засоби розглядаються у наступних розділах даного модуля.

Процес цифрової судової експертизи включає: пошук, отримання, збереження та зберігання цифрових доказів; опис, пояснення цифрових доказів та встановлення їх походження та значущості; аналіз доказів та їх переконливості, достовірності та відношення до справи; та подання доказів, що мають відношення до справи.

Було розроблено та прийнято різні методології цифрової криміналістики. У 2001 році «Digital Forensic Research Workshop», «некомерційна добровільна організація, що спеціалізується на фінансуванні діяльності технічних робочих груп, проведенні щорічних конференцій та вирішенні комплексу завдань з метою надання допомоги у визначенні напрямку досліджень та розробок», розробила модель, засновану на протоколі Федерального бюро розслідувань Сполучених Штатів Америки для проведення обшуку на фізичному місці злочину, який включає сім етапів: ідентифікація, збереження, збір, дослідження, аналіз, подання доказів і прийняття рішення.

У 2002 році була запропонована ще одна модель цифрової криміналістики, яка була заснована на моделі «Digital Forensic Research Workshop» 2001 року та протокол Федерального бюро розслідувань Сполучених Штатів Америки для проведення обшуку на місці злочину (для фізичних місць злочину). Ця модель («Абстрактна модель цифрової криміналістики») складалася з дев'яти етапів:

Ідентифікація (тобто «розпізнання інциденту за ознаками та визначення його типу»);

Підготовка (тобто «підготовка коштів, методів, ордерів на обшук та моніторинг процесу отримання дозволів та підтримки керівництва»);

Стратегія підходу (тобто. «розробка процедури, яка буде використовуватися з метою збору максимального обсягу бездоганих доказів при мінімізації впливу на потерпілого»);

Збереження (тобто «ізолювання, захист та збереження стану речових та цифрових доказів»);

Збір (тобто «складання протоколу огляду фізичного місця злочину та дублювання цифрових доказів з використанням стандартизованих та затверджених процедур»);

Дослідження (тобто «поглиблений систематичний пошук доказів, які стосуються гаданого злочину»);

Аналіз (тобто «визначення значущості, відновлення фрагментів даних та виведення висновку на основі виявлених доказів»);

Подання (тобто «короткий виклад та пояснення висновків»); і

Повернення доказів (тобто повернення фізичного та цифрового майна законному власнику»).

У 2003 році було запропоновано Інтегровану модель цифрового розслідування, яка є більш цілісним підходом до розслідування, що складається з п'яти основних етапів, кожен з яких, у свою чергу, складається з окремих фаз:

готовність (тобто оцінка можливості оперативних служб та інфраструктури надавати підтримку проведенню розслідування);

розгортання (тобто інцидент виявлено, відповідному персоналу повідомлено, та отримано дозвіл на проведення розслідування, наприклад, судовий ордер на провадження розслідування правоохоронними органами, дозвіл керівника для проведення приватних розслідувань);

розслідування на фізичному місці злочину (тобто огороження місця злочину, ідентифікація речових доказів, що належать до справи, документування місця злочину, збір речових доказів на місці злочину, дослідження цих доказів, реконструкція подій на місці злочину та подання результатів у суді);

цифрове розслідування на місці злочину (тобто збір та ідентифікація цифрових доказів, що мають відношення до справи, документування

доказів, вилучення та аналіз доказів, реконструкція подій та подання результатів у суді);

розгляд (тобто після завершення розслідування проводиться оцінка з метою аналізу вилучених уроків).

У 2006 році Національний інститут стандартів і технологій США у своєму Посібнику з інтеграції криміналістичних методів у плани реагування на інциденти (Guide to Integrating Forensic Techniques into Incident Response) запропонував модель цифрової криміналістики, що складається з чотирьох етапів:

етап *збору* доказів, який включає ідентифікацію доказів на місці злочину, маркування, документування і, нарешті, збирання доказів;

етап *дослідження*, на якому визначаються відповідні криміналістичні засоби та методи, які будуть використовуватися для отримання відповідних цифрових доказів та збереження їх цілісності;

етап *аналізу*, у якому вилучені докази оцінюються визначення їх практичної придатності і придатності до справи;

етап *звітності*, який включає опис дій, виконаних в процесі цифрової криміналістики, і подання результатів.

Ще одну модель розслідування було запропоновано Національним інститутом правосуддя (NIJ) Міністерства юстиції США у 2001 році та переглянуто у 2008 році. Зокрема, у посібнику NIJ «Розслідування на електронному місці скоєння злочину: керівництво служб швидкого реагування» (Electronic Crime Scene Investigation: A Guide for First Responders) основну увагу приділено діям на фізичному місці злочину, таким як огороження та оцінка місця злочину (наприклад, для визначення пристроїв, що мають відношення до справи з потенційними цифровими доказами), документування місця злочину, вилучення відповідних пристроїв, упаковка, транспортування та, нарешті, забезпечення безпеки цих пристроїв.

Вищезгадані моделі засновані на припущеннях про те, що при розслідуванні кожного злочину та кіберзлочину всі етапи мають бути пройдені в повному обсязі. Однак на практиці це відбувається не завжди. Оскільки обсяги даних і кількість цифрових пристроїв, що накопичують, зберігають і передають дані, зростають у геометричній прогресії, що веде до збільшення числа справ, пов'язаних з цифровими пристроями того чи іншого типу, все частіше визнається практично недоцільним проводити досконалі перевірки кожного цифрового пристрою.

Як зазначили Кейсі, Ферраро та Нгуєн, «небагато лабораторій цифрової криміналістики все ще можуть дозволити собі створювати дублікат кожного носія інформації та проводити поглиблену судову експертизу всіх даних на цих носіях. Не має особливого сенсу чекати завершення аналізу кожного окремого носія інформації, якщо лише деякі з них дозволять отримати дані, мають доказову цінність».

У зв'язку з цим були розроблені моделі процесів цифрової криміналістики, що враховують цю проблему. Наприклад, у публікації Rogers (2006) було запропоновано модель процесу кіберкриміналістичного сортування даних на місцях (CFFTPM), засновану на проведенні цифрової судової експертизи «на місці» з метою «забезпечення ідентифікації, аналізу та інтерпретації цифрових доказів у короткі терміни без необхідності транспортування систем(и)/носіїв інформації до лабораторії для поглибленого дослідження чи створення повного образу судово-експертного аналізу». На основі цієї моделі Кейсі, Ферраро та Нгуєн запропонували «три рівні судової експертизи», які можна використовувати на місцях або в лабораторії.

Судово-експертний огляд на основі обстеження/сортування. Такий огляд проводиться з метою швидкого вивчення потенційних джерел доказів та визначення пріоритетних джерел для подальшого дослідження на основі значущості доказів, які вони можуть містити, та мінливості цих доказів.

Попередня судова експертиза. Для прискорення процесу цифрової судової експертизи проводиться *попередня судова експертиза* джерел, вибраних на етапі *судово-експертного огляду на основі обстеження/сортуння*, щоб виявити інформацію, яка може бути використана в розслідуванні для отримання прямих, непрямих або інших підкріплювальних доказів передбаченого злочину. Нездатність виявити артефакти для судово-експертного аналізу (тобто даних, які можуть мати значення для цифрової судової експертизи) під час цього огляду, що може статися внаслідок упущення їх на увазі, не означає автоматично, що поглиблена судова експертиза проводитися не буде (Це залежить від конкретної справи та від політики та процедур осіб, які проводять експертизу).

Поглиблена судова експертиза. Досліджуються всі джерела доказів. Експертиза такого типу найчастіше проводиться у випадках, «коли є підозра на знищення доказів, коли виникають додаткові питання, і коли справа наближається до судового розгляду».

Наразі тривають дебати щодо життєздатності та актуальності кожної моделі та її компонентів. Реальність така, що кожна країна дотримується своїх власних стандартів, протоколів та процедур у галузі цифрової криміналістики. Однак відмінності в цих процесах є перешкодою для здійснення міжнародного співробітництва у проведенні розслідувань правоохоронними органами.

Стандарти та передові практичні методи в галузі цифрової криміналістики.

Міжнародна організація зі стандартизації (International Standardization Organization, ISO), міжнародна неурядова організація та Міжнародна електротехнічна комісія (International Electrotechnical Commission, IEC), міжнародна некомерційна організація розробляють та публікують міжнародні стандарти для уніфікації практики, що використовується в різних країнах. У 2012 році Міжнародна організація зі

стандартизації та Міжнародна електротехнічна комісія опублікували міжнародні стандарти, що стосуються поводження з цифровими доказами (ISO/IEC 27037 Посібник з ідентифікації, збирання, отримання та збереження свідoctв, представлених у цифровій формі. Цей посібник охоплює лише початковий процес поводження з цифровими доказами. Пропонуються наступні чотири етапи поводження з цифровими доказами:

Ідентифікація. Цей етап включає пошук і розпізнавання відповідних доказів, а також їх документування. На цьому етапі пріоритетні завдання збору доказів визначаються на основі цінності та мінливості доказів.

Збір. Цей етап передбачає збирання всіх цифрових пристроїв, які можуть містити дані, що мають доказову цінність. Ці пристрої потім транспортуються в лабораторію судової експертизи або іншу установу для збирання та аналізу цифрових доказів. Цей процес називається *збором даних у статичному режимі*. Однак бувають випадки, коли збирання даних у статичному режимі є практично нездійсненним. У таких ситуаціях здійснюється *збір даних у реальному часі*. Розглянемо, наприклад, системи критично важливих об'єктів інфраструктури (наприклад, системи керування виробничими процесами). Ці системи не можуть бути відключені від живлення, оскільки вони надають критично важливі послуги. Тому в цих випадках здійснюється збір даних у реальному часі, коли мінливі та незмінні дані вилучаються із систем, що працюють у реальному часі. Однак такий збір даних у реальному часі може заважати нормальному функціонуванню систем управління виробничими процесами (наприклад, уповільнювати їхню роботу).

Примітка

Перш ніж приступити до збору даних у реальному часі, слід визначити пріоритети збору даних з точки зору їхньої доступності, а також їхньої цінності та мінливості.

Отримання. Цифрові докази необхідно отримувати без шкоди цілісності даних. Національна рада начальників поліції Сполученого

Королівства (The National Council of Police Chiefs, NCPC), раніше відома як Асоціація керівників поліцейських служб Сполученого Королівства, надає цій вимозі велике значення і виділяє її як важливий принцип у практиці цифрової криміналістики (принцип №1: «Жодні дії, що вживаються правоохоронцями особами, які працюють у цих органах, або їх представниками, не повинні призводити до зміни даних, які згодом можуть використовуватися в суді» (UK Association of Chief Police Officers, 2012, р. 6). Таке отримання даних без їх зміни здійснюється шляхом створення копії вмісту цифрового пристрою (процес, відомий як *створення неспотвореного образу*) з використанням пристрою (*блокувальника запису*), який призначений для запобігання зміні даних у процесі копіювання. Для того щоб визначити, чи дублікат є точною копією оригіналу, значення хеш-функції розраховується з використанням математичних обчислень; тут для отримання значення хеш-функції використовується криптографічна хеш-функція. Якщо значення хеш-функції для оригіналу та копії збігаються, то вміст копії є таким самим, як і в оригіналі. Визнаючи можливість існування певних «обставин, у яких будь-яка особа вважає за необхідне отримати доступ до вихідним даним, тобто. здійснити збір даних у реальному часі», Національна рада начальників поліції Сполученого Королівства зазначає, що «особа, яка отримує доступ до цих даних, має бути компетентною для таких дій і мати можливість подати докази, що пояснюють доцільність своїх дій та їх наслідки» (Принцип №2, UK Association of Chief Police Officers, 2012, р. 6).

Збереження. Цілісність цифрових пристроїв та цифрових доказів може бути забезпечена з використанням *системи охорони доказів*, яка визначається як «процес, за допомогою якого слідчі забезпечують охорону місця злочину (або події) та збереження доказів протягом усього періоду провадження у справі. У журналі реєстрації записують інформацію про те, хто здійснював збір доказів, де і яким чином вони були зібрані, які особи отримали ці докази, і коли вони отримали». Ретельне документування

процесу цифрової судової експертизи кожному етапі має значення для забезпечення допустимості доказів у суді. Інші етапи процесу цифрової судової експертизи (аналіз та звітність) не включені до керівництва ISO/IEC 27037. Етап *аналізу* (або дослідження) вимагає використання належних інструментів та методів цифрової криміналістики для виявлення цифрових даних. На ринку є велика кількість інструментів різної якості для проведення цифрової судової експертизи. Приклади інструментів для цифрової криміналістичної експертизи включають програми EnCase, FTK, і X-Ways Forensics. Вибір типу інструменту залежить від типу цифрової судової експертизи (наприклад, для криміналістичної експертизи мобільних пристроїв та хмарних сервісів на мобільних пристроях можна використовувати програму Oxygen Forensics Suite; для мережевої криміналістики, яка передбачає «використання науково-обґрунтованих методів розслідування [злочинів, скоєних щодо та з використанням] комп'ютерних мереж», як інструмент можна використовувати програму Wireshark). Існуючі інструменти цифрової криміналістики (наприклад, EnCase, FTK та NUIX) призначені для роботи з традиційними обчислювальними пристроями. Спеціалізовані інструменти цифрової криміналістики необхідні, наприклад, для експертизи мереж, інтерфейсів та операційних систем критично важливих об'єктів інфраструктури.

Національний інститут стандартів та технологій США має доступну для пошуку базу даних інструментів цифрової криміналістики, яка містить інформацію про інструменти з різними функціями (наприклад, інструменти для проведення криміналістичної експертизи баз даних, хмарних сховищ, безпілотних літальних апаратів, транспортних засобів тощо). Національні правоохоронні органи різних країн мають різні переваги щодо використання інструментів для цифрової криміналістичної експертизи.

4.2. Криміналістична експертиза «розумних» транспортних засобів

Криміналістична експертиза «розумних» транспортних засобів є маловивченою, але важливою областю цифрової криміналістики (Parkinson and McKay, 2016). Масове використання інтелектуальних транспортних засобів з функціями виходу в Інтернет (і розробка автономних транспортних засобів) надали додаткового імпульсу зусиллям щодо створення процедур, стандартів та інструментів проведення криміналістичної експертизи інтелектуальних транспортних засобів, які могли б забезпечити можливість проведення надійної з точки зору криміналістики цифрової експертизи таких коштів. Ці транспортні засоби можуть забезпечити отримання великої кількості інформації (наприклад, про маршрути поїздок і часто відвідувані місця, домашні та робочі адреси, набрані номери телефонів, прийняті дзвінки тощо), яка може використовуватися при розслідуванні злочинів, скоєних щодо інтелектуальних або автономних транспортних засобів (наприклад, злому), або інших злочинів, коли інформація, отримана з цих транспортних засобів, може бути використана як доказ скоєння злочину.

Використовувані інструменти мають бути *надійними з погляду криміналістики*. При цьому процес «збору та подальшого аналізу... [цифрових] даних» за допомогою цих інструментів повинен бути в змозі зберегти «дані в тому стані, в якому вони були вперше виявлені», і «в жодному разі не зменшувати доказову цінність електронних даних через технічних чи процедурних помилок чи помилок у інтерпретації». Простіше кажучи, отримані дані не повинні бути якимось чином змінені, тобто їхня цілісність повинна бути збережена. У рамках Програми тестування інструментів комп'ютерної криміналістики Національного інституту стандартів та технологій США було прийнято методологію тестування програмних засобів комп'ютерно-технічної експертизи на основі розробки загальних специфікацій інструментів, процедур випробувань, критеріїв випробувань, наборів тестів та обладнання для тестування. Тестування дає

можливість отримати інформацію, яка необхідна розробникам для вдосконалення інструментів, що розробляються, дозволяє користувачам робити усвідомлений вибір щодо придбання та використання інструментів комп'ютерно-технічної експертизи та сприяє розумінню можливостей інструментів усіма зацікавленими сторонами.

4.3. Криміналістична експертиза Інтернету речей

Інтернет речей означає мережу взаємопов'язаних та взаємодіючих один з одним пристроїв з виходом в Інтернет (наприклад, камери, телевізори, холодильники, духові шафи, освітлювальні прилади, лічильники електричної енергії, одяг, іграшки, аксесуари та багато іншого), які дозволяють відстежувати об'єкти, людей, тварин та рослини, а також здійснювати збір, аналіз, зберігання та розповсюдження даних про них. Оскільки мережні пристрої Інтернету речей можуть містити значний обсяг інформації про користувачів цих пристроїв, дані, отримані з цих пристроїв, представлялися як докази в судах. Наприклад, у Сполучених Штатах дані з FitBit, мережевого пристрою Інтернету речей, який відстежує стан здоров'я та фізичну активність, були представлені як доказ вбивства Конні Дабейт (Altimari, 2018). Враховуючи, що дані з мережевих пристроїв Інтернету речей подаються як докази в судах, необхідно розробляти процедури, стандарти та інструменти для проведення криміналістичної експертизи таких мережевих пристроїв.

Метою етапу аналізу є визначення значущості та доказової сили свідчень. Це робиться, наприклад, шляхом визначення того, чи має доказ, що розглядається, «тенденцію робити існування будь-якого факту, що має значення для вирішення справи, більш-менш ймовірним, ніж це було б без цього доказу» (Правило 401, Федеральні правила США про докази). Етап *звітності* включає докладний опис кроків, зроблених протягом усього процесу цифрової судової експертизи, виявлених цифрових доказів та висновків, зроблених на основі результатів цифрової судової експертизи та виявлених доказів.

Штучний інтелект (тобто «обчислювальні моделі людської поведінки та розумових процесів, призначені для раціональної та розумної роботи») може використовуватися для отримання достовірних результатів. Однак використання штучного інтелекту може створювати проблеми на етапах аналізу та подання даних процесу цифрової судової експертизи, оскільки експерти можуть бути не в змозі пояснити, як були отримані ці результати.

ISO/IEC опублікували додаткові посібники з процесу цифрової криміналістики, які охоплюють: достовірність та надійність інструментів та методів цифрової судової експертизи (ISO/IEC 27041:2015, Посібник із забезпечення придатності та адекватності методу розслідування інцидентів), а також етапи дослідження та інтерпретації процесу цифрової судової експертизи (ISO/IEC 27042:2015, Посібник з аналізу та інтерпретації цифрових свідочств).

Примітка

Ці стандарти не призначені для нетрадиційних обчислювальних систем, як-от хмарні обчислення. Тим не менш, Cloud Security Alliance (Альянс безпеки у хмарі) опублікував документ під назвою «Прив'язка криміналістичного стандарту ISO/IEC 27037 до хмарних обчислень» з метою «нового тлумачення керівництва ISO 27037 для хмарного контексту».

В даний час доступні посібники з передової практики для визначення та популяризації обґрунтованих та надійних процесів та результатів цифрової судової експертизи. Як приклади можна навести керівництво з передової практики, розроблене в США Науковою робочою групою з цифрових доказів, для комп'ютерно-технічної судової експертизи, збору цифрових доказів та збору даних для комп'ютерно-технічної експертизи, а також керівництво з передової практики *Європейської Мережі* судово-експертних установ для судової експертизи цифрових технологій.

Ці стандарти та передові практичні методи використовуються з метою встановлення *обґрунтованості* та *достовірності* результатів цифрової судової експертизи. По-перше, для того вони були допустимими, інструменти та методи, які використовуються в процесі цифрової судової експертизи, мають бути «науково обґрунтованими», тобто шляхом емпіричного тестування має бути доведено, що вони дають точні результати. По-друге, результати цифрової судової експертизи повинні бути достовірними, тобто одні й ті самі результати мають бути отримані в різних випадках з використанням тих самих даних, інструментів і методів. Зокрема, результати мають бути повторюваними та відтворюваними. Результати є *повторюваними*, коли одні й самі результати цифрової судової експертизи виходять з допомогою тих самих тестованих предметів, устаткування, лабораторії та оператора. Результати є *відтворюваними*, коли одні й самі результати цифрової судової експертизи виходять з допомогою тих самих тестованих предметів, але з використанням різних видів устаткування, лабораторій і операторів. Як відзначила Національна рада начальників поліції Сполученого Королівства, важливим принципом практики цифрової криміналістики є здатність «незалежної третьої сторони... вивчати ці процеси та досягати того самого результату» (Принцип 3).

4.4. Антикриміналістика

Антикриміналістика (або цифрова антикриміналістика) – це термін, що використовується для опису «інструментів і методів, що [використовуються] для видалення, зміни, порушення даних або іншого впливу на докази злочинної діяльності в цифрових системах, аналогічно тому, як якщо б злочинці видалили докази з місця злочину у фізичному світі». Методи антикриміналістики включають приховування даних (наприклад, шифрування, і стеганографія – практика приховування секретних даних, зображень, аудіозаписів, відеоматеріалів та іншого контенту шляхом їх вбудовування в несекретні дані, зображення,

аудіозаписи, відеоматеріали та інший контент), стирання артефакції вміст цифрових пристроїв (наприклад, за допомогою програмного забезпечення, призначеного для видалення окремих або всіх даних та/або вмісту пристроїв) та заплутування цифрового сліду (наприклад, тактика спуфінгу (підміни); помилкова ідентифікація даних, дезінформація та/або фабрикація даних; та використання) проксі-серверів, які діють як шлюз або посередник між запитом, що надсилається від цифрових пристроїв, підключених до Інтернету, до інших серверів). Використання методів антикриміналістики ускладнює зусилля щодо проведення цифрової судової експертизи.

Висновки

Цифрова криміналістика включає процеси ідентифікації, отримання, збереження, аналізу та подання цифрових доказів. Цифрові докази мають бути автентифіковані, щоб забезпечити їхню допустимість у суді. Зрештою, артефакти для судово-експертного аналізу та використовувані криміналістичні методи (наприклад, збір даних у статичному режимі або в реальному часі) залежать від пристрою, його операційної системи та його засобів захисту. Запатентовані операційні системи (з якими слідчі можуть бути незнайомі) та засоби захисту (наприклад, шифрування) є перешкодами для проведення цифрової судової експертизи. Наприклад, *шифрування*, яке блокує доступ третіх осіб до інформації про користувачів та їх повідомлення, може завадити правоохоронним органам отримати доступ до даних, що містяться у цифрових пристроях, таких як смартфони.

Вправа № 1 - Про дані

Виберіть цифровий пристрій (як альтернативу можете обговорити пристрій, який у вас є).

Які дані зберігає цей пристрій?

Який це тип даних?

Де знаходяться ці дані?

Як можна знайти дані?

Вправа № 2 – Інструменти цифрової криміналістики

На ринку є багато інструментів цифрової криміналістики. Знайдіть інструмент цифрової криміналістики, який найчастіше використовується в вашій країні.

Питання для обговорення

Для якого типу криміналістики використовуються інструменти?

Чи цей інструмент криміналістично надійний?

Питання для самоперевірки

1. Яка різниця між даними вмісту та метаданими? Які типи інформації відкриває кожен тип даних?
2. Які є різні типи електронних доказів?
3. Чим відрізняються електронні докази від традиційних?
4. Як автентифікується цифровий доказ?
5. Що таке моделі процесу цифрової криміналістики? Назвіть і опишіть дві з них.
6. Що прагнуть встановити стандарти та передові практики для цифрових доказів і цифрової криміналістики?

Лекція 5. Розслідування кіберзлочинів

5.1. Повідомлення про кіберзлочини.

5.2. Органи кримінального правосуддя

5.3. Приклад рівня ЗНС слідчого у справах про кіберзлочинність

5.3. Органи національної безпеки

5.4. Перешкоди у розслідуванні кіберзлочинів.

5.1. Повідомлення про кіберзлочини.

Перш ніж розпочати розслідування, необхідно зафіксувати факт скоєння кіберзлочину та повідомити про нього. Хоча це здається простим першим кроком у розслідуванні кіберзлочину, реальність така, що значна частина випадків кіберзлочинів у всьому світі не повідомляється (УНЗ ООН, 2013).

Небажання повідомляти про злочини можна пояснити *теорією очікуваної корисності*, висунутої економістом Гері Беккером (1968), яка свідчить, що беруть участь у будь-яких діях, коли очікувана корисність від цих дій перевершує очікувану корисність участі у інших діях. У контексті кіберзлочинності жертви кіберзлочинів не повідомляють про кіберзлочин, якщо очікувана корисність такого повідомлення є низькою. Проте готовність особи чи організації повідомити про кіберзлочин залежить і від типу кіберзлочину. Дослідження, що проводяться в даний час, визначають кілька причин, внаслідок яких кіберзлочини не повідомляються, включаючи почуття сорому і збентеження, які зазнають жертвами певних видів кіберзлочинів (наприклад, романтичної афери); репутаційні ризики, пов'язані з оприлюдненням факту вчинення кіберзлочину (наприклад, якщо жертвою кіберзлочину є комерційне підприємство, або є загроза втрати довіри з боку споживачів); відсутність усвідомлення того, особа стала жертвою злочину; низький ступінь впевненості чи очікувань щодо здатності правоохоронних органів надати допомогу; необхідність витрачання занадто великої кількості часу та зусиль для повідомлення про

кіберзлочин; і відсутність обізнаності про те, кому слід повідомляти про кіберзлочини.

Як реагування на занижену частоту повідомлень про кіберзлочини урядові та неурядові організації реалізували ініціативи, спрямовані на підвищення кількості повідомлень шляхом оптимізації процедури подання інформації про кіберзлочини, яка зазвичай передбачає участь кількох установ залежно від типу скоєного кіберзлочину (наприклад, повідомлення про фінансове шахрайство мережі Інтернет можуть отримувати поліція, банки та інші фінансові установи, а також державні органи, які беруть участь у розслідуванні кіберзлочинів фінансових установ), та привернення уваги до механізмів повідомлення інформації про кіберзлочини, такі як веб-сайти або гарячі лінії. Наприклад, у Новій Зеландії NetSafe – незалежна некомерційна організація, що працює у сфері забезпечення безпеки в Інтернеті, – розробила у співпраці з державними органами веб-сайт Orb для надання громадянам країни єдиного та безпечного місця, де вони можуть залишити повідомлення про кіберзлочин. У Південній Африці Південноафриканський портал ресурсів та інформації про кіберзлочини дозволяє користувачам повідомляти про кіберзлочини на своєму порталі. Крім того, у 2018 році в США Федеральне бюро розслідувань (ФБР) ініціювало інформаційно-роз'яснювальну кампанію з кіберзлочинності за участю актриси з американського телесеріалу «Думати як злочинець», яка інформувала громадськість про можливість направлення повідомлень про кіберзлочини до Центру.

Необхідно оцінювати вплив таких ініціатив на частоту повідомлень про кіберзлочини. В Австралії було створено *Австралійську мережу Інтернет-повідомлень про кіберзлочинність* (Australian Internet Cybercrime Reporting Network, AICRN), щоб спростити процедуру отримання повідомлень про кіберзлочини. У 2016 році Австралійський інститут кримінології опублікував звіт про оцінку AICRN, який показав, що ця ініціатива мала лише незначний вплив на частоту повідомлень про

кіберзлочини та рівень обізнаності громадськості про те, куди слід спрямовувати такі повідомлення. Оцінка таких ініціатив має важливе значення, оскільки вона дозволяє урядам вкладати кошти в ті проєкти, які приносять бажані результати та допомагають вносити зміни та доповнення до програм та ініціатив, які не приносять очікуваних результатів.

Хто проводить розслідування кіберзлочинів?

Особи, які вживають перші заходи у відповідь при розслідуванні кіберзлочинів, відповідають за «збереження» цифрових доказів на «місці» скоєння кіберзлочину (наприклад, це може бути об'єкт чи об'єкти кіберзлочину та/або пристрої інформаційно-комунікаційних технологій, використані для скоєння злочину з використанням кібермереж і /або кіберзалежного злочину). Такою особою, яка приймає перші заходи реагування, може бути співробітник правоохоронних органів, експерт з цифрової криміналістики, офіцер військової поліції, приватний слідчий, спеціаліст з інформаційних технологій або інша особа (наприклад, працівник із найму), якій поставлено завдання реагувати на події, пов'язані з кіберзлочинністю. Це говорить про те, що розслідування кіберзлочинів проводять державний та приватний сектори, а також органи національної безпеки (з тим чи іншим ступенем участі). Незалежно від того, хто вживає перших заходів у відповідь, процедури пошуку та вилучення пристроїв інформаційно-комунікаційних технологій (ІКТ) повинні відповідати національному законодавству, а методи, що використовуються для отримання цифрових доказів з пристроїв ІКТ, повинні бути обґрунтованими та надійними, щоб забезпечити допустимість доказів у суді.

5.2.Органи кримінального правосуддя

Працівники системи кримінального правосуддя, такі як правоохоронці, прокурори та судді, несуть відповідальність за профілактику, пом'якшення негативних наслідків, виявлення, розслідування кіберзлочинів, а також кримінальне переслідування та

винесення судових рішень у справах, пов'язаних з кіберзлочинністю. Конкретні органи, відповідальні розслідування кіберзлочинів, різняться залежно від держави. Наприклад, у Великій Британії розслідування кіберзлочинів проводять кілька органів, у тому числі регіональні правоохоронні органи та Національний підрозділ боротьби з кіберзлочинністю, який входить до складу Національного агентства боротьби зі злочинністю. На відміну від Великобританії, лише одна установа займається розслідуванням кіберзлочинів у таких країнах, як Сьєрра-Леоне, де розслідування проводить відділ поліції щодо запобігання кіберзлочинності (Global CyberSecurity Capacity Centre, 2016d), Еквадор, де «Відділ з розслідування технологічних злочинів Національної дирекції судової поліції та розслідувань несе відповідальність за розслідування кіберзлочинів» (Inter-American Development Bank, 2016, p. 72), та Ісландія, де такими розслідуваннями займається підрозділ цифрової судової експертизи поліції Рейк'явіка (Global Cyber Security Capacity Centre, 2017c).

Більше того, в деяких країнах у розслідуванні одного і того ж кіберзлочину можуть брати участь кілька установ. Участь тієї чи іншої установи залежить від типу кіберзлочину, що розслідується. Наприклад, на Кіпрі злочини, пов'язані з фінансовим шахрайством в Інтернеті, розслідуються Відділом кримінальних розслідувань, а також Групою розслідування фінансових злочинів Головного управління поліції Кіпру (Global CyberSecurity Capacity Centre, 2017b). У зв'язку з тим, що у різних країнах відповідальність за боротьбу з кіберзлочинністю та проведення розслідувань справ про кіберзлочини несуть різні органи, у багатьох країнах створюються офіційні контактні пункти. Наприклад, на Кіпрі цілодобовим контактним пунктом є Управління боротьби з кіберзлочинністю (Global Cyber SecurityCapacity Centre, 2017b).

Співробітники органів кримінального правосуддя повинні володіти спеціальними знаннями (тобто інформацією, що відноситься до предметної галузі, яка необхідна для виконання завдання), навичками (тобто

професійним досвідом у предметній галузі) та здібностями (тобто вмінням застосовувати знання та навички для виконання завдання) (всі разом вони іменуються ЗНС (знання, навички, здібності); див. «Приклад рівня ЗНС для слідчого у справах про кіберзлочинність» у вставці нижче), на додаток до тих знань, навичок та здібностей, які необхідні для розслідування, кримінального переслідування та/або розгляду справ, пов'язаних із злочинами, що скоюються поза мережею Інтернет. Наприклад, правоохоронці повинні бути в змозі розслідувати кіберзлочини та/або інші злочини, які так чи інакше пов'язані з використанням пристроїв інформаційно-комунікаційних технологій (наприклад, смартфонів, в яких зберігаються докази злочину), і належним чином звертатися з ІКТ у ході розслідування (наприклад, виявляти, отримувати, зберігати та аналізувати цифрові докази таким чином, щоб забезпечити їх допустимість у суді) (National Initiative for Cybersecurity Careers and Studies, nd). Можливості правоохоронних органів розслідувати кіберзлочини залежать від країни та варіюються залежно від конкретної установи всередині країни. Наприклад, у Киргизькій Республіці правоохоронні органи мають обмежені можливості для розслідування кіберзлочинів через відсутність спеціалізованих знань, навичок, здібностей, підготовки, а також нестачі кадрових та фінансових ресурсів (Global Cyber Security Capacity Centre, 2017a). На Мадагаскарі звіт за 2017 рік показав, що, хоча у структурі правоохоронних органів «не було спеціалізованого підрозділу боротьби з кіберзлочинністю, ... питаннями кіберзлочинності займалися деякі спеціально призначені для цієї мети співробітники Національної поліції та жандармерії» (Global Cyber Security Capacity Centre, 2017a, р. 33). Для порівняння, у Франції існує кілька підрозділів, співробітники яких мають спеціальну підготовку для проведення розслідувань кіберзлочинів (наприклад, Les investigateurs en Cybercriminalité (слідчі у справах про кіберзлочинність) та N-TECH (слідчі зі спеціальною підготовкою у сфері нових технологій), які входять до складу Національної жандармерії) (для

ознайомлення зі звітами про інші країни див. портал Глобального центру розвитку потенціалу в області кібербезпеки).

5.3. Приклад рівня ЗНС слідчого у справах про кіберзлочинність

Структура трудових ресурсів у сфері кібербезпеки (Cybersecurity Workforce Framework), розроблена в рамках Національної освітньої ініціативи США у сфері кібербезпеки, включає ЗНС для штатних посад, пов'язаних з кібербезпекою і кіберзлочинністю. Наприклад, у Структурі трудових ресурсів у галузі кібербезпеки освітньої ініціативи перераховані такі рівні знань, навичок та здібностей для слідчого у справах про кіберзлочинність (US National Initiative for Cybersecurity Careers and Studies, nd).

Знання

Знання концепцій побудови комп'ютерних мереж, мережевих протоколів та методологій безпеки мережі.

Знання процесів управління ризиками (наприклад, методів оцінки та зниження ризику).

Знання законів, правил, політики та етики, що стосуються кібербезпеки та конфіденційності.

Знання принципів забезпечення кібербезпеки та збереження конфіденційності.

Знання кіберзагроз та вразливостей.

Знання конкретних оперативних наслідків недоліків у системі кібербезпеки.

Знання методологій та методів виявлення вторгнень для виявлення вторгнень на рівні вузла та мережі.

Знання загроз безпеки та вразливостей системи та додатків (наприклад, переповнення буфера, мобільний код, міжсайтовий скриптинг, процедурна мова/мова структурованих запитів [PL/SQL] та впровадження SQL-коду, стан гонки, прихований канал, відтворення, зворотно-орієнтовані атаки, шкідливий код).

Знання інструментів та законів/регламентів для проведення розслідування інсайдерських загроз та складання звітів.

Знання тактики, методів та процедур, що використовуються зловмисниками.

Знання електронних пристроїв (наприклад, комп'ютерних систем/компонентів, пристроїв контролю доступу, цифрових камер, цифрових сканерів, електронних органайзерів, жорстких дисків, карт пам'яті, модемів, мережевих компонентів, мережевих приладів, мережевих пристроїв керування домом, принтерів, знімних пристроїв зберігання даних, телефонів, копіювальних пристроїв, факсимільних апаратів тощо).

Знання процедур вилучення та збереження цифрових доказів.

Знання законних методів управління, пов'язаних із забезпеченням допустимості доказів (наприклад норм доказового права).

Знання процесів збирання, пакування, транспортування та зберігання електронних доказів у рамках системи охорони доказів.

Знання типів і наборів даних, що постійно зберігаються.

Знання соціальної динаміки зломщиків у глобальному контексті.

Знання закону про електронні докази.

Знання правових норм доказового права та процедур судочинства.

Знання застосовних законів, статутів (наприклад, у титулах 10, 18, 32, 50 Кодексу США), президентських директив, директивних вказівок органів виконавчої влади та/або адміністративних/кримінально-правових керівних принципів та процедур.

Знання методів прихованого зв'язку.

Знання протоколів, процедур та методів управління кризовими ситуаціями.

Знання фізичної та фізіологічної поведінки, яка може вказувати на підозрілу чи ненормальну активність.

Знання судових процедур, включаючи процедури подання фактів та доказів.

Знання застосовних статутів, законів, положень та принципів, що регулюють кібератаки та кіберексплуатацію .

Знання ризиків для безпеки програм (наприклад, список Топ-10 спільноти «Відкритий проєкт безпеки веб-додатків»)

Навички

Навички збереження цілісності доказів відповідно до стандартних операційних процедур чи національних стандартів.

Навички збирання, обробки, пакування, транспортування та зберігання електронних доказів для недопущення змін, втрати, фізичного пошкодження або знищення даних.

Навички використання наукових правил та методів для вирішення проблем.

Навички оцінки надійності постачальника та/або продукту.

Здібності

Здатність здійснювати пошук і навігацію по даркнет за допомогою мережі TOR для пошуку ринків та форумів.

Здатність досліджувати цифрові носії на кількох платформах операційних систем.

Інші працівники системи кримінального правосуддя, такі як прокурори і судді, також повинні володіти спеціальними знаннями про кіберзлочинність і *цифрову криміналістику* (що є «однією з галузей криміналістики, що спеціалізується на кримінально-процесуальному праві та доказах стосовно комп'ютерів та пов'язаних з ними пристроїв»). Як і у випадку правоохоронних органів, рівень підготовки прокурорів та суддів варіюється між країнами та навіть усередині країн. Наприклад, у Великобританії Королівська прокурорська служба має всі можливості для судового переслідування винних у скоєнні кіберзлочинів, тоді як станом на 2016 рік прокурори на місцевому рівні не мали такої ж підготовки та ресурсів для здійснення судового переслідування у зв'язку з кіберзлочинами (Global Cyber Security Capacity Centre, 2016c). У 2017 році

влада Сьєрра-Леоне повідомила, що прокурори і судді не мають необхідних знань, навичок, здібностей і ресурсів для судового переслідування і розгляду справ, пов'язаних з кіберзлочинністю (Global Cyber Security Capacity Centre, 2016d). Схожа ситуація спостерігається в Ісландії, де прокурори та судді проходять лише спеціальну підготовку з питань кіберзлочинності на добровільній основі (Global Cyber Security Capacity Centre, 2017c). Співробітники органів правосуддя повинні проходити підготовку для ознайомлення з базовою інформацією про кіберзлочинність та цифрову криміналістику, вивчення питань, що стосуються свідчень експертів у справах про кіберзлочини та допустимості цифрових доказів у суді. У 2017 році влада Сенегалу повідомила, що судді не проходять підготовку подібного типу (Global CyberSecurity Capacity Centre, 2016b).

Крім національних органів кримінального правосуддя, регіональні установи, такі як Агентство Європейського Союзу зі співробітництва правоохоронних органів Europol (для розвитку співробітництва між правоохоронними органами в Європейському союзі) та Eurojust (для розвитку співробітництва між судовими органами країн-членів Європейського союзу), та міжнародні агентства, такі як INTERPOL (Міжнародна організація кримінальної поліції, що сприяє міжнародному співробітництву між правоохоронними органами), сприяють проведенню транскордонних розслідувань кіберзлочинів. Наприклад, в результаті обміну оперативними даними та ресурсами між Європолем та державами-членами Європейського союзу було заарештовано злочинця, відомого тим, що продавав фальшиві банкноти номіналом 50 євро на незаконних ринках у темному Інтернеті.

5.4.Органи національної безпеки

Органи національної безпеки можуть брати участь у розслідуваннях кіберзлочинів (наприклад, у деяких країнах розслідування кіберзлочинів можуть проводитися за участю військових органів, тоді як в інших країнах

такі розслідування можуть проводитися розвідувальними органами або національними управліннями кібербезпеки). Однак участь органів національної безпеки в розслідуваннях кіберзлочинів залежить від розслідуваного кіберзлочину, об'єкта (об'єктів) кіберзлочину та/або виконавців кіберзлочину. Наприклад, військові органи можуть розслідувати кіберзлочини, які мають будь-який зв'язок із збройними силами, тобто кіберзлочини, вчинені проти військовослужбовців, військового майна та/або військової інформації, та/або кіберзлочини, вчинені військовослужбовцями.

Як приклад можна навести Сполучені Штати, де співробітники військової поліції розслідують випадки порушення Єдиного кодексу військової юстиції. На додаток до розслідування таких кіберзлочинів (або, як мінімум, до участі в розслідуванні кіберзлочинів у тій чи іншій якості), військові органи та інші органи національної безпеки можуть відповідати за виявлення, пом'якшення негативних наслідків, запобігання кіберзлочинам, спрямованим на системи, мережі та дані цих органів, системи, що містять секретну інформацію, а також за вжиття заходів реагування на такі кіберзлочини.

Органи національної безпеки по всьому світу розвинули та/або в даний час розвивають свої *кібероборонні* можливості (тобто заходи, які призначені для виявлення та запобігання кіберзлочинів та пом'якшення наслідків цих кіберзлочинів у разі їх скоєння) та *кібернаступальні* можливості це заходи, які «призначені для проникнення в системи супротивника та заподіяння їм шкоди» та/або реагування на кібератаку. Саме визнання кіберпростору як ще одна сфера ведення бойових дій (п'ята сфера поряд із сушею, морем, повітрям і космосом; також відома під назвою сфера операцій, див. вставку «Чи знаєте ви?» нижче), призвело до розширення діяльності органів національної безпеки в кіберпросторі. Наприклад, у Сполучених Штатах таке визнання п'ятої сфери ведення бойових дій спричинило створення Кібернетичного командування США

(USCYBERCOM). За прикладом Сполучених Штатів інші країни, такі як Нідерланди, Німеччина, Іспанія, Республіка Корея та Японія, також створили аналогічні кібернетичні командування та/або кібернетичні центри або підрозділи. Організація Північноатлантичного договору (НАТО) також визнала кіберпростір п'ятою сферою ведення бойових дій (NATOCCDCE, 2016).

Чи знаєте ви?

На Філіппінах вважають за краще використовувати термін «сфера операцій». Відповідно до статті 2 Конституції країни, «Філіппіни відмовляються від війни як інструменту здійснення національної політики, переймають та використовують загальноприйняті принципи міжнародного права як частину законодавства власної країни та дотримуються політики миру, рівності, справедливості, свободи, співробітництва та мирних відносин між усіма націями».

Приватний сектор

Приватний сектор відіграє важливу роль у справі виявлення, запобігання, пом'якшення наслідків та розслідування кіберзлочинів, оскільки в більшості випадків саме приватний сектор має *критично важливу інфраструктуру* (тобто інфраструктуру, яка вважається необхідною для функціонування суспільства) і керує нею і є однією з основних мішеней багатьох кіберзалежних злочинів (тобто кіберзлочинів, мета яких полягає в порушенні конфіденційності, цілісності та доступності систем, мереж, сервісів та даних, таких як злом, поширення шкідливих програм та розподілені атаки типу «відмова в обслуговуванні» або DDoS-атаки) та злочинів з використанням кібермереж (наприклад, фінансове шахрайство в Інтернеті, злочини, пов'язані з використанням персональних даних, крадіжка даних та комерційної таємниці та багато інших).

Відповідно до Резолюції 2341 (2017) Ради Безпеки Організації Об'єднаних Націй, «кожна держава сама визначає, які об'єкти її інфраструктури є критично важливими» на її території. Оскільки такий

статус інфраструктури визначається самою державою, між країнами існують відмінності щодо того, які об'єкти інфраструктури належать до критично важливих. Наприклад, Австралія як критично важлива інфраструктура визначила об'єкти, що стосуються восьми секторів (а саме: охорона здоров'я; енергетика; транспорт; водопостачання; зв'язок; виробництво продовольства та роздрібна торгівля продуктами харчування; банківська справа та фінанси; і уряд Австралійського союзу, тоді як Сполучені Штати визначили 16 типів об'єктів критично важливої інфраструктури (хімічні об'єкти; торговельні підприємства; об'єкти зв'язку; критично важливі промислові об'єкти; греблі; виробнича база оборонної промисловості; аварійні служби; енергетика; фінансові послуги; продовольство та сільське господарство; державні установи; охорона здоров'я та санітарно-епідеміологічні служби; інформаційні технології; ядерні реактори, матеріали та відходи; транспортні системи; та системи водопостачання та видалення стічних вод.

Чи знаєте ви?

Термін «критично важлива інфраструктура» використовується не всіма країнами для опису базової інфраструктури (Виконавчий директорат Контртерористичного комітету Ради Безпеки Організації Об'єднаних Націй та Контртерористичне управління Організації Об'єднаних Націй, 2018 рік). Наприклад, замість терміну «критично важлива інфраструктура» Нова Зеландія використовує термін «життєво важливі комунікації» для позначення своїх важливих об'єктів життєзабезпечення, які включає енергетику, зв'язок, транспорт і водопостачання (New Zealand Lifelines Council, 2017).

«Мережі та системи командування та управління, призначені для підтримки виробничих процесів» на об'єктах критично важливої інфраструктури, відомі під назвою *системи управління технологічними процесами* (СУТП). Як зазначає Європейське агентство з мережевої та інформаційної безпеки, СУТП зазнали значних перетворень,

перетворившись із закритих ізольованих систем на системи відкритої архітектури та стандартних технологій, тісно пов'язані з іншими корпоративними мережами та Інтернетом. Сьогодні продукти СУТП здебільшого засновані на стандартних платформах вбудованих систем, що застосовуються у різних пристроях, таких як маршрутизатори або кабельні модеми, і вони часто використовують готове комерційне програмне забезпечення. Все це призвело до зниження витрат, зручності у використанні та дозволило здійснювати дистанційне керування та моніторинг із різних місць. Однак істотним недоліком, пов'язаним із підключенням до інтрамереж і мереж зв'язку, є підвищена вразливість до атак на основі комп'ютерних мереж (ENISA, nd).

Саме ці вразливості, а також ті, які є результатом неналежних заходів щодо забезпечення фізичної безпеки та захисту від зловмисних дій персоналу (наприклад, працівник може принести заражений флеш-накопичувач на об'єкт критично важливої інфраструктури та фізично підключити його до систем цієї інфраструктури).

Оскільки в більшості випадків критично важливою інфраструктурою володіє приватний сектор, який управляє нею і є однією з основних мішеней кіберзлочинців, він має усі можливості для вжиття заходів забезпечення безпеки, призначених для виявлення кіберзлочинів і кіберзлочинців у попереджувальному порядку з метою запобігання або, як мінімум, наслідків кіберзлочинів, а також реагування на кіберзлочини, які вчиняються або були вчинені. Масштаби таких заходів, що вживаються приватним сектором, залежать від конкретної організації, її сфери діяльності чи організаційно-правової форми, її людських, фінансових та технічних ресурсів та можливостей.

Приватний сектор також проводить приватні розслідування кіберзлочинів. Приватний сектор вразливий як до *внутрішніх загроз* (наприклад, до кіберзлочинів, які вчиняють співробітники або керівники комерційного підприємства або організації), так і до *зовнішніх загроз*

(наприклад, до кіберзлочинів, які вчиняються особами, якимось чином пов'язаними з комерційним підприємством або організацією, наприклад, постачальниками або замовниками, або особами, що ніяк не пов'язані з підприємством або організацією). Коли відбувається кіберзлочин, підприємства та організації часто не звертаються до правоохоронних органів. Це, однак, залежить від виду кіберзлочину, людських, технічних та фінансових ресурсів приватної організації, а також впливу кіберзлочину на організацію з погляду наслідків повідомлення про скоєний кіберзлочин для цієї організації (наприклад, потенційний збиток репутації та/або втрата довіри споживачів).

Неповідомлення інформації про витік даних компанією Yahoo Inc.

Компанія Yahoo Inc. (тепер відома під назвою Altaba) повідомила про один випадок (з кількох випадків) витоку даних, з яким вона стикнулася, через два роки після інциденту. Внаслідок такого розкриття інформації «ціна акцій Yahoo впала на 3 відсотки, що призвело до втрати близько 1,3 мільярда доларів США ринкової капіталізації. Крім того, компанія, яка [в той момент часу] вела переговори про продаж свого бізнесу компанії Verizon, була змушена погодитися зі знижкою у розмірі 7,25 відсотків на запропоновану ціну покупки, що знизило її на 350 млн. доларів США». Через несвоєчасне розкриття відомостей про витік даних компанія Yahoo була також оштрафована на 35 млн. доларів Комісією з цінних паперів та бірж США (US Securities and Exchange Commission, 2018).

Так само, як і правоохоронні органи, приватні компанії та організації проводять розслідування при виявленні кіберзлочину або отриманні повідомлення про кіберзлочин. Розслідування проводиться з метою отримання інформації про інцидент та порушення справи щодо виконавця (виконавців) кіберзлочину (кіберзлочинів). Залежно від розміру та ресурсів приватних компаній та організацій, розслідування може проводитися штатними слідчими або слідчими, найнятими ззовні. До осіб, які беруть

участь у розслідуваннях кіберзлочинів, входять представники приватних компаній, галузових організацій, торгових організацій та компаній, які надають послуги із забезпечення безпеки, розслідувань та цифрової криміналістики. Були випадки, коли фахівці з інформаційних технологій та експерти в галузі цифрової криміналістики з недержавного сектора використовувалися приватними компаніями та організаціями для збирання та збереження цифрових доказів. Однак ці фахівці можуть не мати необхідних знань, навичок та здібностей для проведення розслідувань кіберзлочинів та належного поводження з цифровими доказами кіберзлочину, щоб забезпечити їх допустимість у судах загального права.

Державно-приватні партнерства та цільові групи

Приватний сектор має людські, фінансові та технічні ресурси для проведення розслідувань кіберзлочинів і може надати допомогу органам національної безпеки, правоохоронним органам та іншим державним установам у справах, пов'язаних з кіберзлочинністю. У зв'язку з цим на міжнародному рівні було розроблено безліч проєктів у рамках державно-приватного партнерства з метою посилення можливостей країн для розслідування кіберзлочинів. Як приклад можна навести Центр обробки даних про кіберзлочинність (Cyber Fusion Centre) Інтерполу, де працюють як правоохоронці, так і галузеві експерти з кібербезпеки, які збирають цінну оперативну інформацію та обмінюються нею з відповідними зацікавленими сторонами. Trend Micro (компанія-розробник програм кібербезпеки та кіберзахисту) та інші приватні компанії, які займаються питаннями, пов'язаними з кіберзлочинністю або кібербезпекою, та/або є постачальниками Інтернет-послуг та Інтернет-контенту чи надають інші послуги, пов'язані з Інтернетом, тісно співпрацюють із Інтерполом.

Організація Північноатлантичного договору (НАТО) також співпрацює з союзниками в цілому та з Європейським Союзом та приватною промисловістю, зокрема на основі Технічної угоди про кіберзахист та Кіберпартнерства НАТО з промисловістю.

Механізми державно-приватного партнерства (ДПП) також створюються національному рівні. У Сполучених Штатах Національний альянс кіберкриміналістики та кіберпідготовки (NCFTA) об'єднує фахівців з кіберзлочинності з державних органів, наукових кіл та приватного сектору з метою виявлення та пом'якшення наслідків кіберзлочинів та боротьби з ними.

У Японії в рамках ДПП була створена схожа з NCFTA структура – Центр боротьби з кіберзлочинністю. У Європі проєкт 2Centre (2 Центр) здійснюється на основі співробітництва між правоохоронними органами, освітніми організаціями та приватним бізнесом. Реалізація цього проєкту в рамках ДПП розпочалася зі створення національних центрів в Ірландії та Франції, і згодом національні центри були створені в інших країнах; Станом на 2017 рік такі центри функціонують у Греції, Іспанії, Бельгії, Естонії, Литві, Болгарії та Англії (Cybercrime Centres of Excellence Network for Training, Research and Education, nd).

На додаток до ДПП були створені національні цільові групи для надання допомоги у розслідуванні кіберзлочинів. Ці цільові групи дозволяють правоохоронним органам, які мають різні юрисдикції та повноваження у своїх країнах (чи місцеві, регіональні чи федеральні/національні органи) здійснювати співпрацю у справах, пов'язаних з кіберзлочинністю. Ці групи, залежно від конкретної країни та/або регіону, можуть також включати до свого складу представників наукових кіл та приватних компаній та організацій. Як приклад можна навести Національну об'єднану оперативну групу з кіберрозслідувань (National Cyber Investigative Joint Task Force, NCIJTF) Федерального бюро розслідувань США, яка складається з представників установ-партнерів, які входять до структур правоохоронних органів, розвідувальної спільноти та Міністерства оборони, які базуються в одному місці та тісно взаємодіють з метою виконання завдання організації на основі загальнодержавного підходу. Будучи унікальним міжвідомчим кібернетичним центром, NCIJTF

в першу чергу відповідає за координацію, узагальнення та обмін інформацією на підтримку досліджень кіберзагроз, виконання аналізу оперативних даних та подання його результатів особам, що приймають рішення, та надання сприяння іншим безперервним зусиллям по боротьбі з кіберзлочинністю.

Були створені інші цільові групи, які займаються конкретними видами кіберзлочинів. Наприклад, Цільова *група* боротьби з електронними злочинами (Electronic Crimes Task Force, ECTF), спеціальна група секретної служби США, відповідає за запобігання, пом'якшення наслідків, виявлення та розслідування кіберзлочинів, у тому числі скоєних щодо систем фінансових розрахунків та об'єктів критично важливої інфраструктури. Відповідно до Закону «Про згуртування та зміцнення Америки шляхом забезпечення належними засобами, необхідними для припинення та перешкоджання тероризму» («Патріотичний акт») 2001 року, секретна служба США створила мережу цільових груп по боротьбі з електронними злочинами (ECTF) по всій території Штатів. Ці цільові групи взаємодіють із місцевими, регіональними та федеральними правоохоронними органами, а також з іншими працівниками системи кримінального правосуддя (наприклад, прокурорами), представниками наукової спільноти та приватного сектору. Європейську цільову групу з боротьби з електронними злочинами (European Electronic Crime Task Force, EECTF) було створено у 2009 році. EECTF здійснює збір, аналіз та поширення інформації про передову практику.

Хоча органи кримінального правосуддя, органи національної безпеки, приватний сектор, ДПП та цільові групи є основними дійовими особами під час проведення розслідувань кіберзлочинів, незалежні розслідування кіберзлочинів можуть також проводитися інститутами громадянського суспільства, журналістами та громадськістю. Прикладом може бути лабораторія Citizen Lab, опубліковані дослідження якої включають «розслідування цифрового шпигунства проти громадянського

суспільства, документальне підтвердження фільтрації Інтернет-контенту та інших технологій і методів, що негативно впливають на здійснення права на свободу слова в Інтернеті, аналіз засобів контролю конфіденційності, безпеки та інформаційних потоків, використовуваних у популярних додатках, а також вивчення механізмів забезпечення прозорості та підзвітності у взаємовідносинах між корпораціями та державними установами у сфері захисту персональних даних та інших видів нагляду». Крім того, представники громадськості можуть надавати правоохоронним органам добровільне сприяння шляхом проведення власних незалежних розслідувань в Інтернеті; такий випадок спостерігався після вибухів у Бостоні у 2013 році. Більше того, деякі аспекти розслідування кіберзлочинності (наприклад, виявлення незаконних матеріалів в Інтернеті) можуть доручатися та вже доручалися громадськості шляхом проведення відкритого конкурсу (цей процес називається *краудсорсингом*). Наприклад, Європол виступив з краудсорсинговою ініціативою для залучення широкої громадськості до розширеного пошуку джерел походження зображень сексуального насильства над дітьми. З моменту запуску проєкту, реалізація якого розпочалася 1 червня 2017 року, до Європолу було надіслано понад 22.000 корисних підказок, в результаті розгляду яких станом на той момент вдалося опізнати вісім дітей і затримати одного злочинця завдяки допомозі простих громадян».

5.5. Перешкоди для розслідування кіберзлочинів

Під час проведення розслідувань кіберзлочинів можуть бути різні перешкоди. Однією з таких перешкод є анонімність, яку забезпечують користувачам засоби інформаційно-комунікаційних технологій. *Анонімність* дозволяє людям займатися якоюсь діяльністю, не розкриваючи інформації про свою особистість та/або свої дії іншим особам. Існує кілька методів анонімізації, які використовують кіберзлочинці (див. вставку «Примітка» нижче). Одним із таких методів є використання проксі-серверів. *Проксі-сервер* – це проміжний сервер, який

використовується для з'єднання клієнта (тобто комп'ютера) з сервером, з якого клієнт запитує ресурси. *Анонімайзери* або анонімні проксі-сервери приховують дані ідентифікації користувачів, маскуючи їх IP-адреси та замінюючи їх іншими IP-адресами.

Примітка

Методи анонімізації використовуються як на законних, так і на незаконних підставах. Існують законні підстави для того, щоб залишатися анонімним і зберігати захист анонімності в мережі. Наприклад, анонімність сприяє вільному потоку інформації та повідомлень без побоювань наслідків за висловлювання небажаних або непопулярних думок (якщо тільки не існують законних підстав, що мають переважну юридичну силу, для обмеження права на вираження таких думок) по кіберзлочинності: «Правова база та права людини» для ознайомлення із законними та легітимними обмеженнями права на свободу вираження поглядів».

Кіберзлочинці можуть також використовувати анонімні мережі для шифрування (тобто блокування доступу) трафіку та приховування адреси Інтернет-протоколу (або *IP-адреси*), «унікального ідентифікатора, що присвоюється комп'ютеру [або іншому підключеному до Інтернету цифровому пристрої] постачальником послуг Інтернету при підключенні до мережі», щоб приховати свою активність в Інтернеті та своє місцезнаходження. Добре вивченими прикладами анонімних мереж є Tor, Freenet та Invisible Internet Project.

Чи знаєте ви?

«Цибулевий» маршрутизатор (або Tor), який забезпечує анонімні доступ, комунікацію та обмін інформацією в Інтернеті, був спочатку розроблений Військово-морською дослідницькою лабораторією США для захисту розвідувальних даних. Після того як Tor став доступним для широкої публіки, він став використовуватися окремими особами для захисту від приватного та державного нагляду за їхньою активністю в

мережі. Однак Tor і інші анонімні мережі також використовувалися кіберзлочинцями для скоєння злочинів з використанням кібермереж і кіберзалежних злочинів та/або для обміну інформацією та/або інструментами з метою скоєння таких злочинів (Europol, 2018).

Ці анонімні мережі не тільки «маскують ідентифікуючі дані користувачів, але й розміщують їх веб-сайти на своїх ресурсах, використовуючи можливості [своїх] «прихованих сервісів», що означає, що [ці сайти] можуть бути доступні лише особам» у цих анонімних мережах (Dredge, 2013). Таким чином, ці анонімні мережі використовуються для доступу до сайтів у Даркнет (або Темному павутинні) (див. вставку «Всесвітня павутина: основні відомості» нижче).

Всесвітнє павутиння: основні відомості

Для наочного уявлення Всесвітньої павутини найчастіше використовують образ айсберга в океані. Частина айсберга над поверхнею води називається видимим Інтернетом (або видимим павутинням, або видимою мережею). Ця частина павутини включає індексовані сайти, які доступні і готові до використання для широкої публіки, і які можна знайти з використанням традиційних пошукових систем, таких як Google або Bing. Глибока мережа – це частина айсберга, яка знаходиться нижче за рівень поверхні води. Вона включає сайти, які не індексуються пошуковими системами і не є легкодоступними та/або готовими до використання для широкої публіки, наприклад сайти, захищені паролем. До цих сайтів можна отримати прямий доступ, якщо відомий єдиний покажчик ресурсу (URL; тобто адреса веб-сайту) та/або надані облікові дані користувачів (тобто імена користувачів, паролі, парольні фрази тощо) для доступу до захищених паролем веб-сайтів та онлайн-форумів. Для доступу до сайтів у темному павутинні необхідне спеціалізоване програмне забезпечення, оскільки в ньому використовуються інструменти, що підвищують анонімність, щоб перешкоджати доступу та приховати сайти.

Атрибуція є ще однією перешкодою, що ускладнює розслідування кіберзлочинів. Атрибуція – це визначення того, хто та/або що є відповідальним за скоєння кіберзлочину. Мета атрибуції полягає у віднесенні кіберзлочину на рахунок конкретного цифрового пристрою, користувача пристрою та/або інших осіб, винних у скоєнні кіберзлочину (наприклад, якщо кіберзлочин фінансується або спрямовується державою) (Lin, 2016). Використання інструментів, що підвищують анонімність, може ускладнити ідентифікацію пристроїв та/або осіб, відповідальних за скоєння кіберзлочину.

Чи знаєте ви?

На веб-сайті Інформаційного центру електронної приватності (The Electronic Privacy Information Center) міститься інформація про «інструменти підвищення анонімності» та посилання на ці інструменти.

Процес атрибуції ще більше ускладнюється через використання заражених шкідливими програмами комп'ютерів-зомбі (або *бот-мереж*) або цифрових пристроїв, керованих за допомогою *інструментів віддаленого доступу* (тобто шкідливою програмою, яка використовується для створення бекдора на зараженому пристрої, що дозволяє розповсюджувачу шкідливої програми отримати доступ до систем та керувати ними). Ці пристрої можуть використовуватися без відома користувача, чий пристрій заражений, для скоєння кіберзлочинів.

Зворотне простеження (або *простеження у зворотному напрямку*) – це процес прослідковування незаконних дій для встановлення джерела (тобто виконавця та/або цифрового пристрою) кіберзлочину. Простеження у зворотному напрямку здійснюється після скоєння кіберзлочину або при його виявленні. Попереднє розслідування проводиться з метою виявлення інформації про кіберзлочин шляхом вивчення файлів журналів (тобто *журналів подій*, що відображають активність файлових систем), які можуть допомогти виявити інформацію про кіберзлочин (тобто про те, як він був скоєний). Наприклад, журнали подій «автоматично реєструють

події, що відбуваються в комп'ютері, щоб отримати контрольний слід, який можна використовувати для відстеження, розуміння та діагностики активності та проблем у системі». Прикладами таких журналів є *журнали додатків*, які записують «події, що реєструються програмами та додатками», та *журнали безпеки*, які «реєструють усі спроби входу в систему (як коректні, так і некоректні), а також створення, відкриття або видалення файлів, програм або інших об'єктів користувачем комп'ютера». Ці журнали подій можуть допомогти виявити IP-адресу, використану під час кіберзлочину.

Процес простеження у напрямі може бути тривалим. Час, необхідний на виконання цієї процедури, залежить від знань, навичок і здібностей виконавців злочину та заходів, які вони прийняли приховування своєї особистості та діяльності. Залежно від тактичних прийомів, використаних кіберзлочинцями для вчинення незаконних дій, відстеження може не призвести до єдиного джерела, що ідентифікується. Наприклад, це може спостерігатися в тих випадках, коли для скоєння кіберзлочину використовуються заражені шкідливою програмою комп'ютери-зомбі, або коли кілька зловмисників одночасно проводять розподілену атаку типу «відмова в обслуговуванні» (тобто DDoS-атаку) на систему або веб-сайт.

Адміністрація адресного простору Інтернет (Internet Assigned Numbers Authority, IANA) Інтернет-корпорації з присвоєння імен та номерів (ICANN), крім виконання інших завдань, керує розподілом IP-адрес серед Регіональних Інтернет-реєстратур, які відповідають за нагляд за реєстрацією IP-адрес у своїх регіонах. Існує п'ять Регіональних IP: Африканський мережевий інформаційний центр (AFRINIC); Азіатсько-Тихоокеанський мережевий інформаційний центр (APNIC); Американська реєстратура для числових абонентів Інтернету (ARIN); Латиноамериканський та Карибський мережевий інформаційний центр (LACNIC); та Координаційний центр європейської континентальної мережі (RIPE NCC). Регіональні IP надають інформацію про IP-адреси, організації,

пов'язані з IP-адресами, та контактну інформацію цих організацій (наприклад, адреси електронної пошти та номери телефонів).

Щоб визначити Інтернет-провайдера, пов'язаного з IP-адресою, слідчий у справах кіберзлочинності може використовувати сервіс WHOIS – інструмент ICANN для формування запитів. Регіональний IP надає доступ до сервісів WHOIS через свої веб-сайти. Дані WHOIS є реєстраційною інформацією, що надається фізичними особами, корпораціями, організаціями та урядами при реєстрації *доменних імен* (наприклад, gmail.com), яка включає імена та контактну інформацію (наприклад, номери телефонів, поштові адреси та адреси електронної пошти). Інструмент формування запитів WHOIS може використовуватися для визначення контактної інформації та місцезнаходження організації, пов'язаної з доменним ім'ям. Інструмент WHOIS також можна використовувати для визначення контактної інформації та місцезнаходження організації, пов'язаної з IP-адресою. Однак Загальний регламент Європейського союзу (ЄС) щодо захисту даних (GDPR), єдиний закон про захист даних, який набув чинності 25 травня 2018 року, який регламентує обробку, зберігання, використання даних та обмін даними в державах-членах ЄС та інших країнах, установах та приватних організаціях за межами ЄС, які надають товари та послуги ЄС та обробляють дані резидентів ЄС, вплинув на доступність даних WHOIS (зокрема, даних, які вважаються персональними даними відповідно до GDPR, для отримання додаткової інформації див.

Після того, як буде визначено Інтернет-провайдера, слідчі, які розслідують кіберзлочин, можуть зв'язатися з цим Інтернет-провайдером, пов'язаним з IP-адресою, щоб отримати інформацію про абонента, який використовує цю IP-адресу. Проте Інтернет-провайдерів не завжди можна змусити надавати особисту інформацію без відповідних юридичних документів, і в деяких випадках законодавство про недоторканність приватного життя/захисту персональних даних, що вже існує, може

забороняти видачу таких документів. Юридичний документ (наприклад, повістка до суду, ордер на обшук або судовий ордер), що використовується для отримання цієї інформації, варіюється в залежності від конкретної країни.

Чи знаєте ви?

WHOIS (англ. «хто це?») не є акронімом; «Це система, яка ставить питання: хто відповідає за доменне ім'я чи IP-адресу?».

Відмінності в положеннях законодавства різних країн у галузі кіберзлочинності, відсутність міжнародних стандартів щодо вимог щодо подання доказів (як з точки зору допустимості доказів у суді, так і з точки зору міжнародної відповідальності держави), механізмів надання взаємної правової допомоги у справах, пов'язаних з кіберзлочинністю і своєчасного збору, збереження цифрових доказів та обміну ними між країнами також є перешкодою для розслідування кіберзлочинів. Щодо деяких типів кіберзлочинів, особливо політично мотивованих кіберзлочинів, то спостерігається загальна відсутність волі країн до співробітництва у таких справах.

Слідчі, що розслідують кіберзлочини, також стикаються з проблемами технічного характеру. Наприклад, у багатьох цифрових пристроях використовуються патентовані операційні системи та програмне забезпечення, які вимагають застосування спеціалізованих інструментів для ідентифікації, збирання та збереження цифрових доказів: «Введення в цифрову криміналістику» для отримання додаткової інформації про цифрові докази, цифрові пристрої та інструменти цифрової криміналістики). Більш того, слідчі можуть не мати необхідного обладнання та інструментів цифрової криміналістики, необхідних для належного проведення розслідувань кіберзлочинів, що передбачають використання цифрових пристроїв.

До інших перешкод для розслідування кіберзлочинів можна віднести обмежені можливості правоохоронних органів щодо таких розслідувань. У

країнах, де існують національні спеціалізовані підрозділи, вони розслідують лише обмежену кількість випадків кіберзлочинів. Широке застосування інформаційно-комунікаційних технологій у розслідуваннях кримінальних злочинів робить таку практику неефективною. Підготовка співробітників національних правоохоронних органів, зайнятих у неспеціалізованих галузях поліцейської діяльності та нетехнічних спеціалізованих підрозділах (наприклад, у боротьбі зі злочинами, пов'язаними з наркотиками, організованою злочинністю, злочинами проти дітей), з питань кіберзлочинності, розслідувань, пов'язаних з ІКТ є одним із способів зміцнення національного потенціалу (УНЦ ООН, 2013. Крім того, ці обмежені можливості правоохоронних органів ще більше посилюються коротким терміном актуальності професійних знань слідчих у справах про кіберзлочини. Справа в тому, що інформаційно-комунікаційні технології безперервно розвиваються. Тому слідчі, що розслідують кіберзлочини, повинні навчатися протягом усього життя, постійно йти в ногу з розвитком технологій, не відставати від кіберзлочинців, знати їхні мотиви, цілі, тактичні прийоми та способи скоєння злочинів. Крім того, урядові та національні служби безпеки стикаються з проблемою так званого «витоку мізків», коли висококваліфіковані і досвідчені слідчі, що спеціалізуються на кіберзлочинах, звільняються з цих органів і переходять у приватний сектор, де їм пропонують вищу грошову винагороду за їх знання і здібності. Ці проблеми, пов'язані з потенціалом та кадровими ресурсами, мають бути уважно вивчені країнами, оскільки вони є серйозною перешкодою для розслідувань кіберзлочинів.

Управління знаннями

Концепція *управління знаннями* просувається як спосіб усунення перешкод, що виникають при розслідуванні кіберзлочинів, які пов'язані з кадровими та технічними ресурсами, а також знаннями, навичками та здібностями, необхідними для проведення цих розслідувань. Мета

управління знаннями полягає у «створенні, збереженні та застосуванні широкого спектру ресурсів знань, таких як люди та інформація», для покращення процесу або кінцевого результату.

Процес управління знаннями може застосовуватися – і вже застосовувався – до розслідувань кіберзлочинів. У контексті розслідувань кіберзлочинів, процес управління знаннями включає виявлення та оцінку потреб у знаннях для розслідування кіберзлочинів загального і спеціального характеру. Після виявлення та оцінки таких потреб визначаються та оцінюються знання відповідного органу в галузі кіберзлочинності. При порівнянні потреб у знаннях з поточним рівнем знань, які мають слідчі, визначаються прогалини у знаннях. Після виявлення прогалин у знаннях пропонуються заходи щодо їх усунення. Практичні методи управління знаннями можуть використовуватись для заповнення цих прогалин у знаннях.

Управління знаннями здійснюється за участю людей, які отримують, використовують, створюють знання, управляють та/або діляться ними, а також процесів та технологій, які сприяють управлінню знаннями. Обмін знаннями, що є невід'ємною частиною процесу управління знаннями у правоохоронній діяльності, відбувається за участю як зовнішніх сил, які *просувають* знання серед інших людей (наприклад, просвітницькі та інформаційні кампанії), так і внутрішніх факторів, які спонукають інших до отримання знань (чинники *тяжіння*), наприклад, до пошуку експертних знань або сприяння з того чи іншого питання.

Європол створив Dark Web Team (команду темної мережі), яка є прикладом такої форми обміну знаннями. Зокрема, Dark Web Team; обмінюється інформацією, надає оперативну підтримку та послуги фахівців у різних галузях злочинності і розробляє інструменти, тактичні прийоми та методи проведення розслідувань у темній мережі та виявлення найголовніших загроз та цілей. Ця команда також має на меті підвищення ефективності спільних технічних та слідчих заходів, організації ініціатив з

навчання та нарощування потенціалу одночасно з проведенням кампаній з профілактики та підвищення обізнаності в рамках всебічної стратегії боротьби зі злочинністю у темній мережі.

Процес управління знаннями також орієнтований на забезпечення доступу до знань та джерел знань (наприклад, до людей) для тих, хто їх потребує. Наприклад, Федеральне бюро розслідувань США створило команду кібердій (Cyber Action Team, CAT), що складається з групи кіберекспертів, яка може бути оперативно розгорнута в будь-якому місці в Сполучених Штатах протягом 48 годин для надання підтримки у розслідуванні справ, пов'язаних з кіберзлочинністю (FBI, nd.).

Існують два основні види знань, якими можна керувати та обмінюватися: явні знання та неявні знання (Dean, Filstad, and Gottschalk, 2006). *Явне знання* – це формальне знання, яке систематизується, документується і легко піддається ухвалі (наприклад, документи, судові справи, закони тощо). *Системи керування контентом*, які були створені для зберігання явних знань, можуть керувати знаннями про кіберзлочини та розслідування кіберзлочинів, роблячи їх доступними через веб-сайт та/або доступну для пошуку базу даних. Прикладом може бути портал управління знаннями Управління ООН з наркотиків та злочинності (УНЦ ООН або UNODC) – Поширення електронних ресурсів та законів про боротьбу зі злочинністю (SHERLOC). На цьому порталі розміщено довідник з компетентних національних органів (Довідник з КНВ), які уповноважені отримувати, розглядати та відповідати на прохання країн про надання допомоги з питань, що стосуються взаємної правової допомоги, а також база даних із прецедентного права, база даних про законодавство та бібліографічна база даних. УНЦ ООН також має репозиторій даних про кіберзлочинність, який включає бази даних по прецедентному праву, законодавству і висновкам, зробленим за підсумками розслідувань кіберзлочинів.

Також було створено національні системи управління контентом. Наприклад, у Литві було створено портал електронних послуг литовських судів, щоб забезпечити судовим органам доступ до бази даних судових рішень та цивільних справ. В Україні Єдиний державний реєстр судових рішень надає можливість доступу до всіх судових рішень та постанов, прийнятих у країні з 2006 року, і є доступною для пошуку базою даних з двома типами доступу: загальним (для всіх) та повним (для судових органів). Національні та міжнародні бази даних та репозиторії дозволяють окремим особам здійснювати пошук та отримувати явні знання, що зберігаються у цих базах даних, тим самим сприяючи обміну такими явними знаннями.

На відміну від явного знання, *неявне знання* – це ноу-хау, яке нелегко піддається визначенню та засноване на досвіді. Обмін неявними знаннями передбачає обмін цими знаннями через соціалізацію, найчастіше у неструктурованій формі. Неявними знаннями можна поділитись через наставництво, викладання та неформальне спілкування, а також під час програм навчання та семінарів. У деяких випадках міжнародні організації наголошують на обмін неявними знаннями. Наприклад, УНЦ ООН організовує підготовку прокурорів, слідчих та правоохоронців з питань збирання цифрових доказів та проведення розслідувань кіберзлочинів. Крім того, Глобальний інноваційний комплекс Інтерполу (The INTERPOL Global Complex for Innovation, IGCI) надає підтримку у проведенні транснаціональних розслідувань кіберзлочинів (наприклад, забезпечує координацію розслідувань кіберзлочинів та операцій по боротьбі з кіберзлочинністю), сприяє обміну оперативними даними між правоохоронними органами. Так само, як і УНЦ ООН, Глобальний інноваційний комплекс Інтерполу організує курси підготовки з питань розслідування кіберзлочинів та тенденцій у галузі кіберзлочинності (наприклад, проводить курси підвищення кваліфікації та розробляє навчальні програми, такі як програми навчання навичкам розслідування у

темній мережі), а експерти з Європолу, Євроюсту, Інтерполу та інших агентств діляться неявними знаннями про інструменти, тактичні прийоми та методи розслідування, які використовуються, наприклад, при проведенні розслідувань у темній мережі (Europol, 2018b). На національному рівні обмін неявними знаннями поки що не набув широкого поширення на практиці.

Засоби інформаційно-комунікаційних технологій (ІКТ), такі як програмне забезпечення спільної роботи для синхронної (тобто в режимі реального часу) та асинхронної взаємодії (наприклад, системи відео-конференц-зв'язку та спільного використання файлів) та інтерактивні робочі простори для спільної роботи (наприклад, документи Google, де учасники колективної роботи можуть обмінюватись завантаженими документами, редагувати та/або коментувати їх), можуть використовуватися для об'єднання людей з різних місць та здійснення обміну неявними знаннями. Незважаючи на зусилля з використання ІКТ для сприяння обміну неявними знаннями, ця практика не набула широкого поширення на міжнародному та національному рівнях. Наприклад, у 2017 році Литва повідомила, що «не існує механізму, що дозволяє здійснювати обмін інформацією та передовою практикою між прокурорами та суддями для забезпечення дієвого та ефективного судового переслідування у справах про кіберзлочинність».

Транснаціональний характер кіберзлочинності та взаємозалежність систем та цифрових пристроїв, підключених до Інтернету, в межах та за межами територій країн вимагають здійснення обміну інформацією про кіберзлочини між країнами. Крім того, необхідно здійснювати обмін знаннями про передові методи розслідування кіберзлочинів. Величезна кількість зацікавлених сторін, що беруть участь у розслідуваннях кіберзлочинів, вимагає вжиття скоординованих заходів реагування на кіберзлочини та обміну явними і неявними знаннями між усіма зацікавленими сторонами. Підходи до розслідування кіберзлочинів та

знання про розслідування варіюються залежно від зацікавлених сторін та конкретної країни, в якій вони проживають та/або провадять діяльність. Процеси управління цими знаннями всередині країни та за її межами необхідні для забезпечення ефективного розслідування кіберзлочинів на національному та міжнародному рівнях. Заходи, що передбачають використання інформаційно-комунікаційних технологій для полегшення обміну знаннями, мають першорядне значення, оскільки вони дозволяють обмінюватися явними та неявними знаннями незалежно від географічного розташування розповсюджувачів та одержувачів знань.

Вправа № 1 Кому ви будете дзвонити?

Дослідіть механізми звітності про кіберзлочини в Україні та дайте відповіді на наведені нижче запитання.

Питання для обговорення

Куди треба повідомити про кіберзлочин?

Чи були ви поінформовані про те, куди повідомляти про кіберзлочин? Якщо так, то коли і ким?

Чи проводяться національні просвітницькі та/або інформаційні кампанії щодо звітування про кіберзлочини в Україні? Чи було оцінено ці кампанії?

Вправа № 2 Гіпотетичне розслідування кіберзлочинів

Веб-сайт E-Bank був вимкнений, що перешкоджало клієнтам отримати доступ до веб-сайту. Вас найняли для проведення розслідування кіберзлочинів. Ви підозрюєте DDoS-атаку.

Питання для обговорення

З якими перешкодами ви можете зіткнутися під час розслідування?

Які кроки ви вживатимете, щоб спробувати встановити особу чи виконавців цього кіберзлочину?

Вправа №3 Хто відповідає?

Проведіть дослідження та визначити сторін, залучених до розслідування кіберзлочинів в Україні. Дайте відповіді на наведені нижче запитання.

Питання для обговорення

Хто розслідує кіберзлочини в Україні?

Яка роль кожної із сторін у розслідуванні кіберзлочинів?

Які кіберзлочини розслідують ці сторони?

Питання для самоперевірки

1. Куди повідомляють про кіберзлочинність?
2. Чому кількість кіберзлочинів знижується?
3. Хто розслідує кіберзлочини?
4. Що таке державно-приватне партнерство? Чому їх було створено для розслідування кіберзлочинів?
5. Які перешкоди виникають під час розслідування кіберзлочинів?
6. Що таке управління знаннями (knowledge management)? Які переваги управління знаннями?
7. Як можна застосувати управління знаннями до розслідувань кіберзлочинів?

Лекція 6. Практичні аспекти цифрової криміналістики.

- 6.1. Правові та етичні обов'язки.
- 6.2. Правила поведінки з цифровими доказами.
- 6.3. Допустимість цифрових доказів.

6.1. Правові та етичні зобов'язання

Слідчі, що розслідують кіберзлочини, та фахівці з цифрової криміналістики повинні враховувати правові та етичні аспекти при розслідуванні кіберзлочинів, обробці, аналізі та тлумаченні цифрових доказів та поданні результатів. У той час як правові зобов'язання наказуються національними, регіональними та міжнародними нормами права, етичні зобов'язання (в усіх застосовних випадках) накладаються добровільно та/або встановлюються державними органами та/або приватними професійними організаціями.

У випадках, коли існує *кодекс етики* (тобто керівні принципи, які визначають правильну і неправильну поведінку в процесі прийняття рішень), він часто включає опис того, що слідчі у справах про кіберзлочини та /або фахівці з цифрової криміналістики *повинні робити* у всіх випадках, і що вони *ніколи не повинні робити* за жодних обставин.

Наприклад, Міжнародне суспільство судових експертів з комп'ютерів (*International Society of Forensic Computer Examiners, ISFCE*) прийняло кодекс етики, якого повинні дотримуватися його члени, щоб забезпечити дотримання стандартів, а також точність та достовірність результатів цифрової судової експертизи. Цей кодекс етики включає опис видів поведінки, якого повинні дотримуватися члени суспільства (наприклад, дотримання законних розпоряджень і проведення всебічного дослідження доказів відповідно до чинних законів, стандартів, процедур і керівних принципів), і заборонених видів поведінки (наприклад, приховування

доказів, упередженість при аналізі або поданні доказів та подання свідомо неправдивих відомостей про свою кваліфікацію).

6.2. Правила поведінки з цифровими доказами

Чи знаєте ви? У приватному секторі заходи реагування на інциденти, пов'язані з кібербезпекою (наприклад, розподілена атака типу «відмова в обслуговуванні», несанкціонований доступ до систем або витік даних), включають конкретні процедури, яким необхідно слідувати, щоб локалізувати інцидент, пов'язаний з кібербезпекою, розслідувати та/або усунути його (Cyber Security Coalition, 2015). Існують два основні способи дій у разі виникнення інцидентів, пов'язаних з кібербезпекою: швидке відновлення; збір доказів. Перший підхід, що забезпечує швидке відновлення, передбачає локалізацію інциденту з метою мінімізації шкоди, а не збереження та/або збирання даних. Оскільки основна увага приділяється задачі швидкого реагування та відновлення, суттєво важливі докази можуть бути втрачені. Другий підхід передбачає відстеження інциденту, пов'язаного з кібербезпекою, та використання додатків, призначених для проведення цифрової судової експертизи, з метою збирання доказів та інформації про інцидент. Оскільки основний акцент робиться на збиранні доказів, відновлення після інциденту, пов'язаного з кібербезпекою, відкладається. Ці підходи є для приватного сектора єдино можливими. Підхід, який використовується приватним сектором, варіюється в залежності від конкретної організації та її пріоритетів.

Цифрові докази є нестійкими та недовговічними, і неналежне поводження з такими доказами може призвести до їхньої зміни. У зв'язку з нестійкістю та недовговічністю доказів необхідно дотримуватись протоколів, щоб не допустити зміни даних у процесі поводження з ними (тобто під час отримання доступу до даних, їх збору, пакування, передачі та зберігання). У цих протоколах описуються дії, які слід виконувати при поводженні з цифровими доказами. Початковий процес поводження з

цифровими доказами складається з чотирьох етапів: ідентифікація, збирання, отримання та збереження (лекція 4).

Існують протоколи для збору *нестійких доказів*. Збір нестійких доказів повинен здійснюватися в порядку зростання ступеня стійкості, тобто насамперед слід збирати докази з найменшим ступенем стійкості, а докази з найбільшим ступенем стійкості слід збирати в останню чергу. У документі під назвою «Запит коментарів (RFC) 3227» (Request for Comments, RFC, 3227) наведено наступний приклад порядку збору нестійких даних (від найменш стійких до найбільш стійких) для стандартних систем:

- реєстри, кеш;

- таблиця маршрутизації, кеш протоколу визначення адреси (*Address Resolution Protocol, ARP*), таблиця процесів, ядро (статистика), пам'ять (ОЗП);

- системи для тимчасових файлів;

- диск;

- дані видаленого журналу та дані моніторингу, що стосуються досліджуваної системи;

- фізична конфігурація, топологія мережі;

- архівний носій даних.

Ідентифікація

На етапі ідентифікації до початку збору цифрових доказів необхідно отримати попередню інформацію про скоєний кіберзлочин. Ця попередня інформація схожа на ту, яка збирається під час традиційного кримінального розслідування. Слідчий намагається відповісти на такі питання.

- Хто причетний до кіберзлочину?

- Що сталося?

- Коли було скоєно кіберзлочин?

- Де було скоєно кіберзлочин?

Як було скоєно кіберзлочин?

Відповіді на ці питання підкажуть слідчим, з чого слід розпочати розслідування справи. Наприклад, у відповідь питання: «Де було скоєно кіберзлочин?», тобто чи була вона скоєна на території країни або за її межами (лекція 3) – допоможе слідчому зрозуміти, як слід розслідувати цю справу (наприклад, які органи слід залучити до участі та/або з ким слід встановити зв'язок).

На етапі ідентифікації слідчі у справах про кіберзлочини використовують велику кількість традиційних методів розслідування (див. посібник УНП ООН).

Робота поліції: Розслідування злочинів для ознайомлення з докладним аналізом цих методів), особливо на етапі збирання інформації та доказів. Наприклад, з метою збирання інформації та доказів розслідуваного кіберзлочину проводиться допит жертв, свідків та підозрюваних (лекція 9).

Правоохоронні органи також проводять негласні розслідування з метою встановлення особи, розшуку та кримінального переслідування кіберзлочинців (приклади таких розслідувань у лекціях 12 та 13). Крім того, слідчі, які розслідують кіберзлочин, проводять приховане спостереження. Таке спостереження є «високо інтрузивним методом збору доказів. Використання прихованого (негласного) спостереження потребує ретельного балансу між правом підозрюваного на приватне життя та необхідністю розслідувати тяжкі злочини. Положення про приховане спостереження мають повністю враховувати права підозрюваного. Міжнародні органи та суди з прав людини ухвалили низку рішень про неприпустимість негласного спостереження та його параметри, які мають виконуватись». Правоохоронні органи навіть використовують шкідливі програми для здійснення спостереження з метою збирання інформації про кіберзлочин та докази його скоєння. Наприклад, правоохоронні органи США використовують методику проведення слідчих дій у комп'ютерних

мережах (networks investigation technologies, NIT) – «спеціально розроблені експлойти або шкідливі програми» – у своїх розслідуваннях справ, пов'язаних із сексуальною експлуатацією дітей та сексуальним насильством над дітьми в мережі Інтернет.

Перш ніж розпочати збір цифрових доказів, слідчий повинен визначити типи доказів, що шукаються. Цифрові докази можна знайти у цифрових пристроях, таких як комп'ютери, зовнішні жорсткі диски, *флеш-накопичувачі*, маршрутизатори, смартфони, планшети, камери, «розумні» телевізори, побутові прилади з виходом в Інтернет (наприклад, холодильники та пральні машини), ігрові приставки (і багато інших), а також на загальнодоступних ресурсах (наприклад, платформи соціальних мереж, веб-сайти та дискусійні форуми) та приватні ресурси (наприклад, журнали інтернет-провайдерів про активність користувачів; ділові документи провайдерів комунікаційних послуг; журнали провайдерів хмарного зберігання з реєстрацією активності користувачів та матеріалів користувача). Багато програм, веб-сайтів та цифрових пристроїв використовують сервіси хмарного зберігання. Таким чином, дані про користувачів можуть зберігатися повністю або у вигляді фрагментів різними провайдерами на серверах у кількох місцях. Тому завдання отримання даних від цих провайдерів є здійсненним. Тип доказів, що шукаються, залежить від розслідуваного кіберзлочину. Якщо розслідуваний кіберзлочин є шахрайство з використанням персональних даних, то на цифрових пристроях, що вилучаються, буде проводитися пошук доказів цього злочину (наприклад, доказів шахрайських транзакцій).

Збір

При розслідуванні кіберзлочину місце злочину не обмежується фізичним місцем розташування цифрових пристроїв, які використовувалися для вчинення кіберзлочину та/або були метою кіберзлочинців. Місце скоєння кіберзлочину також включає цифрові

пристрої, які можуть містити цифрові докази, і охоплює кілька цифрових пристроїв, систем і серверів.

У випадках, коли спостерігається факт скоєння кіберзлочину, надходить повідомлення про кіберзлочин та/або є підозра у скоєнні кіберзлочину, вживаються заходи щодо охорони місця злочину. Особа, яка приймає перші заходи у відповідь, визначає місце злочину, захищає його від забруднення і забезпечує збереження нестійких доказів, ізолювавши користувачів від усіх цифрових пристроїв, виявлених на місці злочину (наприклад, перемістивши їх в окреме приміщення або місце). Користувачі повинні бути позбавлені можливості подальшого використання цифрових пристроїв. При цьому ні особа, яка приймає перші заходи у відповідь, ні слідчий не повинні звертатися за допомогою до будь-якого користувача в процесі обшуку та документування. Слідчий, якщо він не є особою, яка приймає перші заходи у відповідь, обшукує місце злочину та ідентифікує докази.

На початок збору доказів місце злочину документується. *Документування* є необхідним протягом усього процесу розслідування (до, під час та після отримання доказів). Документація повинна включати докладну інформацію про зібрані цифрові пристрої, у тому числі про робочий стан пристрою, чи було воно увімкнено, вимкнено або знаходилося в режимі очікування, і його фізичні характеристики, такі як марка, модель, серійний номер, з'єднання, будь-які відмітні знаки або пошкодження.

На додаток до письмових нотаток, для документування місця злочину та доказів необхідні також схеми, фотографії та/або відеозаписи місця злочину та доказів.

Примітка:

Збір нестійких даних може змінити вміст пам'яті цифрових пристроїв та дані всередині них.

Слідчий чи експерт-криміналіст збирає докази. Процедури варіюються залежно від типу цифрового пристрою, а також загальнодоступних та приватних ресурсів, де знаходяться цифрові докази (наприклад, комп'ютери, телефони, соціальні мережі та хмарне сховище; для ознайомлення з різними практичними методами цифрової судової експертизи мультимедійних, виду та мобільних пристроїв). Правоохоронні органи використовують *стандартні оперативні процедури*, в яких докладно описуються дії, які необхідно виконати при поводженні з цифровими доказами на мобільних пристроях, об'єктах з виходом в Інтернет (наприклад, годинник, фітнес-монітори) та побутові прилади), хмарному сховищі та платформах соціальних мереж.

Стандартна оперативна процедура (СОП) призначена для надання допомоги слідчим, оскільки в ній описуються методи та послідовність дій, яких слід дотримуватись при розслідуванні кіберзлочину таким чином, щоб забезпечити допустимість зібраних доказів у суді; у ній також описуються інструменти та інші ресурси, необхідних проведення розслідування. Таким чином, СОП включає опис процедур, яких необхідно дотримуватися під час проведення розслідування.

Необхідно визначити унікальні обмеження, з якими можуть зіткнутися слідчі під час розслідування. Наприклад, при розслідуванні кіберзлочину слідчі можуть мати справу з безліччю цифрових пристроїв, операційних систем та складних мережевих конфігурацій, що вимагатиме наявності спеціальних знань, зміни у процедурах збору доказів та сприяння у виявленні з'єднань між системами та пристроями (наприклад, топології мереж). Під час розслідування слідчий може також стикатися з методами *антикриміналістики* (лекція 4), такими як *стеганографія* (тобто приховування секретних даних, коли вміст повідомлення приховується та робиться невидимим) та *шифрування* (тобто «фізичне блокування доступу третіх сторін до файлу»), шляхом використання пароля або шляхом приведення файлу або елементів файлу в непридатний для використання

стан». Тому слідчий має бути готовий до таких ситуацій і мати у своєму розпорядженні необхідні людські та технічні ресурси, потрібні для усунення цих обмежень. Дії, які вживаються слідчим у таких випадках (наприклад, здатність слідчого отримати паролі до цих пристроїв та/або розшифрувати файли), якщо вони взагалі робляться, залежать від національних законів. Інструменти цифрової криміналістики можуть бути корисними в таких ситуаціях і допомогти, наприклад, виявити стеганографію та розшифрувати файли, а також виконати інші важливі завдання цифрової судової експертизи.

Приклади таких інструментів включають програмні забезпечення для проведення комп'ютерних експертиз, такі як Forensic Toolkit (FTK) виробництва компанії AccessData, Volatile Framework, X-Ways Forensics. Поряд з цими ресурсами необхідний комплект криміналістичних інструментів, який включає предмети, що використовуються для документування місця злочину, інструменти, необхідні для розбирання пристроїв та видалення інших видів доказів з місця злочину, а також матеріали, необхідні для маркування та пакування доказів (наприклад, для транспортування смартфонів використовуються екрануюча сумка Фарадея, яка блокує прийом та передачу бездротових сигналів цифровим пристроєм, і зарядний пристрій живлення), та інші інструменти.

Процес збору доказів передбачає збереження нестійких доказів і відключення живлення цифрових пристроїв. Робочий стан виявлених цифрових пристроїв визначає процедури збирання доказів. Наприклад, якщо комп'ютер увімкнено, нестійкі докази (наприклад, часові файли, регістр, кеш, стан мережі, з'єднання тощо) зберігаються до вимкнення живлення та вилучення комп'ютера.

Якщо пристрій вимкнено, він залишається у вимкненому стані та вилучається.

Існують обставини, за яких цифрові пристрої не можуть бути вилучені (наприклад, через розмір та/або складність систем та/або

конфігурацій їх апаратного та програмного забезпечення, оскільки ці системи забезпечують критично важливі послуги). У таких ситуаціях нестійкі та стійкі дані збираються за допомогою спеціальних процедур, які вимагають *збору даних у реальному часі*.

Тип цифрового пристрою, з яким має справу слідчий під час розслідування, також визначає спосіб збору цифрових доказів.

Чи знаєте ви?

Для отримання нестійких даних із систем, що у робочому стані, можуть використовуватися спеціальні команди. Наприклад, для операційних систем Windows *ipconfig* використовується для отримання інформації про мережу, тоді як для операційних систем Unix використовується команда *ifconfig*. І для Windows, і для Unix *netstat* використовується для отримання інформації про активні мережеві з'єднання.

Крім цифрових пристроїв також необхідно зібрати інші предмети, що стосуються справи (наприклад, нотатки та/або записні книжки, які можуть містити паролі або іншу інформацію про мережні облікові дані, телефони, факсимільні апарати, принтери, маршрутизатори тощо).

Дії, які вживаються слідчим під час збирання доказів, повинні документуватися. Кожен пристрій повинен бути промаркований (разом зі сполучними кабелями та мережевими шнурами), упакований та відправлений до лабораторії цифрової судової експертизи. Після транспортування предметів до лабораторії, вони «інвентаризуються, реєструються і передаються на зберігання в приміщення, що закривається, захищене від екстремальних температур, вологості, пилу та інших можливих забруднювачів».

Отримання

Існують різні методи одержання доказів. Метод, що використовується, залежить від типу цифрового пристрою. Наприклад, процедура отримання доказів жорсткого диска комп'ютера відрізняється

від процедури, необхідної для отримання цифрових доказів з мобільних пристроїв, таких як смартфони.

Крім випадків, коли здійснюється збір даних у реальному часі, докази вилучаються із вилучених цифрових пристроїв у лабораторії судової експертизи (тобто здійснюється *збір даних у статичному режимі*). У лабораторії судової експертизи цифрові докази мають бути отримані таким чином, щоб зберегти *цілісність* доказів (забезпечити, щоб дані залишилися без змін), тобто *надійним з погляду криміналістики* способом. Для цього інструменти та методи, що використовуються для отримання цифрових доказів, повинні запобігати зміні даних або, коли це неможливо, принаймні мінімізувати зміни. Використовувані інструменти та методи мають бути обґрунтованими та надійними. Перш ніж використовувати ці інструменти та методи, необхідно визначити та врахувати межі їх можливостей. Національний інститут стандартів і технологій США має доступну для пошуку базу даних інструментів цифрової криміналістики, де описуються інструменти з різними функціональними можливостями (наприклад, інструменти для судової експертизи хмарних сховищ тощо).

Чи знаєте ви?

Сортування, тобто перевірка властивостей та вмісту потенційних джерел даних, може проводитися, щоб зменшити обсяг даних, що збираються, щоб уникнути отримання даних, які не мають відношення до справи, або дотриматися обмеження повноважень щодо виробництва обшуку.

Вилучені цифрові пристрої є основним джерелом доказів. Експерт із цифрової криміналістики отримує дані не з первинного джерела. Натомість створюється дублікат вмісту цього пристрою, і експерт працює з копією. Дублікат вмісту цифрового пристрою створюється (такий процес називається *створенням неспотвореного образу*) до початку збору даних у статичному режимі для збереження цілісності цифрових доказів. Для того щоб визначити, чи дублікат є точною копією оригіналу, значення

криптографічної хеш-функції розраховується з використанням математичних обчислень; якщо значення хеш-функції для оригіналу та копії збігаються, то вміст копії є дзеркальним відображенням (тобто дублікатом) вмісту оригіналу. *Блокувальник запису*, який призначений для запобігання зміні даних у процесі копіювання, слід використовувати до вилучення даних у всіх випадках, коли це можливо, щоб не допустити змін даних під час копіювання. Важливо, що описаний вище процес отримання даних застосовується в основному до комп'ютерів. При отриманні даних з мобільних телефонів та схожих з ними пристроїв, де пам'ять не може бути фізично відокремлена від пристрою для створення неспотвореного образу, застосовується інша процедура.

Існують два способи вилучення даних: фізичне та логічне. *Фізичне вилучення* передбачає пошук та отримання доказів з такого місця в цифровому пристрої, де зберігаються докази, наприклад, жорсткого диска комп'ютера. Фізичне вилучення може здійснюватися шляхом використання *пошуку за ключовими словами* (на основі термінів, наданих слідчим), методу *вичленування однорідних масивів даних* (тобто пошуку «на основі верхніх і нижніх колонтитулів та інших ідентифікаторів») та шляхом вивчення нерозподіленого простору (тобто «простору в системі, що є вільним, тому що він ніколи не використовувався, або тому що інформація з нього була видалена») та розділів, які відокремлюють сегменти жорсткого диска один від одного. *Логічне вилучення* передбачає пошук та отримання доказів з місця, в якому вони «перебувають щодо файлової системи комп'ютерної операційної системи, яка використовується для відстеження імен та розташування файлів, які зберігаються на носії даних, такому як жорсткий диск». Спосіб логічного вилучення залежить від цифрового пристрою, файлової системи, програм на пристрої та операційної системи. *Логічне вилучення* передбачає отримання даних з активних та віддалених файлів, файлових систем, нерозподіленого та

невикористовуваного простору, а також стислих, зашифрованих та захищених паролем даних.

Примітка

Логічне вилучення файлів може призвести до втрати *метаданих* (тобто даних про дані).

Весь процес отримання доказів має документуватись. При цьому документація повинна включати докладну інформацію про цифрові пристрої, з яких були вилучені докази, апаратне та програмне забезпечення, використане для отримання доказів, способі, за допомогою якого були отримані докази (тобто про те, як вони були отримані), а також про те, коли, де і чому вони були отримані, які докази були отримані і чому вони були отримані.

Збереження

Мета збереження доказів полягає у захисті цифрових доказів від змін. Цілісність цифрових доказів повинна зберігатись на кожному етапі поводження з цифровими доказами (ISO/IEK 27037). Особи, які вживають перші заходи у відповідь, слідчі, експерти-техніки, що вивчають місце злочину, та/або експерти з цифрової криміналістики повинні по можливості продемонструвати, що цифрові докази не були змінені на етапі ідентифікації, збору та отримання. Вочевидь, що здатність продемонструвати це залежить від цифрового пристрою (наприклад, комп'ютера та мобільних телефонів) та обставин, з якими вони стикаються (наприклад, необхідність швидкого збереження даних). Для цього необхідно підтримувати *систему охорони доказів*. *Система охорони доказів* – це «процес, з якого слідчі забезпечують збереження місця злочину (чи обставини) і доказів протягом усього періоду провадження у справі. До журналу реєстрації вноситься інформація про те, хто здійснював збір доказів, де і яким чином вони були зібрані, які особи отримали ці докази, і коли вони їх одержали». У документах, що ведуться в системі охорони доказів, необхідно вказувати імена, посади та контактну

інформацію осіб, які ідентифікували, зібрали та отримали докази, а також будь-яких інших осіб, кому було передано докази, докладну інформацію про докази, які були передані цим особам, час і дату передачі, а також про мету передачі.

Аналіз та звітність

На додаток до етапу поводження з цифровими доказами, процес цифрової судової експертизи також передбачає вивчення та тлумачення цифрових доказів (етап *аналізу*) та подання результатів аналізу (етап *звітності*). На етапі *аналізу* цифрові докази витягуються із пристрою, дані аналізуються, а події реконструюються. До початку аналізу цифрових доказів експерт з цифрової криміналістики в лабораторії повинен бути поінформований про цілі пошуку та отримати деякі відомості довідкового характеру про справу, що розслідується, та будь-яку іншу інформацію, отриману в ході розслідування, яка може допомогти експерту-криміналісту на цьому етапі (наприклад, IP- адресу або MAC-адреси). Застосовуються різні види аналізу в залежності від типу шуканого цифрового доказу, наприклад, аналіз мережі, файлової системи, програми, відеоматеріалів, зображень і носія (тобто аналіз даних у пристрої).

Файли аналізуються для встановлення їх походження, а також визначення того, коли і де ці дані були створені, змінені, коли і звідки відбувалося звернення до них, коли і де вони були завантажені або вивантажені, і для визначення можливого підключення цих файлів, що знаходяться в пам'яті пристрою, наприклад, до віддаленого сховища, такого як хмарне сховище. Тип цифрових доказів (наприклад, електронні листи, текстові повідомлення, геолокація, документи текстового редактора, зображення, відео та журнали чату) залежить від конкретного виду кіберзлочину.

Існують чотири основні типи аналізу, які можуть бути виконані на комп'ютерах: аналіз часових рамок; аналіз власності та володіння; аналіз додатків та файлів; та аналіз методу приховування даних.

Ціль *аналізу часових рамок* полягає у створенні часової шкали або часової послідовності дій з використанням міток часу (дати та часу), які призвели до події, або у встановленні часу та дати, коли користувач здійснив певну дію. Такий аналіз проводиться з метою співвіднесення злочину з його виконавцем чи, як мінімум, співвіднесення діяння, що призвело до злочину, з конкретною особою; однак є певні труднощі, пов'язані з перевіркою результатів аналізу часових рамок.

Аналіз власності та володіння використовується для встановлення особи, яка створила файли в комп'ютерній системі, отримала доступ до них та/або змінила їх. Наприклад, такий аналіз може допомогти виявити матеріали зі сценами сексуального насильства над дітьми (тобто «будь-яке зображення дитини, що робить реальні або змодельовані відверто сексуальні дії, або будь-яке зображення статевих органів дитини головним чином в сексуальних цілях» на пристрої підозрюваного. Однієї інформації недостатньо, щоб довести, хто є власником матеріалів зі сценами сексуального насильства над дітьми. Для цього потрібні додаткові докази, такі як факт виняткового користування комп'ютером, на якому було виявлено матеріали.

Аналіз додатків та файлів виконується для дослідження додатків та файлів у комп'ютерній системі, щоб встановити обізнаність, наміри та можливості злочинця щодо кіберзлочину (наприклад, ярлик або ім'я файлу можуть вказувати на вміст файлу; зокрема, ім'я файлу може виявитися іменем жертви кіберзлочину).

Примітка

Дані мітки можуть бути змінені. Тому не можна робити висновок на основі лише цих доказів. Те саме стосується й інших даних. Наприклад, історія відвідувань у веб-браузері показує, що за сайти відвідувалися і скільки разів вони відвідувались. Необхідні додаткові докази, щоб показати, що особа, чиї цифрові докази використовувалися для доступу до

цих веб-сайтів, була власником та/або передбачуваним користувачем пристрою.

Можна також використовувати *аналіз методу приховування даних*. Як випливає з назви, аналіз методу приховування даних передбачає пошук схованих даних в системі. Злочинці використовують кілька методів приховування даних, щоб приховати свою протиправну активність та інформацію, що ідентифікує, наприклад, шляхом використання методу шифрування. На цьому етапі аналізу слідчому необхідно визначити методи приховування даних, які злочинці могли використовувати для приховування своєї особи та діяльності. Приховані дані можуть допомогти розкрити інформацію про скоєння злочину, про власника контенту або намір вчинити злочин.

Видалені файли

Коли файл видаляється, він переміщується в кошик. Якщо кошик очищується (наприклад, видалення вмісту), видалені файли видаляються з *таблиці розміщення файлів*, яка архівує імена файлів та їх розташування на жорстких дисках. Простір, в якому знаходиться файл, позначається як вільний простір (тобто нерозподілений простір) після його видалення, проте файл все ще знаходиться в цьому просторі (принаймні, доки він не буде повністю або частково зайнятий новими даними).

Національний інститут правосуддя США дійшов висновку, що «власними силами результати, отримані за підсумками виконання будь-якого з цих типів аналізу, що неспроможні вважатися достатніми для виведення укладання. Однак зв'язки між окремими результатами, якщо їх розглядати загалом, можуть дати повнішу картину».

Метою цих типів аналізу є *реконструкція злочину* (чи реконструкція подій). *Реконструкція подій* проводиться для того, щоб встановити, *хто* несе відповідальність за подію, *що* сталося, *де* сталася ця подія, *коли* вона сталася і *як* вона розвивалася, шляхом ідентифікації, зіставлення даних (для розкриття «загальної картини» або суті події). Процес реконструкції

подій може включати *тимчасовий аналіз* (тобто встановлення часу і послідовності подій), *реляційний аналіз* (тобто визначення учасників подій, їх дій, а також зв'язків і відносин між ними) і *функціональний аналіз* (тобто оцінка продуктивності та можливостей систем та пристроїв, задіяних під час подій). Загалом реконструкція події проводиться для того, щоб довести чи спростувати робочу гіпотезу щодо будь-якого випадку (тобто обґрунтованого припущення щодо послідовності дій, що призвели до події).

Примітка

Слідчі повинні брати участь у попередніх заходах щодо реконструкції подій на етапах ідентифікації та збору доказів. Виконання цих завдань допоможе слідчим виявити нові потенційні джерела цифрових доказів.

Зрештою, для реконструкції подій на етапі аналізу використовуються неповні знання для виведення висновків щодо справи, що розслідується, на основі наявних доказів і результатів аналізу цих доказів. Тому важливо, щоб слідчі, що розслідують кіберзлочин, і експерти з цифрової криміналістики визнавали такі обмеження і уникали упереджених тлумачень результатів аналізу, наприклад, тлумачень, які є наслідком упередженості підтвердження, коли люди *шукають* і підтримують результати, які підтверджують їх, і які суперечать їхній робочій гіпотезі.

Результати аналізу документуються у звіті. Звіти мають бути максимально чіткими та точними. Вони повинні включати ілюстративні матеріали (наприклад, малюнки, графіки, вихідні дані інструментів) та допоміжні документи, такі як документація системи охорони доказів, а також докладне роз'яснення використаних методів та дій, що вживаються для дослідження та вилучення даних. Результати повинні роз'яснюватися з урахуванням цілей аналізу (тобто мети розслідування та справи, що розслідується). Інформація про обмеженість отриманих результатів також має бути включена до звіту. Зміст звіту варіюється в залежності від

юрисдикції та національної політики (якщо така є) щодо розслідувань та цифрової криміналістики. Щоб уникнути неправильного тлумачення або визначення неправильного вагового значення цифрових доказів, у звіті має бути сказано про відомі помилки та невизначеність результатів.

6.3.Допустимість цифрових доказів

Для забезпечення допустимості цифрових доказів у суді мають бути дотримані певні правові та технічні вимоги. Щодо правових вимог, то суд розглядає такі питання, як наявність законного дозволу на проведення обшуку та вилучення пристроїв інформаційно-комунікаційних технологій та пов'язаних з ними даних, а також відносність до справи, справжність, цілісність та достовірність цифрових доказів. При розгляді питання відповідності технічним вимогам суд критично оцінює процедури та інструменти цифрової криміналістики, використані для вилучення, збереження та аналізу цифрових доказів; лабораторії цифрової судової експертизи, у яких проводяться аналізи; звіти експертів з цифрової криміналістики; та академічні та професійно-технічні кваліфікації експертів з цифрової криміналістики та свідків-експертів (якщо це необхідно). У 2017 році Антві-Боасіако (Antwi-Boasiako) та Вентер (Venter) розробили структуру під назвою *Уніфікована модель оцінки допустимості цифрових доказів (Harmonized) Model for Digital Evidence Admissibility Assessment (HM-DEAA)*, яка включає основні технічні та юридичні вимоги, що визначають допустимість доказів. Зокрема, модель HM-DEAA передбачає три етапи для оцінки допустимості доказів, включаючи етапи оцінки, розгляду та ухвалення рішення щодо допустимості цифрових доказів. Модель HM-DEAA описується в наступному розділі даного модуля, щоб детально проілюструвати правові та технічні вимоги, які широко використовуються у різних юрисдикціях для забезпечення допустимості цифрових доказів у національних судах.

Оцінка цифрових доказів

На цьому етапі суди визначають, чи були використані належні законні дозволи на проведення обшуку та вилучення пристроїв інформаційно-комунікаційних технологій (ІКТ) та пов'язаних із ними даних. До законних дозволів належать ордер на обшук, розпорядження суду чи повістка до суду. Тип юридичного документа, необхідний для вилучення пристроїв ІКТ та пов'язаних з ними даних, варіюється залежно від юрисдикції та визначається національним законодавством. Однак у більшості країн для вилучення пристроїв ІКТ як такий юридичний документ переважно використовується ордер на обшук. Проте, національні закони різних країн різняться щодо вимог до законних розпоряджень залежно від обставин справи, обставин, у яких проводяться обшук та вилучення, та повноважень осіб, які проводять обшук.

У цьому етапі також оцінюється значимість цифрових доказів з погляду криміналістики. *Значимість з погляду криміналістики* визначається тим, чи можуть цифрові докази: встановити чи виключити зв'язок між злочинцем і його мішенню (наприклад, жертвою, цифровим пристроєм, веб-сайтом тощо) та/або місцем злочину (місцем, де було скоєно злочин або кіберзлочин); підтвердити або спростувати свідчення злочинця, потерпілого та/або свідка; встановити особу виконавця (виконавців) кіберзлочину; дозволити висунути слідчі версії; забезпечити отримання інформації про спосіб дій (спосіб скоєння злочину, використаному злочинцем (тобто про звички, методи та особливості поведінки злочинця); і показати, що злочин дійсно мав місце (вказати на склад злочину (*corpus delicti*)).

Чи знаєте ви?

Цифрові докази можуть допомогти виявити характерні ознаки поведінки (почерк) кіберзлочинців, таких як розробники шкідливих програм та хакери. *Почерк злочинця* – це розпізнаваний і помітний характер діяльності (наприклад, конкретні методи, інструменти та прізвисько), який можна віднести на рахунок конкретного джерела, і який

забезпечує кіберзлочинцю певне психологічне чи емоційне задоволення (наприклад, схвалення та визнання з боку колег).

Розгляд цифрових доказів

На цьому етапі оцінюється цілісність цифрових доказів шляхом вивчення процедур та інструментів цифрової судової експертизи, використаних для отримання доказів, компетенції та кваліфікації експертів з цифрової криміналістики, які отримали, зберегли та проаналізували цифрові докази та лабораторій цифрової судової експертизи, де розглядалися та досліджувалися. По суті, мета такої оцінки полягає в тому, щоб визначити, чи використовувалися наукові принципи для збереження, отримання та аналізу цифрових доказів, і чи дотримувалися стандарти при поводженні з цифровими доказами та їх дослідженні (наприклад, чи були атестовані інструменти цифрової криміналістики, чи були атестовані). вони сучасними, чи підтримувалися вони у справному стані і чи випробовувалися перед використанням, щоб забезпечити їх належне функціонування).

Експерти з цифрової криміналістики дають свідчення в суді, щоб розповісти про свою кваліфікацію та роз'яснити такі питання: як працюють цифрові пристрої, Інтернет-платформи та інші джерела, пов'язані з ІКТ; процес цифрової судової експертизи; чому використовувався той чи інший інструмент цифрової криміналістики, а не інші інструменти; яким чином було збережено, отримано та проаналізовано цифрові докази; тлумачення результатів проведеного аналізу та точність цих тлумачень; та будь-які зміни даних, які мали місце, і чому вони мали місце.

Крім того, оцінюється кваліфікація експертів з цифрової криміналістики, щоб встановити компетенцію осіб, які поводяться з цифровими доказами та аналізують їх. Така компетенція має важливе значення для забезпечення якості результатів роботи та зміцнення довіри до цих результатів. Однак при цьому немає жодних універсальних стандартів компетенцій для експертів з цифрової криміналістики. Вимоги

до кваліфікації експертів у галузі цифрової криміналістики варіюються залежно від конкретної країни. У деяких випадках сертифікація експертів у галузі цифрової криміналістики є обов'язковою, в інших випадках вона не потрібна; це залежить від юрисдикції (УНЗ ООН, 2013). Таким чином, на цьому етапі оцінюється, чи мають експерти необхідну кваліфікацію, щоб виступати як свідок-експерт та/або проводити необхідне дослідження пристроїв ІКТ та пов'язаних з ними даних. Крім того, визначається, чи були підтверджені та перевірені компетенції цих експертів та аналітиків.

Чи знаєте ви?

База даних Daubert Tracker, що отримала таку назву на честь справи *Daubert v. Merrell Dow Pharmaceuticals Inc.* (1993), містить критерії, які використовують суди США для визначення надійності судової експертизи або достовірності доказів, що пред'являються в суді, та відстежує судові справи, опубліковані та не опубліковані у збірниках судових рішень, при розгляді яких були оскаржені методи, використані експертами, та їх кваліфікація.

Також вивчаються стандарти та протоколи лабораторії цифрової судової експертизи, щоб визначити компетентність лабораторії, необхідну для поводження з цифровими доказами та їх аналізу та отримання достовірних результатів. Зокрема, оцінюється, «чи лабораторія використовує надійні методи, належне обладнання та програмне забезпечення, компетентний персонал, і чи виводить вона обґрунтовані висновки». Виконанню такої оцінки може сприяти акредитація, яка є «інструментом для підвищення якості, оцінки ефективності роботи, проведення незалежної експертизи діяльності, дотримання встановлених стандартів та служить справі заохочення, стимулювання та підтримання найвищих стандартів практики судової експертизи». Незважаючи на те, що стандарт ISO/IEC 17025 «прийнятий з метою стандартизації лабораторій у всьому світі з точки зору результатів випробувань, контролю якості та калібрування», його підтримують не всі учасники співтовариства експертів

з цифрової криміналістики. Крім того, хоча акредитація забезпечує необхідні механізми нагляду та підзвітності для забезпечення дотримання стандартів практики судової експертизи, вона не практикується повсюдно. Наприклад, у Сполучених Штатах акредитація є обов'язковою у деяких штатах, але не в усіх. У Великій Британії організації, що займаються цифровою криміналістикою, акредитує Регулятор судової експертизи, тоді як у Південній Африці уповноваженим національним органом з акредитації є Південноафриканська національна система акредитації.

Прийняття рішення щодо допустимості цифрових доказів

На цьому етапі справжність, цілісність та достовірність цифрових доказів оцінюється на основі результатів оцінки процедури цифрової судової експертизи, проведеної на попередньому етапі (тобто на етапі *розгляду цифрових доказів*); наприклад, оцінюється використання надійних з точки зору криміналістики методів та інструментів для отримання цифрових доказів та показання свідків-експертів та експертів з цифрової криміналістики для підтвердження справжності, цілісності та достовірності цих доказів. Цифровий доказ є допустимим, якщо він встановлює фактичні обставини справи, залишається без змін протягом усього процесу цифрової судової експертизи, а результати експертизи є достовірними, надійними та пройшли експертну оцінку. Для того, щоб результати були визнані допустимими, вони повинні тлумачитися неупереджено, і повинна бути розкрита інформація про помилки та невизначеності у результатах, а також обмеження у тлумаченні результатів.

Таким чином, ця триетапна модель поєднує загальні правові та технічні вимоги щодо допустимості доказів у різних юрисдикціях. Стандартизація практики цифрової судової експертизи є ключем до забезпечення допустимості цифрових доказів у різних країнах. Враховуючи транснаціональний характер кіберзлочинності, уніфікація

практичних методів проведення цифрової судової експертизи не тільки має першорядне значення для розслідування кіберзлочинів, але також є необхідною для здійснення міжнародного співробітництва у справах, пов'язаних із кіберзлочинністю.

Пошук електронних документів (Electronic Discovery)

Так само, як і цифрова судова експертиза, пошук електронних документів (e-Discovery) є процесом, при якому здійснюється «пошук цифрових доказів, визначається їх місцезнаходження, забезпечується їх зберігання і перегляд з метою використання їх як докази в судовому процесі». Однак є ключові відмінності між цифровою судовою експертизою та пошуком електронних документів. На відміну від цифрової судової експертизи, пошук електронних документів насамперед зосереджений на збереженні даних з метою звітності (найбільш економічно ефективним способом) та для виконання правових вимог щодо подання цифрових доказів у ході судового розгляду, коли це необхідно зробити за рішенням суду.

Висновок

Слідчі, що розслідують кіберзлочини, та експерти з цифрової криміналістики звертаються з цифровими доказами та/або іншим чином вивчають їх. Ці фахівці повинні дотримуватись національної політики та керівних принципів передової практики для забезпечення допустимості цифрових доказів у судах. Такі принципи включають технічні та правові вимоги, дотримання яких необхідне для забезпечення допустимості доказів. Крім цих вимог, уніфікація практичних методів проведення розслідування кіберзлочинів та цифрової судової експертизи, що використовуються в різних країнах, має важливе значення для розслідувань, які найчастіше торкаються кількох юрисдикцій.

Вправа № 1 Кваліфікація експерта з цифрової криміналістики

Дослідити необхідні кваліфікації експертів із цифрової криміналістики в Україні. Дайте відповіді на наведені нижче запитання.

Питання для обговорення

Яка кваліфікація потрібна експертам із цифрової криміналістики?

Чи оцінюються ці кваліфікації? Якщо так, то яким чином?

Навіщо потрібні кваліфіковані цифрові криміналісти?

Питання для самоперевірки

1. Які юридичні та етичні зобов'язання мають розслідувачі кіберзлочинів і спеціалісти з цифрової криміналістики?

2. Які основні етапи процесу цифрової криміналістики?

3. Як ідентифікуються цифрові докази?

4. Як слід збирати цифрові докази?

5. Як отримати цифрові докази?

6. Як слід зберігати цифрові докази?

7. Як аналізуються цифрові докази?

8. Як повідомляти про результати аналізу цифрових доказів?

9. Що потрібно обґрунтувати, перш ніж докази будуть прийняті в суді?

Лекція 7. Міжнародне співробітництво у боротьбі з кіберзлочинністю.

7.1. Суверенітет та юрисдикція.

7.2. Офіційні та неофіційні механізми міжнародного співробітництва.

7.3. Збереження та забезпечення цілісності та доступності даних.

7.4. Проблеми, пов'язані з екстериторіальними доказами.

7.5 Проблеми, пов'язані з екстериторіальними доказами

7.1.Суверенітет та юрисдикція

Територіальний суверенітет означає повне та виключне здійснення державою своїх прав та повноважень щодо своєї географічної території. Захист суверенітету займає чільне місце у міжнародних та регіональних правових документах у сфері боротьби з кіберзлочинністю. Як приклад можна навести Конвенцію Ліги арабських держав про боротьбу зі злочинами в галузі інформаційних технологій 2010 року. Зокрема, стаття 4 цієї конвенції говорить: «Кожна держава-учасниця зобов'язується, керуючись своїми власними законами або конституційними принципами, здійснювати свої зобов'язання відповідно до цієї конвенції відповідно до принципів суверенної рівності та територіальної цілісності держав та принципу невтручання у внутрішні справи інших держав».

Територіальний суверенітет може поширюватися на кіберпростір, зокрема на інфраструктуру інформаційно-комунікаційних технологій (ІКТ) держав. Державний суверенітет може бути порушений, коли треті сторони отримують несанкціонований доступ до ІКТ у зарубіжних країнах без відома та дозволу країни, в якій розташовані ІКТ, та/або її правоохоронних органів. Суверенітет вважається порушеним навіть у тому випадку, якщо такий несанкціонований доступ здійснюється в рамках розслідування кіберзлочину, скоєного в іншій країні, коли ця країна намагається

визначити джерело кібератаки та/або запобігти її вчиненню (тактика, відома як зворотний злом або *контратака* хакерів).

Юрисдикція, яка має прив'язку до суверенітету, забезпечує державам права та повноваження визначати та зберігати обов'язки та права людей на своїй території, забезпечувати дотримання законодавства та карати за порушення законів. Держави в першу чергу заявляють про свою юрисдикцію щодо злочинів, скоєних на їхній території (*принцип територіальності*). Стаття 22(1) Конвенції Ради Європи про комп'ютерні злочини 2001 року говорить: «Кожна Сторона вживає законодавчих та інших заходів, необхідних для встановлення юрисдикції щодо будь-якого правопорушення, передбаченого цією Конвенцією, коли таке правопорушення вчинено на її території». Тим не менш, визначення того, «чи був злочин скоєний на території країни, є, однак, непростим завданням, коли злочин був пов'язаний із використанням кіберпростору».

Юрисдикція щодо кіберзлочинів визначається іншими факторами, такими як громадянство правопорушника (принцип громадянства; активний персональний принцип), громадянство жертви (принцип громадянства; пасивний персональний принцип) та наслідки кіберзлочину для інтересів та безпеки держави (принцип захисту), якщо тільки можна встановити «наявність «достатнього чи справжнього зв'язку» між [кіберзлочином] та державою, яка здійснює юрисдикцію». Наприклад, у Великій Британії Апеляційний суд у справі *R v. Sheppard and Anor* (2010 p.) залишив чинним рішення про застосування положень Закону про громадський порядок 1986 року до матеріалів, що підбурюють расову ненависть, викладених на веб-сайті, розміщеному на сервері в США, та обвинувальний вирок стосовно двох жителів Великої Британії за публікацію цих матеріалів.

Юрисдикція щодо кіберзлочинів встановлюється відповідно до національного законодавства про кіберзлочинність. Наприклад, у Малайзії Закон про комп'ютерні злочини 1997 року встановив юрисдикцію держави

щодо кіберзлочинів. Зокрема, стаття 9 цього Закону говорить, що «положення цього Закону щодо будь-якої особи, незалежно від її громадянства чи підданства, мають юридичну силу як на території Малайзії, так і за її межами, і у випадках, коли злочин, передбачений цим Законом, вчиняється будь-якою особою, яка перебуває в будь-якому місці за межами Малайзії, ця особа може бути притягнута до відповідальності за такий злочин, начебто вона була скоєна в будь-якому місці на території Малайзії».

Для порівняння, Танзанія заявляє про свою юрисдикцію щодо кіберзлочину у випадках, коли дія або бездіяльність, яка становить злочин, вчинена повністю або частково – на території Об'єднаної Республіки Танзанія; на борту морського чи повітряного судна, зареєстрованого в Об'єднаній Республіці Танзанії; громадянином Об'єднаної Республіки Танзанія; громадянином Об'єднаної Республіки Танзанії, який проживає за межами Об'єднаної Республіки Танзанії, якщо дія або бездіяльність однаковою мірою є злочином відповідно до законодавства цієї країни; або будь-якою особою, незалежно від її громадянства, підданства або місцезнаходження, коли злочин скоєно з використанням комп'ютерної системи, пристрою чи даних, що знаходяться на території Об'єднаної Республіки Танзанія; або скоєно щодо комп'ютерної системи, пристрою чи даних або особи, які перебувають в Об'єднаній Республіці Танзанії (стаття 30 Закону про кіберзлочини 2015 року).

При цьому Кенія встановлює свою юрисдикцію щодо кіберзлочинів таким чином:

дія або бездіяльність, вчинена за межами Кенії, яка, якщо вчинена в Кенії, є злочином відповідно до цього Закону, вважається вчиненою в Кенії, якщо ... особа, яка вчинила дію або бездіяльність, є ... громадянином Кенії; або ... зазвичай мешкає в Кенії; і ... дію чи бездіяльність скоєно ... проти громадянина Кенії; ... проти майна, що належить уряду Кенії поза Кенії; або ... щоб змусити уряд Кенії вчинити будь-які дії або утриматися

від їх вчинення; або ... особа, яка вчинила дію або бездіяльність, після її вчинення перебуває на території Кенії (стаття 66 Закону про неправомірне використання комп'ютерних технологій та кіберзлочини 2018 року).

Відповідно до цих та інших національних законів про кіберзлочинність юрисдикція встановлюється в основному за ознакою місцезнаходження злочинців або жертв та наслідків кіберзлочинів.

7.2.Офіційні механізми міжнародного співробітництва

Успіх міжнародного співробітництва залежить від наявності уніфікованих національних законодавств у сфері боротьби з кіберзлочинністю, що передбачають кримінальну відповідальність за скоєння кіберзлочинів, та національних процесуальних законодавств про кіберзлочинність, які встановлюють норми доказового права та правила здійснення кримінального судочинства. Міжнародному співробітництву може також сприяти уніфікація двосторонніх, регіональних та багатосторонніх правових документів щодо кіберзлочинності. Приєднання до регіональних та багатосторонніх документів про боротьбу з кіберзлочинністю та їх ратифікацію також необхідні для надання цим документам обов'язкової юридичної сили.

Міжнародному співробітництву також сприяють двосторонні, регіональні та багатосторонні договори в галузі боротьби з кіберзлочинністю за умови взаємного визнання відповідного діяння злочином (тобто пункту в договорах, відповідно до якого передбачуване діяння має вважатися протизаконним у країнах, що співпрацюють). За відсутності взаємного визнання відповідного діяння злочином та уніфікованих законів створюються «безпечні притулки» для осіб, які вчинили кіберзлочини, в яких виконавці кіберзлочинів не можуть зазнавати судового переслідування. Це можна було спостерігати у 2000 році на прикладі випадку з творцем та розповсюджувачем комп'ютерного вірусу «LOVE BUG», якого неможливо було притягнути до кримінальної

відповідальності, оскільки на момент інциденту його дії не вважалися злочином у країні його проживання (на Філіппінах).

Тим не менш, міжнародне співробітництво все ще можливе навіть без суворого тлумачення вимог щодо взаємного визнання відповідного діяння злочином. Більше того, «коли стосовно питань міжнародного співробітництва потрібно дотримання принципу взаємного визнання відповідного діяння злочином, цей принцип вважається дотриманим незалежно від того, чи включає законодавство запитуваної Держави-учасниці відповідне діяння в ту ж категорію злочинів чи описує вона її за допомогою таких термінів, як запитуюча Держава-учасниця, якщо діяння, що утворює склад злочину, у зв'язку з яким запитується допомога, визнано кримінальним відповідно до законодавства обох Держав-учасниць».

Однак є винятки з вимоги щодо взаємного визнання відповідного діяння злочином. Наприклад, стаття 29(3) Конвенції Ради Європи про комп'ютерні злочини 2001 року не вимагає жодного визнання відповідного діяння злочином за необхідності «невідкладного забезпечення безпеки ... комп'ютерних даних», «які зберігаються в комп'ютерній системі, розташованій на території цієї іншої Сторони, та щодо яких запитуюча Сторона має намір у рамках взаємної допомоги направити прохання про обшук або аналогічні забезпечуючі доступ дії, про виїмку або про аналогічне забезпечення безпеки або розголошення цих даних» за основними правопорушеннями, переліченими в цій Конвенції (у статтях з 2 по 11). Стаття 29(4) передбачає право держав відмовляти у проханні про забезпечення безпеки у випадках, якщо в рамках взаємної правової допомоги умова про кваліфікацію правопорушення як кримінально караного обома Сторонами висувається для правопорушень, не перерахованих у конвенції.

На додаток до вимог щодо взаємного визнання відповідного діяння злочином іншою суттєвою вимогою для міжнародного співробітництва є дотримання зобов'язань міжнародного права в галузі прав людини (УНП

ООН, 2013, с. 229). Прохання про надання міжнародної допомоги може бути відхилено, якщо внаслідок задоволення цього прохання запитувана держава порушить свої міжнародні зобов'язання у галузі прав людини.

Чи знаєте ви?

У базі даних УНП ООН з кіберзлочинності (Cybercrime Repository) є розділ Lessons Learned (Отримані уроки), що охоплює такі тематичні питання: попередження кіберзлочинності; розслідування (слідчі повноваження, отримання даних від провайдерів послуг та інші слідчі дії); докази та процедури (судова практика, цифрові докази, юрисдикція та інша процесуальна практика); міжнародне співробітництво (оперативне співробітництво, видача, міжнародне співробітництво та взаємна правова допомога); технічне сприяння; та судові переслідування. Ця база даних забезпечує можливість пошуку в тематичній області або країні.

Офіційні механізми міжнародного співробітництва включають двосторонні, регіональні та багатосторонні договори в галузі боротьби з кіберзлочинністю. Питання співробітництва займають чільне місце у цих договорах. Наприклад, Угода про співробітництво держав-учасниць Співдружності Незалежних Держав у боротьбі зі злочинами у сфері комп'ютерної інформації 2001 року містить кілька статей, присвячених міжнародному співробітництву (статті 5-7), в яких перераховані форми співробітництва, що охоплюються цією угодою (а саме: обмін інформацією) (надання правової допомоги відповідно до міжнародних документів; попередження, виявлення, припинення та розслідування злочинів у сфері комп'ютерної інформації тощо), а також способи, за допомогою яких держави-члени можуть запитувати допомогу, та керівні вказівки для держав-членів щодо виконання запитів. У статті 8 цієї Угоди зазначені обставини, за яких у проханні про надання допомоги може бути відмовлено (а саме: коли виконання запиту суперечить національному законодавству запитуваної держави), та вимога, відповідно до якої держава, яка відмовляється виконувати запит, зобов'язана письмово

повідомити запитуючу державу . про відмову із зазначенням причин відмови.

Чи знаєте ви?

Іbero-американська угода про співробітництво в галузі досліджень, запевнень та отримання доказів у справах, пов'язаних з кіберзлочинністю (Convino Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia), також спрямована на заохочення співпраці між країнами, які підписали угоду у сфері збору та забезпечення безпеки доказів у справах, пов'язаних з кіберзлочинністю.

Крім того, статті 32 та 34 Конвенції Ліги арабських держав про боротьбу зі злочинами в галузі інформаційних технологій 2010 року містять положення про надання взаємної допомоги, процедури співробітництва та подання запитів про надання взаємної допомоги. Більше того, стаття 28 Конвенції Африканського союзу про кібербезпеку та захист персональних даних 2014 року включає положення про уніфікацію, взаємну правову допомогу у справах, пов'язаних з кіберзлочинністю, та обмін інформацією. У положенні про обмін інформацією міститься заклик до держав створювати установи, які можуть сприяти обміну інформацією про загрози кібербезпеці та вразливості, такі як групи реагування на комп'ютерні інциденти (CERT) або групи реагування на інциденти у сфері комп'ютерної безпеки (CSIRT).

Відповідно до статті 28(4) державам наказано «використовувати існуючі механізми міжнародного співробітництва», які можуть включати «міжнародні, міжурядові, регіональні або... державно-приватні партнерства», для вжиття заходів реагування на кіберзлочинність.

Іншими механізмами, які сприяють міжнародному співробітництву у розслідуванні кіберзлочинів та судовому переслідуванні кіберзлочинців, є договори про надання взаємної правової допомоги та видачу. Договори про взаємну правову допомогу (ДВПД) є угодами між країнами, які застосовуються до злочинів з переліку, наведеного в цих угодах, і

визначають види допомоги, що надається кожною країною (наприклад, збір доказів) при проведенні розслідувань.

Підхід, заснований на переліку злочинів, є застарілим і не враховує еволюційний характер кіберзлочинності. Враховуючи змінний характер злочинності (і кіберзлочинності), у деяких ДВПП замість зазначення переліків злочинів сторони домовляються співпрацювати у розслідуваннях та судовому переслідуванні щодо всіх злочинів, які вважаються такими за їхнім внутрішнім законодавством (за деякими винятками).

Запити про надання взаємної допомоги повинні складатися в письмовій формі та включати наступну інформацію: найменування запитуючого органу; ціль запиту; опис запиту; розслідування або судовий розгляд, до якого надається запит про надання допомоги; опис правопорушення чи правопорушень та порушених законів; будь-які прохання щодо процедур, які необхідно дотриматися для отримання, забезпечення збереження та передачі речових та цифрових доказів запитувального органу; терміни забезпечення збереження даних та виконання запиту; та будь-яка інша інформація, яка допоможе запитаній державі виконати запит (див., наприклад, статтю 5 Конвенції про надання взаємної допомоги з кримінальних питань 1992 року Економічного співтовариства західноафриканських держав).

У виконанні запитів щодо надання взаємної допомоги може бути відмовлено за певних обставин. Наприклад, якщо запит «завдасть шкоди суверенітету, безпеці та громадському порядку» (стаття 4 Конвенції ЕКОВАС про надання взаємної допомоги з кримінальних питань; див. також статтю 2 Європейської конвенції про взаємну правову допомогу у кримінальних справах 1959 року, статтю 25 (4) Конвенції Ради Європи про комп'ютерні злочини та статтю 18 Закону Алжиру No.09-04 від 14 числа місяця Шаабан 1430 року (від 5 серпня 2009 року відповідно), що містить спеціальні правила запобігання злочинам у сфері інформаційних

технологій та зв'язку та боротьби з ними). У проханнях про надання взаємної правової допомоги може бути відмовлено, якщо, наприклад, запит «стосується правопорушення, що розглядається Стороною, яку запитує, як політичний злочин або як правопорушення, пов'язане з політичним злочином» (стаття 25(4) Конвенції про комп'ютерні злочини). У проханні про надання даних також може бути відмовлено, якщо виконання запиту або розкриття даних призведе до порушення запитуваних державою міжнародних зобов'язань у галузі прав людини (УНЗ ООН, 2013, с. 228).

Деякі держави (наприклад, Бразилія, Японія та Україна) надають взаємну правову допомогу, якщо держава, що запитує, гарантує дотримання *принципу взаємності* (тобто якщо аналогічний запит запитуваної держави буде задоволений державою, що запитує, у майбутньому). Більше того, Конвенція Ради Європи про комп'ютерні злочини 2001 року діє як ДВПП для країн, які не мають такого договору з країною, яка запитує допомогу. За відсутності договорів і угод, *судові доручення* (тобто письмові запити національних судів, які включають «інформацію про справу, опис необхідних доказів із зазначенням того, для чого вони необхідні, та обіцяння дотримання принципу взаємності в майбутньому) також можуть використовуватися для отримання допомоги у справах, пов'язаних із кіберзлочинністю.

Значні тимчасові затримки (тобто коли «мова йде про кілька місяців») також мають місце під час використання інших офіційних механізмів співробітництва (наприклад, механізмів надання взаємної правової допомоги та видачі). Такі затримки є дуже проблематичними з огляду на нестійкість цифрових доказів.

Складання прохань про надання взаємної правової допомоги

Хоча деякі країни видають посібники щодо складання запитів про надання взаємної правової допомоги та судових доручень і навіть складають зразки запитів, ця практика не є загальноприйнятою. З метою

надання сприяння країнам у складанні запитів щодо надання взаємної допомоги, Управління Організації Об'єднаних Націй з наркотиків та злочинності (УНЗ ООН) розробило Програму складання прохань про надання взаємної правової допомоги, щоб упорядкувати цю процедуру шляхом уніфікації форматів запитів та, тим самим, прискорити подання запитів та їх виконання.

Договори про видачу, такі як Європейська конвенція про видачу 1957 року та Міжамериканська конвенція ОАД про екстрадицію 1981 року, є угодами про затримання та/або видачу осіб запитуючої країни у випадках, коли злочин, що тягне за собою видачу, відповідає встановленому мінімальному порогу покарання. Наприклад, відповідно до статті 3 Конвенції ЕКОВАС про видачу 1994 року поріг покарання становить «мінімум два роки». Регіональні ордери на арешт, такі як європейський ордер на арешт, забезпечують можливість для арешту злочинців за злочини, пов'язані з комп'ютерами, які «караються у видатній ордер державі покаранням або запобіжним заходом, пов'язаними з позбавленням волі з верхньою межею не менше трьох років без проведення перевірки щодо подвійної злочинності діяння взаємного визнання діяння злочином».

Наявність договору про видачу не гарантує, що особа буде видана країні, що запитує. Це спостерігалось у випадку з Лорі Лав (Lauri Love), британським хакером, у видачі якого США було відмовлено, незважаючи на існування підписаного у 2003 році договору про екстрадицію між Великою Британією та США.

Крім того, договори про видачу включають умови, за яких видача не проводиться. Наприклад, відповідно до Міжамериканської конвенції ОАД про екстрадицію, запити про видачу відхиляються, коли покаранням за злочин є довічне ув'язнення або смертна кара. У видачі також буде відмовлено у випадках, коли особа, яка підлягає видачі, буде піддана нелюдському або такому, що принижує гідність, поводженню або

покаранню. Запити про видачу можуть також відхилятися з інших причин, таких як відсутність достатніх доказів, що обґрунтовують видачу (наприклад, Закон Ботсвани про видачу 1990 року), коли запит пов'язаний із злочином, що не тягне за собою видачу (наприклад, військовий злочин, стаття 7 Конвенції ЕКОВАС (Економічне співтовариство країн Західної Африки, англ. The Economic Community of West African States (ECOWAS)) про видачу), або коли запитується видача особи, яка є громадянином країни, що запитується (наприклад, стаття 698 Кримінально-процесуального кодексу Алжиру та стаття 5 (LI) Конституції Бразилії). Що стосується видачі громадян держав, що запитуються, то принцип невидачі власних громадян закріплений у конституції, а також у регіональних та міжнародних договорах. Незалежно від цього принципу «міжнародне публічне право закріплює за державами юридичне зобов'язання видавати або здійснювати судові переслідування осіб, які вчинили серйозні міжнародні злочини». Деякі договори про ордери на арешт можуть також виключати зі сфери своєї дії певні правопорушення, такі як політичні злочини (наприклад, див. статтю 3 Договору про визнання ордерів на арешт Карибської спільноти 2008 року).

7.3. Неофіційні механізми міжнародного співробітництва

Неофіційні механізми міжнародного співробітництва, такі як обмін інформацією між правоохоронними органами, також використовують у розслідуванні кіберзлочинів. Тип інформації, якою обмінюються правоохоронні органи неофіційними каналами, варіює залежно від конкретної держави. В Австралії «органи влади мають можливість надавати такі види допомоги в рамках міжвідомчої співпраці: взяття добровільних свідчень свідків, проведення добровільних опитувань свідків, взяття добровільних показань свідків з відеозв'язку, прийняття співробітників іноземних поліцейських органів, які проводять розслідування в Австралії, обмін оперативними даними, здійснення фізичного спостереження, отримання відомостей про судимість чи

отримання загальнодоступних матеріалів». Інші країни домовляються про використання деяких даних особистого характеру.

Чи знаєте ви?

Існує механізм неофіційного міжнародного співробітництва у сфері судового переслідування у справах, пов'язаних із кіберзлочинністю: Глобальна прокурорська мережа з протидії електронним злочинам (GPEN) Міжнародної асоціації прокурорів.

Неофіційні механізми співробітництва сприяють оперативному обміну інформацією між правоохоронними органами (тобто протягом днів, а чи не місяців). Крім того, мережі 24/7 (наприклад, Мережа 24/7 підгрупи G7 щодо злочинів у галузі високих технологій та контактний центр 24/7 сторін Конвенції Ради Європи про комп'ютерні злочини, створений відповідно до статті 35 конвенції) створюються з метою отримання невідкладних запитів про надання цифрових доказів та сприяння міжнародному співробітництву. Неофіційні канали співробітництва в основному використовуються для отримання юридичних та технічних консультацій та сприяння у справах, пов'язаних із кіберзлочинністю, а не для запитів щодо збору цифрових доказів. Наприклад, у Японії запити про надання інформації по неофіційних каналах дозволяється виконувати тільки в тому випадку, якщо країна, що запитує, не має наміру використовувати цю інформацію як докази. Якщо країна має намір використати цю інформацію як доказ, необхідно надіслати офіційний запит щодо надання взаємної правової допомоги. Цифрові докази, отримані цими каналами, можуть бути визнані неприпустимими в національних судах держави, що запитує, якщо не підтримується система охорони доказів. Якщо інформація неофіційно передається правоохоронними органами Сполучених Штатів Америки, Парагваю, Аргентини (та інших країн), країни, що запитують, повинні діяти офіційними каналами.

Міжнародні та регіональні організації також сприяють неофіційному міжнародному співробітництву. Наприклад, термінові запити про надання

взаємної допомоги можуть надсилатися до Організації американських держав. Термінові запити про надання допомоги можна також надсилати через ІНТЕРПОЛ, найбільшу у світі міжнародну поліцейську організацію, яка своєю глобальною поліцейською телекомунікаційною мережею I-24/7 охоплює понад 190 країн. За допомогою цієї мережі національні правоохоронні органи діляться досвідом, технологіями та ресурсами для боротьби з транснаціональними злочинами.

Інтерпол виступає як вузол зв'язку між країнами, допомагаючи їм поширювати інформацію, наприклад, *повідомлення*, і навіть сприяючи їм у координації спільних операцій. Наприклад, у 2012 році Інтерпол допоміг місцевій владі в Іспанії, Аргентині, Чилі та Колумбії заарештувати 25 членів міжнародної хакерської групи Anonymous в рамках операції «Викриття» (Operation Unmask) (Whiteman, 2012; Interpol, «Operation Unmask»). У 2017 році «операція, проведена під керівництвом Інтерполу, за участю правоохоронних органів Індонезії, Малайзії, М'янми, Філіппін, Сінгапуру, Таїланду та В'єтнаму», а також Китаю та організацій приватного сектору дозволила «ідентифікувати близько 9.000 командних серверів (C2) веб-сайтів, включаючи урядові портали» (INTERPOL, 2017).

У статті Уайтмена (2012) йдеться про те, що підозрюваних заарештував Інтерпол. Це помилка. Інтерпол не має повноважень заарештовувати злочинців. Інтерпол може допомогти створити щось на кшталт *спільної слідчої групи* (Europol, nd), яка може сприяти проведенню розслідувань кримінальних справ, але тільки місцеві слідчі мають повноваження здійснювати арешти на території своїх країн. На жаль, засоби масової інформації часто неправильно зображують Інтерпол як міжнародну поліцію, яка має *повноваженнями на місцях*. Замість наділення Інтерполу повноваженнями провадити арешти в країні, кожна держава створює своє національне центральне бюро (НЦБ) (INTERPOL, 2018). Штаб-квартира Інтерполу може надавати інформацію та рекомендації НЦБ, але вона не може змусити їх вжити будь-яких дій. Крім

того, співробітниками НЦБ у деяких випадках – але не завжди – є місцеві кадрові поліцейські чи прокурори.

Як зазначено у Проекті доповіді УНЗ ООН: «Всебічне дослідження проблеми кіберзлочинності» (2013), країни зазначили, що неофіційна співпраця все ще значною мірою залежить від наявності двосторонніх та регіональних угод, мереж регіональних та міжнародних організацій та існуючих зв'язків та партнерських відносин між правоохоронними органами (УНЗ ООН, 2013, с. 235). Партнерства також відіграють ключову роль у співпраці між правоохоронними органами та приватним сектором під час розслідування кіберзлочинів. Співпраця між групою Microsoft з розслідування Інтернет-злочинів та правоохоронними органами Сполучених Штатів Америки, Марокко та Туреччини призвела до виявлення та подальшого арешту творців та розповсюджувачів комп'ютерного черв'яка Zotob (FBI, 2006).

7.4.Зберігання та забезпечення збереження даних та доступ до даних

Запити про допомогу в рамках міжнародного співробітництва можуть також відхилятися через процедурні вимоги. Розглянемо, наприклад, практичні методи зберігання, забезпечення збереження даних та отримання до них доступу. Виконання прохання про надання даних, які зберігають постачальники послуг Інтернету, залежить від умов надання послуг, політики конфіденційності та практики ведення бізнесу провайдера послуг. У зв'язку з цим провайдери послуг відрізняються між собою не лише типом даних, які вони зберігають (наприклад, журнали реєстрації IP-адрес або інформація про деактивовані облікові записи), а й періодом їх зберігання (дні, тижні, місяці або роки) (див., наприклад, «Guidelines for Law Enforcement» («Керівні принципи забезпечення законності») Twitter і «Data Policy» («Політика використання даних») Facebook для отримання додаткової інформації). Політика щодо зберігання даних, а також отримання доступу до них також варіює залежно від національних, регіональних та міжнародних законів у галузі захисту даних.

Прохання про забезпеченні збереження даних надсилаються постачальникам послуг правоохоронними органами з метою збереження даних до того, як вони будуть видалені або якимось чином змінені. Процедура доступу до збережених даних прописується в національному законодавстві. Законні розпорядження (наприклад, судова ухвала або ордер на обшук), якщо такі взагалі передбачені, необхідні для отримання різноманітних даних від постачальників послуг, варіюють залежно від конкретної країни. Наприклад, в той час як у Сполучених Штатах повістки та судові постанови необхідні для отримання *даних, що не належать до контенту* (або *метаданих*; наприклад, даних абонента та IP-адрес), а ордери на обшук – для отримання *даних, що належать до контенту* (наприклад, текстів електронних листів або інших повідомлень) (Закон США про збережені повідомлення 1986 року; титул II Закону про конфіденційність електронних повідомлень 1986 року), турецьким правоохоронним органам не потрібні законні розпорядження для отримання доступу до даних, що не належать до контенту, та даних, до контенту (Закон про Інтернет 5651).

Більше того, органи, які можуть отримати доступ до збережених та/або збережених даних, також різняться залежно від конкретної країни. Наприклад, у Кенії співробітник правоохоронних органів або інша уповноважена особа (а саме «експерт з кібербезпеки, який призначається секретарем Кабінету міністрів з питань національної безпеки») може отримати доступ до збережених та/або збережених даних відповідно до Закону Кенії про неправомірне використання комп'ютерних технологій та кіберзлочинах 2018 року, тоді як на Ямайці лише правоохоронці мають право отримувати доступ до даних.

Крім того, у певних ситуаціях, які визначаються національним законодавством, допускається добровільне розкриття інформації постачальниками Інтернет-послуг без законних розпоряджень. Як приклад такої ситуації можна навести екстрений запит про надання даних з метою

запобігання серйозним тілесним ушкодженням або смерті. Якщо постачальники послуг відмовляються надавати запитані дані добровільно, то за певних обставин і залежно від конкретного випадку, доказів, тягара доказування і національного законодавства, ці постачальники послуг можуть бути примушені в передбаченому законом порядку до надання цієї інформації.

Чи знаєте ви?

Соціальні мережі та інші онлайн-платформи публікують звіти про прозорість (див., наприклад, звіти Pinterest, Tumblr, Twitter, LinkedIn, Facebook і т.д.), які включають інформацію про кількість отриманих запитів про надання доступу до даних про користувачів сайту, національних чи міжнародних органах, які запросили цю інформацію, про те, які правові механізми використовувалися для запиту та/або доступу до даних, і чи був задоволений отриманий запит.

7.5. Проблеми, пов'язані з екстериторіальними доказами

Навіть за наявності офіційних та неофіційних механізмів міжнародного співробітництва виникають проблеми при ідентифікації та збиранні цифрових доказів, що зберігаються у хмарних сховищах та інших постачальників послуг. Проблема хмарних обчислень у тому, що важко дізнатися, де зберігаються дані. Без такої інформації неможливо визначити «відповідну юрисдикцію, до якої має надсилатися запит про співпрацю для отримання цифрових доказів» (УНЗ ООН, 2013, стор. 241).

Хмарні дані можуть бути розбиті на фрагменти та зберігатися у різних місцях та у кількох країнах. Таку проблему фрагментації даних можна проілюструвати на прикладі справи *United States v. Microsoft* (2018). У рамках розслідування цієї справи уряд США видав ордер на обшук відповідно до Закону США про збережені повідомлення (SCA) 1986 року, щоб отримати докази у справі про незаконний обіг наркотиків. Компанія Microsoft задовольнила цей запит, передавши відповідні дані, що не стосуються контенту, які зберігалися на серверах у США (наприклад,

адресну книгу підозрюваного), але не надала уряду США відповідні дані, що стосуються контенту (наприклад, вміст електронних листів цієї особи), оскільки ці дані зберігалися у дата-центрі Microsoft у Дубліні (Ірландія).

Суть спору, що лежав основою справи *United States v. Microsoft* (2018) полягала в тому, чи дозволяють положення Закону про збережені повідомлення отримувати доступ до даних, що знаходяться на серверах в іншій країні, і чи вважається такий доступ юридично необґрунтованим екстериторіальним застосуванням закону. Наразі це питання втратило свою актуальність у зв'язку з ухваленням у США Закону, який роз'яснює порядок законного використання даних за кордоном 2018 року. З його прийняттям до параграфу 2713 Закону про збережені повідомлення (глави 18 Зводу законів США) було внесено такі поправки: «Постачальник послуг електронного зв'язку або послуг дистанційної обробки даних повинен дотримуватися зобов'язань цього розділу щодо збереження, резервного копіювання або розкриття вмісту телеграфних або електронних повідомлень та будь-якого запису або іншої інформації, що стосуються клієнта або передплатника, які знаходяться у веденні, розпорядженні або під контролем такого постачальника послуг, *незалежно від того, чи знаходиться таке повідомлення, запис чи інша інформація на території чи за межами території Сполучених Штатів* ». Закон «Cloud» забезпечує прямий доступ до екстериторіальних даних. Однак «загальних стандартів та гарантій щодо обставин, якщо такі є, відповідно до яких правоохоронні органи можуть мати прямий доступ до екстериторіальних даних» (УНЗ ООН, 2013, стор. 240), станом на 2018 рік поки не існує.

Закон «Cloud» та Загальний регламент ЄС із захисту даних

Висловлюються побоювання щодо того, що Закон «Cloud» завдасть шкоди Загальному регламенту ЄС із захисту даних (ЗРЗД), всеосяжному положенню про захист даних, яке набуло чинності 25 травня 2018 року (ЛЕКЦІЯ 10). Компанії стикаються з перспективою сплати великих штрафів та накладення санкцій у разі недотримання ЗРЗД. Компанії, яких

необхідно дотримуватися одночасно і Закону «Cloud», і ЗРЗД, змушені забезпечувати баланс між вимогами Закону «Cloud» щодо забезпечення доступу до даних та вимогами ЗРЗД щодо захисту прав суб'єктів даних, а також забезпечувати вжиття необхідних заходів захисту та дотримання вимог статті 44-49 ЗРЗД під час передачі даних третім сторонам або міжнародним організаціям.

Національний потенціал та міжнародне співробітництво

Ефективність міжнародного співробітництва залежить від здатності держав виконувати запити про надання доказів в такий спосіб, щоб забезпечити допустимість цих доказів у суді. Для цього потрібна наявність кваліфікованих фахівців у галузі кіберзлочинності, які можуть забезпечити отримання доказів відповідно до національних норм доказового права та правил кримінального судочинства. Проте таких спеціалістів не вистачає. Більше того, країни в усьому світі мають брак національного потенціалу, необхідного для боротьби з кіберзлочинністю.

Такий дефіцит національного потенціалу є нестачею кадрових, фінансових і технічних ресурсів. По-перше, у багатьох країнах немає достатньої кількості кваліфікованих фахівців для проведення розслідувань кіберзлочинів, а також для судового переслідування кіберзлочинців та розгляду запитів про допомогу в рамках міжнародного співробітництва у справах, пов'язаних із кіберзлочинністю. По-друге, країнам може не вистачати фінансових ресурсів, необхідних для підбору, найму та утримання кваліфікованого персоналу, а також для організації регулярної та сучасної підготовки для слідчих, які займаються кіберзлочинами та інших відповідних фахівців. По-третє, в країнах відсутня необхідна матеріальна база для аналізу цифрових доказів та бракує коштів для придбання необхідного обладнання та інструментів цифрової криміналістики для належного проведення розслідувань кіберзлочинів.

Для вирішення проблеми дефіциту національного потенціалу було створено та продовжують створюватися партнерства з національними,

регіональними та міжнародними організаціями (наприклад, Міністерством юстиції США, Організацією американських держав та Міжнародним союзом електрозв'язку), а також приватними компаніями з метою надання фінансової, кадрової та технічної допомоги з питань , пов'язаним з кіберзлочинністю, країнам, які потребують такої допомоги, та надання підтримки їх зусиллям щодо розвитку національного потенціалу в галузі боротьби з кіберзлочинністю.

Відповідно до резолюції Генеральної асамблеї Організації Об'єднаних Націй №.65/230, резолюції №.22/7 Комісії ООН щодо запобігання злочинності та кримінального правосуддя «Зміцнення міжнародного співробітництва з метою боротьби з кіберзлочинністю» та резолюцією №.22/8 Комісії ООН з попередження злочинності та кримінальному правосуддю «Сприяння технічної допомоги та нарощування потенціалу для посилення національних заходів та міжнародного співробітництва в галузі боротьби з кіберзлочинністю», УНЗ ООН уповноважено надавати державам допомогу у боротьбі з кіберзлочинністю шляхом організації технічної підготовки з метою нарощування потенціалу та здійснення програм з попередження інформаційно-просвітницьких кампаній. Ці тренінги, програми та кампанії мають важливе значення, оскільки вони забезпечують довгострокові вирішення проблем існуючого дефіциту національного потенціалу шляхом підвищення рівня знань, навичок та можливостей, необхідних для проведення розслідувань кіберзлочинів.

Висновок

Взаємне визнання відповідного діяння злочином та уніфікація національних, двосторонніх, регіональних та багатосторонніх законів про кіберзлочинність мають важливе значення для міжнародного співробітництва. Навіть за наявності вимоги щодо взаємного визнання відповідного діяння злочином та уніфікованих законів міжнародне співробітництво у галузі розслідування кіберзлочинів може виявитися

скрутним. Ситуація посилюється відсутністю домовленостей щодо своєчасного збирання та забезпечення збереження цифрових доказів та обміну ними між країнами через офіційні механізми співробітництва. Країни в усьому світі також мають брак національного потенціалу для розслідування кіберзлочинів з погляду кадрових, фінансових та технічних ресурсів. На додаток до проблеми відсутності або браку необхідних коштів, кваліфікованого персоналу, технічного обладнання та інструментів для проведення розслідувань кіберзлочинів, також відсутні загальноприйняті стандарти та протоколи щодо цифрової криміналістики та збору доказів, які забезпечують допустимість цифрових доказів у національних судах співробітництва. Тільки багатосторонній підхід, націлений на вирішення вищезгаданих проблем, здатний покращити якість міжнародного співробітництва у справах, пов'язаних із кіберзлочинністю.

Вправа №1 – Територіальний суверенітет і кіберзлочинність

Яким чином кіберзлочинність може втручатися в територіальний суверенітет?

Знайдіть справу про кіберзлочин, який негативно вплинув на територіальний суверенітет держави. Опишіть, що сталося у цій справі, і чому ви вважаєте, що територіальний суверенітет держави було порушено, використовуючи доказові аргументи (тобто аргументи, підтверджені літературою та дослідженнями), щоб підтвердити свої думки.

Вправа № 2 - Міжнародні організації та міжнародне співробітництво

Проведіть онлайн-дослідження та визначте національну, регіональну чи міжнародну організацію (не згадану в цій лекції), яка надає певну форму допомоги країнам у боротьбі з кіберзлочинністю.

Які послуги пропонує організація (наприклад, навчання, розслідування, спілкування)?

З якими країнами працює організація?

Вправа № 3 – Доступ до даних і законні розпорядження

Визначте національні закони, які стосуються доступу до даних. Який закон в Україні (інших країнах) регулює доступ до збережених персональних даних?

Хто має право доступу до цих даних? За яких обставин?

Чи потрібен законний порядок для доступу до вмісту даних? Якщо так, то який?

Чи потрібен законний порядок для доступу до метаданих? Якщо так, то який?

Питання для самоперевірки

1. Які відмінності між суверенітетом і юрисдикцією? Чи можна застосувати ці концепції до кіберзлочинності? Будь ласка, поясніть свою відповідь.
2. Які сильні сторони та обмеження офіційних механізмів міжнародного співробітництва?
3. Які переваги та недоліки неформальних механізмів міжнародного співробітництва?
4. Чи узгоджені вимоги щодо зберігання, збереження та/або доступу до даних у різних країнах? Як це впливає на неформальну та офіційну співпрацю у розслідуванні кіберзлочинів? Будь ласка, поясніть свою відповідь.
5. Які проблеми постають перед екстериторіальним збором доказів?
6. Як дефіцит національного потенціалу впливає на розслідування кіберзлочинів?

ЗМІСТОВИЙ МОДУЛЬ 3. СТРАТЕГІЇ, ПОЛІТИКА ТА ПРОГРАМИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ.

ЛЕКЦІЯ 8. КІБЕРБЕЗПЕКА ТА ПОПЕРЕДЖЕННЯ КІБЕРЗЛОЧИННОСТІ: СТРАТЕГІЇ, ПОЛІТИКА ТА ПРОГРАМИ

8.1 Управління Інтернетом

8.2 Стратегії кібербезпеки: основні особливості

8.3 Міжнародне співробітництво з питань кібербезпеки

8.4 Стан справ у галузі кібербезпеки

8.1 Управління Інтернетом

Виділяють «два переважаючі погляди на Інтернет»: з одного боку, Інтернет розглядається як «глобальна метанережа, яка служить як відкрита платформа для передачі інформації між кінцевими користувачами, які підключають комп'ютери до мережі»; з іншого боку, Інтернет розглядається «в контексті додатків, яким він забезпечує можливість функціонування, та того, як ці додатки впливають на кінцевих користувачів». Саме останнє з перерахованих уявлень про Інтернет «призводить до сприйняття кіберпростору як якоїсь віртуальної реальності» (або середовища), в якому ведеться онлайнова активність.

У літературі, присвяченій теоріям регулювання стосовно управління Інтернетом та кіберпростором, основна увага приділяється тому, які особи, групи, підприємства, організації та державні установи регулюють Інтернет та кіберпростір, а також способи регулювання кіберпростору та Інтернету.

Ця думка знаходить підтвердження в літературі, в якій стверджується, що кіберпростір та Інтернет регулюються, наприклад, законами, кодом комп'ютерної програми, системною архітектурою та архітектурою Інтернету; фізичними особами, підприємствами та організаціями з деякою участю держави або без участі держави (тобто на основі саморегулювання); та фізичними особами, підприємствами та

організаціями, що несуть спільну відповідальність за управління (тобто на основі розподіленого захисту).

Як було сказано на Всесвітній зустрічі на найвищому рівні з питань інформаційного суспільства (ВЗПС), глобальному форумі, організованому Організацією Об'єднаних Націй, Управління Інтернетом являє собою «розробку та застосування урядами, приватним сектором та громадянським суспільством, при виконанні ними своєї відповідної ролі, спільних принципів, норм, правил, процедур прийняття рішень та програм, що регулюють еволюцію та застосування Інтернету». Як зазначив Мюллер (Mueller) (2010), відповідальність за управління Інтернетом несуть не лише «офіційні установи, які формують політику»; навпаки, «у більшості випадків фізичне управління Інтернетом є децентралізованим та незалежним, воно засноване на взаємодії десятків тисяч операторів мереж та постачальників послуг, а іноді й самих користувачів, які з'єднані між собою через Інтернет». Інтернет впливає на глобальні інтереси, і процес управління ним «включає не лише питання, пов'язані з присвоєнням імен та адрес в мережі Інтернет, якими займається Корпорація з розподілу імен і номерів в Інтернеті (ICANN); він також включає інші важливі питання державної політики, такі як критично важливі інтернет-ресурси, безпека та захист Інтернету, а також аспекти та проблеми розвитку, пов'язані з використанням Інтернету». Натомість процес управління Інтернетом в основному здійснюється на міжнародному рівні кількома учасниками – урядом, приватним сектором, науковою спільнотою та громадянським суспільством – і охоплює цілу низку технічних та нетехнічних питань. Проте країни розходяться в думках щодо того, які учасники мають відігравати основну роль в керуванні Інтернетом. У той час як деякі країни вважають, що відповідальність за управління Інтернетом мають нести кілька учасників, інші країни вважають, що управління Інтернетом має входити до сфери виключної компетенції держави.

Чи знаєте ви?

Форум з управління Інтернетом (Internet Governance Forum, IGF) включає ресурси для обговорення питань, пов'язаних з управлінням Інтернетом.

Навіть якщо країни домовляться про склад учасників, відповідальних за управління Інтернетом, існують інші перешкоди для прийняття загальних принципів управління Інтернетом, які пов'язані з відмінностями в системах кримінального правосуддя та законах, що діють у різних країнах, та у їхніх позиціях з культурних, релігійних, соціальних та політичних питань. Хоча головною метою управління Інтернетом є спільне регулювання Інтернету всіма країнами, реальність така, що країни розходяться у думках щодо того, як має здійснюватись таке регулювання. Це можна спостерігати на прикладі того, як різні країни ставляться до деяких основоположних принципів роботи Інтернету, таких як свобода (тобто доступ до інформації та обміну інформацією можуть здійснюватися «без обґрунтованих обмежень»), відкритість (тобто безперешкодний потік інформації) в мережі), функціональна сумісність (тобто здатність різних цифрових пристроїв та комп'ютерних систем з'єднуватися, передавати дані та обмінюватися даними), безпека (тобто захист конфіденційності, цілісності та доступності систем, мереж, послуг та даних) та стійкість (тобто підтримка роботи під час збоїв та зміни умов). З платформи для поширення інформації та обміну інформацією – відповідно до принципу відкритості – Інтернет еволюціонував у платформу для соціальних взаємодій, торгівлі та комерції та надання державних послуг. У той же час Інтернет та ІКТ використовувалися і продовжують використовуватися неправомірно та зловмисно людьми та організаціями, що становлять загрозу, та іншими зловмисниками, що сприяє зростанню кіберзлочинності, і, отже, викликає необхідність посилення заходів забезпечення безпеки.

Окремі країни не дотримуються та не заохочують деякі з цих принципів. Наприклад, деякі країни як першочергове завдання

наголошують на безпеці на шкоду принципам свободи і відкритості. Інші країни не схвалюють принципу відкритості, позбавляючи громадян доступу до інформації з інших країн. Крім того, країни, які в тій чи іншій формі підтримують принципи роботи Інтернету, робили дії, які суперечили одному чи кільком таким принципам. Наприклад, принцип мережного нейтралітету, який заохочує відкритість, вимагаючи однакового ставлення до всіх даних, незалежно від джерела (див. також визначення у законодавчих нормах; наприклад, у статті 3 Федерального закону Бразилії 12,965 від 2014 року), може не застосовуватись на практиці, що дозволяє Інтернет-провайдерам блокувати або уповільнювати швидкість передачі даних, а також пропонувати високошвидкісні канали передачі даних (тобто платну пріоритизацію). Понад те, під час реалізації чи дотриманні цих принципів виникають протиріччя. Як приклад можна навести принципи відкритості та безпеки; міжмережевий екран, система мережного захисту, що обмежує вільний потік інформації – тобто принцип відкритості, – блокуючи несанкціонований трафік. При цьому блокування несанкціонованого мережного трафіку (вхідного потоку інформації) міжмережевим екраном відбувається з метою забезпечення безпеки системи та мережі.

Чи знаєте ви?

Freedom House розмістила в мережі інтерактивну карту (Freedom on the Net 2018 Map) на якій показано, які країни мають «вільний», частково вільний або обмежений доступ до Інтернету.

8.2 Стратегії кібербезпеки: основні особливості

Стратегії забезпечення кібербезпеки та стратегії протидії (або попередження) кіберзлочинності є термінами, які використовуються як взаємозамінні. Хоча стратегії забезпечення кібербезпеки та стратегії протидії кіберзлочинності доповнюють одна одну та місцями перетинаються, між ними існують відмінності. У стратегіях протидії кіберзлочинності описані зусилля, які прямо чи опосередковано пов'язані з

боротьбою з кіберзлочинністю, такі як заходи реагування, що вживаються правоохоронними органами, та сприяння національному та міжнародному співробітництву між урядами, діловими колами, науково-освітніми установами, організаціями та громадськістю з метою контролю /або зниження рівня кіберзлочинності. Простіше кажучи, стратегії протидії кіберзлочинності зосереджені виключно на заходах політики, програмах та практиці в галузі кримінального правосуддя та запобігання злочинності. На відміну від них, стратегії забезпечення кібербезпеки містять керівні вказівки з питань кібербезпеки (які можуть включати вказівки щодо попередження кіберзлочинності) і визначають завдання, а також плани дій, заходи та обов'язки установ, необхідні для досягнення цих цілей. Ці стратегії передбачають прийняття правових, процедурних, технічних та інституційних заходів, призначених для захисту систем, мереж, послуг та даних.

Стратегії запобігання кіберзлочинності та стратегії забезпечення кібербезпеки

Національні стратегії кібербезпеки відображають прагнення країн у сфері забезпечення кібербезпеки та запобігання кіберзлочинності на національному та міжнародному рівнях. У цих стратегіях викладаються принципи, на яких заснована стратегія, описуються інтереси, які ця стратегія покликана захищати, визначаються інструменти, що використовуються для просування та захисту цих інтересів, позначаються кіберзагрози та проблеми, які ці загрози становлять для національної та економічної безпеки, визначаються пріоритетні завдання політики кібербезпеки та ресурси, що виділяються для виконання цих завдань. Ці стратегії «закликають органи, відповідальні за розробку політики, позначити стратегічні завдання (цілі), визначити ресурси, що є для виконання цих завдань (засоби), та розробити керівні вказівки щодо того, як слід використовувати такі ресурси виконання поставлених завдань».

У стратегіях кібербезпеки докладно пояснюється, чому стратегія є важливою та необхідною (контекст), чого потрібно досягти (завдання), у чому вона полягає, і на що та кого вона вплине (сфера дії). Ключовими компонентами цих стратегій є завдання, пріоритетні дії, очікувані результати та механізми оцінки.

Завдання стратегій кібербезпеки включають завдання, пов'язані з національною безпекою, а також завдання, пов'язані з інформаційно-комунікаційними технологіями. Наприклад, стратегія кібербезпеки Швеції «заснована з метою забезпечення безпеки Швеції: захист життя і здоров'я населення, функціонування суспільства і здатність підтримувати фундаментальні цінності, такі як демократія, верховенство закону і права і свободи людини. Стратегія також базується на спільній меті політики в галузі інформаційних технологій (ІТ) – зробити Швецію світовим лідером у справі реалізації можливостей цифрової трансформації» (Swedish Ministry of Justice, 2017, р. 1; див. також: Міністерство юстиції Швеції, Національна стратегія кібербезпеки). У Нігерії завданнями стратегії кібербезпеки Cybersecurity Strategy (2014) є такі:

Всеосяжне законодавство щодо кіберзлочинності та заходи протидії кіберзагрозам, які можуть бути прийняті на національному рівні та є актуальними на регіональному та глобальному рівнях у контексті забезпечення безпеки кіберпростору країни.

Реалізація заходів щодо захисту критично важливої інформаційної інфраструктури, а також зниження факторів національної вразливості за допомогою механізму забезпечення кібербезпеки.

Визначення можливостей у сфері ефективного реагування на комп'ютерні інциденти.

Національні механізми щодо створення потенціалу, інформування громадськості та розширення можливостей підвищення кваліфікації, що необхідно для зміцнення нашої здатності оперативно та ефективно реагувати на кібератаки.

Надійний механізм для забезпечення участі національних зацікавлених сторін та міжнародних партнерів у колективних зусиллях боротьби з кіберзагрозами.

Захист уряду від усіх форм кібератак та стримування таких кібератак.

Координація ініціатив у сфері забезпечення кібербезпеки всіх рівнях уряду країни.

Створення національних можливостей для протидії кіберзагрозам на основі послідовної співпраці в рамках державно-приватного партнерства та взаємодії всіх зацікавлених сторін.

Популяризація національної концепції кібербезпеки шляхом підвищення обізнаності, розвитку партнерства на основі спільної відповідальності та участі надійних зацікавлених сторін.

Сприяння координації, співпраці та взаємодії регіональних та глобальних учасників у справі забезпечення кібербезпеки.

Мета пріоритетних дій полягає у виконанні поставлених завдань. Наприклад, у Європейському союзі більшість національних стратегій забезпечення кібербезпеки як пріоритетні дії визначають створення стандартів, норм і законів у галузі кібербезпеки (де це необхідно), заохочення культури кібербезпеки не лише серед відповідних зацікавлених сторін (наприклад, державних установ, науково-освітніх установ, компаній та організацій), а також широкому загалу, а також розвиток національної та міжнародної співпраці та взаємодії між відповідними зацікавленими сторонами. Пріоритетні дії, перелічені в Стратегії національної кібербезпеки США за 2018 рік, включають: «пріоритет розробки та впровадження інновацій»; «заохочення загального дотримання норм у кіберпросторі»; «лідерство з об'єктивними та колективними розвідданими»; «вдосконалення системи затримання злочинців за кордоном» та багато інших дій.

Очікувані результати цих пріоритетних дій включають показники, які повинні бути досягнуті після їх здійснення (наприклад, розробка стандартів кібербезпеки). Наприклад, у Стратегії національної кібербезпеки США 2018 року очікувані результати включають: успішне усунення вразливостей у структурі кібербезпеки; зниження шкоди від «деструктивної, шкідливої та підривної хакерської діяльності, спрямованої проти інтересів Сполучених штатів, або її запобігання» та стримування «діяльності, що суперечить відповідальній поведінці в кіберпросторі за допомогою примусових заходів, мережевого та іншого характеру»; та здатність Сполучених Штатів «використовувати кіберможливості для досягнення цілей національної безпеки».

Механізми оцінки включають інструменти, які можна використовувати для того, щоб встановити, які результати були насправді досягнуті (і наскільки вони відповідають очікуваним результатам). До стратегії також включаються ключові показники діяльності, які використовуються для оцінки прогресу у реалізації стратегічних завдань національної стратегії кібербезпеки. На основі цієї оцінки до стратегії національної безпеки вносяться зміни та переглядаються пріоритетні дії.

Типові стратегії кібербезпеки передбачають використання відповідних політичних інструментів (наприклад, стандартів, заходів політики, законодавства, освітніх програм тощо), необхідні виконання цих стратегій, і навіть участь осіб, відповідальних за здійснення контролю над реалізацією цих інструментів. Наприклад, у Чилі у Національній політиці в галузі забезпечення кібербезпеки на 2017-2022 роки. вказані заходи, які мають бути реалізовані на основі конкретних стратегічних завдань, та установи, відповідальні за реалізацію та/або сприяння у реалізації цих заходів. Так само на Філіппінах у Плані національної кібербезпеки 2022 р. визначено заходи щодо досягнення стратегічних завдань, а також ролі та обов'язки ключових зацікавлених сторін.

Національні стратегії кібербезпеки: життєві цикли, передова практика та репозиторії

Життєвий цикл національної стратегії кібербезпеки складається з п'яти етапів:

Перший етап (етап 1) – ініціювання, що передбачає визначення відповідних зацікавлених сторін та їх ролей у процесі розробки стратегії, а також підготовку плану розробки стратегії.

Другий етап (етап 2) – огляд та критичний аналіз наявного досвіду, передбачає оцінку стану справ у країні в галузі кібербезпеки, виявлення загроз кібербезпеці та аналіз поточних та майбутніх ризиків кібербезпеки.

Третій етап (етап 3) – розробка національної стратегії кібербезпеки. Цей етап передбачає підготовку проекту стратегії, консультації з відповідними заінтересованими сторонами, остаточне доопрацювання стратегії з урахуванням зауважень та публікацію стратегії.

Четвертий етап (етап 4) – імплементація, передбачає розробку плану дій, визначення того, які ініціативи, що ґрунтуються на завданнях стратегії, будуть реалізовані, визначення ресурсів, необхідних для реалізації цих ініціатив, та визначення конкретних дій та термінів виконання цих дій. На цьому етапі також розробляються параметри та ключові показники діяльності для оцінки ефективності (тобто своєчасності) та результативності (тобто позитивного результату) ініціатив.

Як правило, у планах дій вказуються рішення (або заходи), які можуть бути реалізовані для досягнення цілей, зацікавлені сторони, відповідальні за виконання завдань, параметри, які будуть використовуватись для оцінки термінів виконання завдань та досягнення бажаних результатів. Плани дій реалізуються на національному рівні (наприклад, Національна служба безпеки, План дій з реалізації концепції кібербезпеки Словацької Республіки на 2015-2020 роки) та регіональному

рівні (наприклад, План дій щодо забезпечення кібербезпеки та запобігання кіберзлочинності КАРИКОМ).

П'ятий етап (етап 5) – моніторинг та оцінка, передбачає оцінку відповідності плану дій завданням стратегії кібербезпеки, а також аналіз стратегії та плану дій, щоб встановити, чи зберігають вони свою актуальність, чи задовольняють вони потребам країни в галузі забезпечення кібербезпеки, і чи можуть вони протидіяти новим ризикам кібербезпеки. Якщо завдання стратегії кібербезпеки не виконуються в результаті реалізації плану дій, до плану дій вносяться зміни. Зміни можуть також вноситись у стратегію у разі, якщо вона більше не є актуальною та/або не може застосовуватись для протидії новим загрозам кібербезпеки.

Чи знаєте ви?

Нові технології (наприклад, блокчейн, штучний інтелект та квантові обчислення) згадуються в деяких національних стратегіях кібербезпеки (див., наприклад, Стратегію національної кібербезпеки США та Національну стратегію кібербезпеки Великобританії на 2016-2021 роки. *Джерело: ICE (2018). Посібник із розробки національної стратегії кібербезпеки, стор.17).*

Керівництво з передової практики розробки національної стратегії кібербезпеки (2016), прийняте Європейським агентством з мережевої та інформаційної безпеки (ENISA), включає приклади стратегічних цілей і завдань, які необхідно виконати для досягнення цих цілей, і містить керівні вказівки з розробки національної стратегії кібербезпеки (pp. 14-21). У 2014 році агентство ENISA також наголосило на необхідності створення національних стратегій кібербезпеки, заснованих на фактичних даних, шляхом проведення одноразових та періодичних оцінок цих стратегій (тобто вивчення результатів на основі попередньо встановлених критеріїв оцінки) та використання результатів цих оцінок для зміни стратегій та планів дій щодо реалізації стратегій.

Національні стратегії кібербезпеки можуть бути включені в єдиний документ або частини стратегії можуть бути розподілені між різними документами, кожен з яких охоплює певні аспекти кібербезпеки. Міжнародний союз електрозв'язку (МСЕ) має архів даних національних стратегій кібербезпеки (National Cybersecurity Strategies repository), який включає національні стратегії, плани та інші документи, що стосуються кібербезпеки. Крім того, Центр передового досвіду із спільного захисту від кіберзагроз Організації Північноатлантичного договору (НАТО) розміщує на своєму веб-сайті стратегії кібербезпеки та пов'язані з ними документи, прийняті країнами-членами НАТО та країнами, що не входять до НАТО. Більше того, агентство ENISA розробило інтерактивну карту, на якій показані національні стратегії кібербезпеки держав-членів Європейського союзу та завдання цих стратегій (наприклад, боротьба з кіберзлочинністю; створення можливостей реагування на інциденти; участь у міжнародному співробітництві; встановлення вимог щодо базових рівнів безпеки; створення державно-приватних партнерств тощо).

8.3 Міжнародне співробітництво з питань кібербезпеки

Міжнародна спілка електрозв'язку (МСЕ), установа Організації Об'єднаних Націй, що є «головним всесвітнім форумом, в рамках якого сторони можуть домагатися консенсусу щодо широкого кола питань, що впливають на майбутній напрямок розвитку галузі ІКТ», ініціював Глобальну програму яка представляє для МСЕ «основу міжнародного співробітництва, мета якого полягає в тому, щоб запропонувати стратегії для пошуку рішень у галузі зміцнення довіри та безпеки в умовах інформаційного суспільства». У Глобальній програмі кібербезпеки МСЕ визначено п'ять стратегічних принципів: правові заходи, технічні заходи, організаційні заходи, створення потенціалу та співробітництво. *Джерело:* Асауо, Grace. (2017). Огляд глобального індексу кібербезпеки. Міжнародна спілка електрозв'язку, 2-а щорічна нарада Співтовариства практики

побудови композитних індикаторів та систем показників (9-10 листопада 2017 року, Іспра, Італія).

Правовий принцип зосереджений на уніфікації регламентів та законів, що стосуються кібербезпеки та кіберзалежних злочинів, а також злочинів, які скоюються з використанням кіберпростору. Як приклад можна навести закони про боротьбу з кіберзлочинністю, закони та регламенти про захист даних, закони про кіберзлочинність та інші відповідні закони (наприклад, Данія, Закон про захист даних 2018 року, Фіджі, Указ про злочини 2009 року: розділ 6 - комп'ютерні злочини, Об'єднані Арабські Емірати, Федеральний закон №.1 від 2006 року про електронну комерцію та укладання угод в електронному вигляді; неправомірне використання комп'ютерних технологій 1990 року та Закон про захист даних 2018).

Технічний принцип охоплює існуючі технічні установи, стандарти та протоколи кібербезпеки, а також заходи, необхідні для боротьби з загрозами кібербезпеки. Прикладом технічної установи є група реагування на порушення комп'ютерного захисту (CERT), яка визначається як «організація або група, яка надає чітко визначеному колу клієнтів послуги та підтримку як для запобігання інцидентам, пов'язаним з комп'ютерною безпекою, так і для реагування на них». Можливості CERT варіюються в залежності від діапазону та поєднання пропонованих реактивних та попереджувальних послуг управління, а також послуг управління якістю безпеки. Наприклад, такі послуги можуть включати оперативне реагування на інцидент, щоб отримати можливість для швидкої локалізації та розслідування атаки і сприяти швидкому відновленню до вихідного стану. На додаток до реагування на інциденти CERT може брати участь в інших заходах, таких як оцінка вразливостей та інструктажів з питань безпеки; участь у таких додаткових заходах залежить від самої організації (Proffitt, 2007). Країни можуть мати національні, урядові та галузеві CERT та групи реагування на інциденти у сфері комп'ютерної безпеки (або CSIRT) або

використовувати комбінацію за участю кількох або всіх таких груп. CERT/CSIRT також створили у своїх регіонах групи обмінюватись інформацією, координації дій тощо. (наприклад, Азіатсько-тихоокеанська група CERT або APCERT; Африканська група CERT або AfricaCERT).

Чи знаєте ви?

CERT® є зареєстрованим товарним знаком Інституту розробки програмного забезпечення Університету Карнегі-Меллона. Групи CSIRT можуть вимагати дозволу на використання символу CERT. На наступному веб-сайті вказано кроки, які слід зробити групі CSIRT для отримання дозволу на використання символу CERT.

Принцип, пов'язаний з *організаційними заходами*, включає організаційні структури та заходи політики у сфері кібербезпеки та установи, відповідальні за координацію політики забезпечення кібербезпеки. Цей принцип включає національні стратегії кібербезпеки та національні механізми забезпечення кібербезпеки, а також регулюючі органи, які здійснюють нагляд за реалізацією цих стратегій і механізмів (наприклад, Рада з кібербезпеки в Ісландії; Федеральне управління з інформаційної безпеки в Німеччині; Управління кібербезпеки та інформаційного забезпечення в Великобританії, Міністерство науки, інформаційних технологій та планування майбутнього в Республіці Корея; Департамент національного планування та Міністерство інформаційних технологій та зв'язку в Колумбії тощо).

Принцип *створення потенціалу* охоплює зусилля щодо заохочення обізнаності, освіти та навчання у сфері кібербезпеки. Прикладами можуть бути кампанії з інформування громадськості, дослідження та розробки в галузі кібербезпеки, професійна підготовка, а також національні освітні програми та навчальні плани. Наприклад, у Домініканській Республіці «*Національна комісія з питань суспільства інформації та знань (CNSIC)*» здійснює офіційно визнану національну програму підвищення обізнаності, яка пропагує норми, цінності та соціальну поведінку, що сприяють

сумлінності, креативності та інноваціям при навігації в кіберпросторі». Відповідні кампанії з підвищення обізнаності та освіти у сфері кібербезпеки були ініційовані й іншими країнами (див. вставку «Приклади національних та міжнародних кампаній щодо підвищення обізнаності та освіти у сфері кібербезпеки»). На додаток до цих інформаційних та просвітницьких кампаній у галузі кібербезпеки МСЕ надає інструменти для надання допомоги країнам у їх зусиллях щодо створення потенціалу. Ці інструменти призначені для «збору інформації про конкретні загрози, яким наражається країна» (дослідна мережа Honeypot або HORNET), та «агрегування та розповсюдження відповідних даних про інциденти» (Механізм попередження та складання звітів про інциденти або AWARE).

Приклади національних та міжнародних кампаній щодо підвищення обізнаності та освіти у сфері кібербезпеки

Австралія

В Австралії проводиться кампанія Stay Smart Online, яка надає приватним особам та малим підприємствам інформацію про те, як захистити себе від загроз кібербезпеці та знизити такі загрози. Крім того, управління Комісара з електронної безпеки *Австралії через свій веб-сайт сприяє забезпеченню безпеки в Інтернеті, надаючи освітні матеріали для дітей, батьків та інших осіб та інформуючи їх про різні форми кіберзлочинності та способах захисту від них в Інтернеті, а також надає користувачам можливість повідомляти про певні кіберзлочини через свій веб-сайт.* Наприклад, це управління має портал для розміщення повідомлень про випадки наруги з використанням зображень, на якому потерпілі можуть залишати повідомлення про випадки розміщення (завантаження/розповсюдження) їх фотографій інтимного або сексуального характеру без їхньої згоди. Після отримання такого повідомлення управління вживає заходів щодо виявлення цих фотографій та звертається до відповідних соціальних мереж або Інтернет-посередників

(а в деяких випадках і до самих зловмисників) з вимогою про зняття та видалення фотографій.

Канада

У Канаді компанія Get Cyber Safe надає приватним особам та підприємствам інформацію про ризики кібербезпеки та способи, за допомогою яких приватні особи та підприємства можуть захистити себе від загроз кібербезпеці.

Великобританія

GetSafeOnline, що здійснюється у Великій Британії, є ініціативою щодо підвищення поінформованості про кібербезпеку, яка надає людям інформацію про безпечні методи роботи вдома і на робочому місці.

США

Ініціатива StaySafeOnline Національного альянсу з кібербезпеки пропонує людям інформацію про безпечні методи роботи в Інтернеті, кіберзлочинності, захист ключових облікових записів у мережі та цифрових пристроїв та контроль конфіденційності. Національний місячник знань про кібербезпеку (National Cybersecurity Awareness Month, NCSAM), який проводиться у жовтні кожного року, був ініційований у 2004 році державно-приватним партнерством (а саме Національним альянсом з кібербезпеки та Міністерством внутрішньої безпеки США) з метою надання ресурсів, людям для безпечної навігації в Інтернеті та використання цифрових пристроїв захищеним чином. Так само Європейський місячник кібербезпеки (ECSM), кампанія з підвищення поінформованості про кібербезпеку, яка також проводиться у жовтні кожного року, спрямована на інформування людей про кіберзлочинність та кібербезпеку з метою зміни небезпечних методів роботи в Інтернеті. Більше того, День безпечного Інтернету (Sfer Internet Day, SID) відзначається в усьому світі щороку в лютому з метою сприяння безпеці та підтримки здорових та щасливих Інтернет-спільнот.

Міністерство внутрішньої безпеки США також організувало міжнародну кампанію з освіти та підвищення поінформованості про кібербезпеку, відому під назвою «Зупинися. Подумай! Підключися» (STOP. THINK. CONNECT.™). Підприємства, національні урядові міністерства та НУО національного масштабу, наприклад, у Болівії, Панамі, Монголії, Тонга, Нігерії, Тринідаді та Тобаго, Антигуа та Барбуді, Ямайці, Індії та Японії (і багатьох інших країнах) прийняли та розгорнули у себе таку інформаційно-просвітницьку кампанію. Міністерство внутрішньої безпеки США створило інформаційний пакет своєї кампанії STOP.THINK.CONNECT.™, щоб забезпечити можливість іншим країнам ініціювати аналогічні внутрішні кампанії на території своїх країн. Цей пакет включає передовий досвід здійснення програми інформаційної роботи, зразковий план інформаційної роботи та показники успіху кампаній щодо підвищення поінформованості про кібербезпеку (European Cyber Security Month, nd).

Південно-Африканська Республіка

Південно-Африканська Республіка розгорнула кілька кампаній щодо підвищення обізнаності про кібербезпеку, які проводять лише наукова спільнота, приватні організації та державні установи (Dlamini and Modise, 2012). Крім того, Міністерство телекомунікацій та поштового зв'язку ПАР створило портал кібербезпеки (Cybersecurity Hub), який містить інформацію та матеріали про заходи захисту від кіберзлочинності та кампанії щодо підвищення поінформованості про кібербезпеку. Так само, як у США та інших країнах, у ПАР ініційовано кампанію щодо підвищення обізнаності про кібербезпеку, яка проводиться щорічно в жовтні (Pazvakavambwa, 2016).

М'янма

CyberBayKin, кампанію з кібербезпеки в М'янмі, була запущена в 2018 році з метою підвищення поінформованості про кібербезпеку та ризики. Вона ініційована Університетом Монаша (Австралія) та компанією

Kernellix Co., Ltd. (М'янма) у співпраці з Національним центром кібербезпеки Міністерства транспорту та комунікацій М'янми. Шість м'янманських комічних персонажів, розроблених для кампанії, було представлено перед її запуском. У ході цієї річної кампанії на платформі кампанії у Facebook кожні два тижні з'являються комічні ілюстрації, які сприяють підвищенню поінформованості про кібербезпеку. Компанія підтримується та фінансується Міністерством закордонних справ та торгівлі Австралії в рамках стратегії міжнародної взаємодії у кіберпросторі та Школою соціальних наук Університету Монаша.

Принцип *співробітництва* зосереджений на міжустановчих та державно-приватних партнерствах, мережах обміну інформацією та угодах про співпрацю. Як приклад можна навести австралійську стратегію міжнародної взаємодії в кіберпросторі (International Cyber Engagement Strategy), метою якої є розвиток державно-приватного партнерства та зміцнення співробітництва між країнами. Інші приклади включають партнерства на рівні країн та обмін інформацією з МСЕ, Агентством з мережевої та інформаційної безпеки Європейського Союзу (ENISA), Організацією з безпеки та співробітництва в Європі (ОБСЄ) та Організацією Північноатлантичного договору (НАТО), а також договори про співробітництво, такі як Конвенція Ради Європи про комп'ютерні злочини 2001 року, Угода про співпрацю держав-учасниць Співдружності Незалежних Держав у боротьбі зі злочинами у сфері комп'ютерної інформації 2001 року, Конвенція Ліги арабських держав про боротьбу зі злочинами, Конвенція¹ Африканського союзу про кібербезпеку та захист персональних даних 2014 року та багато інших.

Порівняльний аналіз національних стратегій кібербезпеки десяти країн (Австралії, Канади, Фінляндії, Франції, Німеччини, Японії, Нідерландів, Іспанії, США та Великобританії), проведений Організацією економічного співробітництва та розвитку (ОЕСР) у 2012 році, виявив відмінності у визначеннях поняття кібербезпеки, також подібності у

підходах країн до комплексного вирішення проблеми кібербезпеки, які передбачають використання у тому чи іншій мірою кожного із стратегічних принципів – правові, технічні, організаційні заходи, створення потенціалу та співробітництво.

Для розробки всеосяжної та ефективної національної стратегії кібербезпеки, МСЕ, у своєму Посібнику з розробки національної стратегії кібербезпеки, опублікованому в 2018 році, пропонує включити до стратегії такі тематичні галузі: управління (розглядається в даному модулі); управління ризиками (тобто процес виявлення, оцінки та контролю та/або ліквідації загроз); забезпечення готовності та стійкості; послуги життєво важливої інфраструктури та основні послуги; розвиток можливостей, створення потенціалу та підвищення обізнаності; законодавство та регулювання; та міжнародне співробітництво. Інші організації також пропонують посібники з розробки політики та нормативно-правової бази в галузі кібербезпеки, вжиття технічних та організаційних заходів, створення потенціалу та співробітництва (наприклад, модель управління кіберпростором (Commonwealth Cybergovernance Model), прийнята у 2014 році Телекомунікаційною організацією Співдружності).

8.4 Стан справ у галузі кібербезпеки

Стан справ у сфері кібербезпеки є терміном, який використовується для опису можливостей країни, організації або компанії для забезпечення кібербезпеки. Існує кілька інструментів, що використовуються для оцінки стану справ у галузі кібербезпеки. Одним із таких інструментів є Глобальний індекс кібербезпеки (ГІК) Міжнародного союзу електрозв'язку. Згідно з МСЕ, ГІК є інструментом нарощування потенціалу, який оцінює відданість країн справі забезпечення кібербезпеки, визначає їх стан справ у галузі кібербезпеки та аспекти, що потребують поліпшення. Стан справ країн у сфері кібербезпеки може оцінюватися на основі п'яти принципів (правові, технічні, організаційні заходи, створення потенціалу та співробітництво), визначених у

Глобальній програмі кібербезпеки МСЕ. Зокрема, країни отримують бали ГІК залежно від рівня їхньої прихильності до цих п'яти принципів. Ці оцінки відносять країни до груп *початківців* (тобто країн, які роблять перші кроки, що демонструють їхню прихильність до цих принципів), *що розвиваються* (тобто країн, які віддані цим принципам) і *провідних* країн (тобто країн, які прийняли високі зобов'язання щодо цих принципів).

Результати дослідження Глобального індексу кібербезпеки 2017 показали, що половина країн-респондентів не мають національної стратегії кібербезпеки. Результати дослідження Глобального індексу кібербезпеки 2017 року також виявили значні відмінності між державами всередині та за межами їхніх регіонів з точки зору прийнятих зобов'язань щодо забезпечення кібербезпеки. Результати також показали, що рівень зобов'язань країн щодо забезпечення кібербезпеки варіює залежно від конкретного показника (тобто країни отримали високі оцінки за одним показником, але середні та низькі оцінки за іншими показниками). Однак, для того, щоб зусилля були ефективними, зобов'язання в галузі кібербезпеки повинні бути виконані за всіма показниками.

Глобальний центр створення потенціалу в галузі кібербезпеки (GCSCC) при Оксфордському університеті розробив модель зрілості потенціалу в галузі кібербезпеки (ЗПК) для оцінки стану справ країн у сфері кібербезпеки (тобто зрілості можливостей забезпечення кібербезпеки) шляхом вивчення зусиль країн у таких галузях, як «нормативне регулювання та стратегія в галузі кібербезпеки», «кіберкультура та суспільство», «освіта, навчання та навички в галузі кібербезпеки», «нормативно-правова база», а також «стандарти, організації та технології». Ця оцінка дозволяє країнам отримати інформацію про рівень зрілості їхнього потенціалу: *початковий* (тобто кібербезпека відсутня або лише починає розвиватися); *що формується* (тобто існує деяка кібербезпека); *встановлений* (тобто кібербезпека існує; приділяється мінімальна увага питанню виділення ресурсів); *стратегічний* (тобто

усвідомлений та зважений вибір щодо кібербезпеки); та *динамічний* (тобто заходи забезпечення кібербезпеки адаптуються до змін умов та потреб). Модель СММ використовувалася для оцінки багатьох країн по всьому світу окремо або в рамках регіонального дослідження (Global Cyber Security Capacity Centre, 2018). На додаток до моделі ЗПК, Глобальний центр створення потенціалу в галузі кібербезпеки розробив портал Cybersecurity Capacity Portal, який містить матеріали щодо створення потенціалу в галузі кібербезпеки, інформацію про передову практику та полегшує обмін інформацією, щоб допомогти країнам покращити стан справ у галузі кібербезпеки.

Деякі країни також реалізували рамкові програми з метою сприяння державному та приватному секторам у покращенні їхнього стану справ у галузі кібербезпеки. Як приклад можна навести прийняту Національним інститутом стандартів і технологій США (NIST) Рамкову концепцію зміцнення кібербезпеки життєво важливих інфраструктурних систем (Framework for Improving Critical Infrastructure Cybersecurity), стандарти та передові практичні методи сприяння державному та приватному секторам у покращенні їх стану справ у галузі кібербезпеки. У 2017 році було прийнято виконавчий указ Президента США «Про зміцнення кібербезпеки федеральних мереж та критичної інфраструктури», який наказував федеральним агентствам використовувати цей документ для зміцнення своїх сил і засобів забезпечення. Цей документ був також прийнятий та/або адаптований приватними компаніями та організаціями у США та деяких інших країнах (наприклад, в Італії, Уругваї та на Бермудських островах). Асоціація з аудиту та контролю інформаційних систем (при згадці якої тепер використовують лише акронім ISACA) розробила програму аудиту для перевірки ефективності заходів забезпечення кібербезпеки, які компанії, організації та агенції впровадили з використанням Рамкової концепції NIST (ISACA, 2017). Так само нормативні акти уряду Китаю, такі як Спеціальний регламент про розкриття інформації комерційними

банками та заходи щодо подання звітів про інциденти інформаційної безпеки в Інтернеті, та нормативні акти Тайваню, такі як Посібник з подання звітів про серйозні непередбачені інциденти в банках та заходи щодо подання звітів про інциденти в системі безпеки національної інформаційної та комунікаційної системи та реагування на них є регламентами, прийнятими з метою сприяння розвитку державно-приватного партнерства в галузі кібербезпеки.

Визнавши, що стан справ у сфері кібербезпеки залежить від кількості та якості кадрових ресурсів, що забезпечують кібербезпеку, у 2017 році Сполучені Штати також створили системну структуру трудових ресурсів у галузі кібербезпеки в рамках Національної освітньої ініціативи в галузі кібербезпеки (NICE) (Cybersecurity Workforce Frame). Ця структура є частиною стратегічних цілей ініціативи NICE, спрямованих на розвиток трудових ресурсів за допомогою визначення рівня знань, навичок та умінь, необхідних для різних посад у системі кібербезпеки, а також на надання керівних вказівок освітнім установам та роботодавцям щодо розробки та здійснення навчальних програм та професійної підготовки. Проблема нестачі кваліфікованих професіоналів у галузі кібербезпеки, що спостерігається у всьому світі, наочно свідчить про необхідність приділяти увагу заходам щодо розвитку трудових ресурсів у галузі кібербезпеки у більшості країн.

Висновок

Уряди, неурядові організації, освітні установи, підприємства та приватні особи широко використовують інформаційно-комунікаційні технології (ІКТ). Взаємозалежність пристроїв і систем у всьому світі та важливість ІКТ для економічної та національної безпеки країн, а також для національного та світового розвитку вимагають вжиття колективних та узгоджених заходів у відповідь усіма країнами світу. Національні стратегії кібербезпеки вживаються з метою опису способів здійснення захисту, а також заходів, які необхідно вжити, та організацій, відповідальних за

нагляд за реалізацією цих заходів. Існують показники, які можна використовуватиме оцінки ефективності цих стратегій. Більше того, є інструменти та ресурси, які дозволяють країнам оцінювати свої сили та засоби забезпечення кібербезпеки та допомагають їм покращити свій стан справ у галузі кібербезпеки.

Питання для самоперевірки

1. Якими принципами керується управління Інтернетом?
2. Які перешкоди для універсального управління Інтернетом?
3. Які основні риси стратегії кібербезпеки?
4. Які відмінності між стратегіями кібербезпеки та стратегіями запобігання кіберзлочинності?
5. Які етапи життєвого циклу стратегії кібербезпеки?
6. Які зусилля спрямовані на посилення та/або сприяння міжнародній співпраці з питань кібербезпеки?
7. Яким чином було оцінено стан кібербезпеки в різних країнах?

ЛЕКЦІЯ 9. КІБЕРЗЛОЧИННІСТЬ. СТРАТЕГІЯ, ПОЛІТИКА, ПРОГРАМИ ПРОТИДІЇ

9.1 Активи, уразливості та загрози

9.2 Ситуаційне попередження злочинності

9.3 Виявлення інцидентів, реагування на них, відновлення та забезпечення готовності

9.1 Активи, уразливості та загрози

Заходи забезпечення кібербезпеки реалізуються з метою захисту активів, які визначаються як «щось важливе або цінне, включаючи людей, майно, інформацію, системи та обладнання», таких як працівники організації, цифрові пристрої, комп'ютерне програмне забезпечення та дані. Активи сприйнятливі (тобто вразливі) до різних видів шкоди. Зокрема, активи мають внутрішні (або вбудовані) та зовнішні (або привнесені) *уразливості*. Наприклад, стосовно інформаційно-комунікаційних технологій (ІКТ), внутрішні вразливості можуть бути присутніми в конструкції системи, конфігураціях системи безпеки, апаратному та програмному забезпеченні та в інших компонентах. Прикладом може бути програмна помилка. У 2018 році було виявлено програмну помилку в гаманці криптовалюти Monero, яка дозволяла окремим особам використовувати цю вразливість для незаконного подвоєння сум переказу криптовалюти. Навпаки, зовнішні вразливості не присутні всередині самих активів, таких як пристрої ІКТ. Прикладом такої вразливості є користувач ІКТ. Користувач може виконувати дії, які роблять пристрій сприйнятливим до зараження шкідливими програмами (наприклад, відкривати вкладення в електронних листах від невідомих відправників). Вбудовані та привнесені властивості роблять активи вразливими для *загроз* (тобто до всього, що може спричинити несприятливі наслідки). Ці погрози можуть завдати ненавмисного та навмисного збитку. Наприклад, апаратне забезпечення цифрового

пристрою може працювати зі збоями або може бути навмисно пошкоджено внаслідок експлуатації уразливостей вбудованого програмного забезпечення.

Ризик

Рішення про захист активів приймаються за умов невизначеності; тобто вони приймаються за відсутності повної інформації про потенційні загрози, уразливості та експлуатації цих уразливостей. Спочатку *ризик* мав вузьке визначення як ймовірність (або можливість) загрози та її впливу (або наслідків) у разі її матеріалізації. Ця концепція ризику зображується такою формулою:

$$P = \text{Можливість} \times \text{Наслідки}$$

Формули, подібні до наведеної вище, використовуються для кількісної оцінки ризиків.

У 2009 році Міжнародна організація зі стандартизації (ISO), міжнародна неурядова організація, яка розробляє та публікує міжнародні стандарти з метою уніфікації практики, що використовується в різних країнах, запропонувала інше визначення, яке мало служити еталоном для сприяння взаєморозумінню та послідовності при використанні основних понять ризику та термінів, що належать до ризику. Зокрема, у Керівництві ISO 73 (2009) ризик визначається як «вплив невизначеності на цілі», такі як короткострокові та/або довгострокові фінансові цілі. У цьому визначенні ризику *невизначеність* означає «стан, також частково, відсутності інформації щодо розуміння чи знання події, його наслідків або ймовірності».

Процес оцінки ризиків (рис.1) передбачає виявлення вразливостей активів, визначення внутрішніх та зовнішніх загроз та/або отримання інформації про них від засобів масової інформації, державно-приватних партнерств та/або інших осіб з державного та приватного секторів, а також визначення наслідків та ймовірностей загроз. Метою оцінки ризиків є виявлення загроз; шкоди (тобто несприятливої дії), яка може бути

заподіяна, враховуючи можливість експлуатації вразливостей; і ймовірності того, що шкода буде заподіяна».

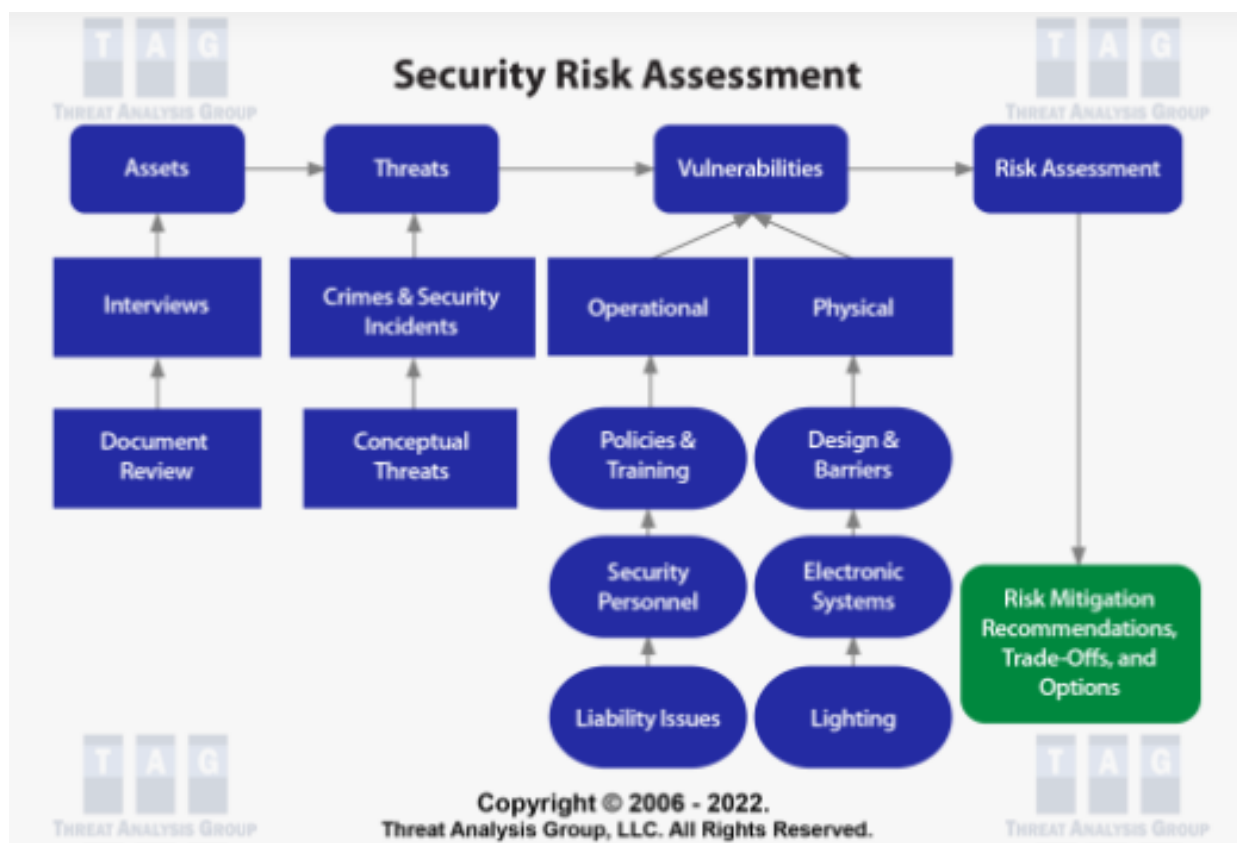


Рисунок 1: Threat Analysis Group. Управління ризиками безпеки - методологія *Security Risk Management - Methodology*.

Після завершення оцінки ризиків визначаються заходи реагування на ризики (тобто заходи для *обробки ризиків*), пріоритетність яких встановлюється з урахуванням наявних ресурсів (наприклад, фінансових) і потреб. На цьому етапі реалізуються заходи щодо усунення, зменшення або пом'якшення ризиків.

Розкриття інформації про вразливість

Терміни «інформаційна безпека» і «кібербезпека» використовуються як взаємозамінні, хоча це не зовсім правильно. Незважаючи на відсутність узгодженого визначення поняття інформаційної безпеки, широко використовується визначення, включене до стандарту ISO/IEC 27002. У стандарті ISO/IEC 27002 інформаційна безпека визначається як «збереження конфіденційності,

цілісності та доступності інформації». Як і у разі інформаційної безпеки, немає універсального визначення поняття кібербезпеки. Згідно з Міжнародним союзом електрозв'язку (МСЕ), «кібербезпека полягає у прагненні забезпечити досягнення та збереження властивостей безпеки у ресурсів організації або користувача, спрямованих проти відповідних загроз безпеці в кіберсередовищі». Таким чином, кібербезпека має на увазі захист не тільки кіберпростору, «але і тих, хто функціонує в кіберпросторі, і будь-які їх ресурси, які можуть бути доступні через кіберпростір».

Чи знаєте ви?

Стандарт ISO/IEC 27002 включає 14 областей контролю інформаційної безпеки, а також посібник з реалізації заходів контролю інформаційної безпеки та вимоги для кожного з цих заходів контролю. Цими областями є: політика інформаційної безпеки; організація інформаційної безпеки; безпека персоналу; управління активами; контроль доступу; криптографія; фізична безпека та захист від природних загроз; безпеку виробничої діяльності; безпека обміну інформацією; придбання, розробка та обслуговування систем; відносини із постачальниками; керування інцидентами інформаційної безпеки; аспекти інформаційної безпеки у менеджменті безперервності бізнесу; та відповідність.

Інформаційна безпека та кібербезпека залежать від розкриття інформації про вразливість. Коли вразливості виявлено дослідниками та фахівцями в даній галузі, розкриття інформації про такі вразливості може бути повним або відповідальним. *Повне розкриття* передбачає оприлюднення інформації про вразливість програмного або апаратного забезпечення в Інтернеті (наприклад, на веб-сайті) до того, як ці уразливості будуть усунені. Навпаки, *відповідальне розкриття* має на увазі нерозкриття інформації про вразливість доти, доки організація, відповідальна за апаратне або програмне забезпечення, не усуне вразливість. При відповідальному розкритті дослідник чи фахівець

зв'язується із порушеною організацією і чекає, доки організація не випустить виправлення для виявленої вразливості. Після випуску виправлення дослідник або фахівець може офіційно розкрити інформацію про вразливість та отримати визнання та винагороду за знаходження вразливості. При використанні такого методу розкриття інформації дослідник або фахівець може просити про надання йому так званого ідентифікатора загальновідомих уразливостей інформаційної безпеки (Common Vulnerabilities and Exposures, CVE). CVE, який являє собою «список загальних ідентифікуючих елементів загальновідомих уразливостей кібербезпеки», використовується для відстеження вразливостей в основних елементах програмного забезпечення, а також осіб, які виявляють такі вразливості. На додаток до методів повного та відповідального розкриття інформації, дослідник або фахівець може вибрати принцип нерозкриття вразливості. Ще одним методом розкриття інформації є *координоване розкриття вразливостей*, яке означає «процес збору інформації від осіб, які виявили вразливості, координації обміну цією інформацією між відповідними зацікавленими сторонами і розкриття інформації про наявність уразливостей програмного забезпечення та пом'якшення негативних наслідків різних».

Існують керівні принципи передової практики щодо розкриття інформації про вразливості та управління вразливістю. Як приклад можна навести посібники з передової практики, розроблені та опубліковані Міжнародною організацією зі стандартизації та Міжнародною електротехнічною комісією, для розкриття вразливостей (ISO/IEC 29147) та процесів управління *вразливістю* (ISO/IEC 30111).

Заходи забезпечення кібербезпеки та зручність використання

В ідеалі заходи реагування на ризики повинні мати на меті захист конфіденційності, цілісності та доступності систем, мереж, послуг та даних при одночасному забезпеченні зручності використання цих заходів. *Зручність використання цифрових*

пристроїв (тобто легкість, з якою вони можуть використовуватися) часто має перевагу перед безпекою цих пристроїв та їх вмісту. Однак безпека та зручність використання не обов'язково є взаємовиключними. Заходи кібербезпеки можуть забезпечувати як безпеку, так і зручність використання.

До заходів кібербезпеки відносяться заходи, спрямовані на встановлення особи користувача, щоб запобігти несанкціонованому доступу до систем, послуг та даних. Ці заходи *автентифікації* включають перевірку того, «що ви знаєте» (наприклад, паролі, парольні фрази та PIN-коди), «що ви маєте» (наприклад, смарт-карти та токени) і «ким ви є» (наприклад, біометричні дані, такі як відбитки пальців). Багатофакторна аутентифікація передбачає використання двох або більше таких методів аутентифікації для встановлення особи користувача.

Ще одним типом заходів кібербезпеки є контроль доступу. *Засоби контролю доступу*, які встановлюють привілеї, визначають санкціонований доступ і запобігають несанкціонованому доступу, включають заходи автентифікації та інші заходи, призначені для захисту імен та паролів для входу в систему, додатки, веб-сайти, соціальні мережі та інші онлайн-платформи та цифрові пристрої. Як приклад, можна привести обмеження кількості спроб введення пароля на смартфоні. На смартфонах є опція, що дозволяє користувачам стирати всі дані на пристрої після певної кількості невдалих спроб введення пароля. Ця функція була створена для того, щоб забезпечити користувачам можливість захисту даних на своїх пристроях у разі крадіжки цифрового пристрою та/або отримання доступу до них без авторизації користувача.

Інші приклади засобів контролю доступу включають додавання часу очікування при кожному невірному введенні пароля та/або обмеження кількості невдалих спроб введення пароля, які можуть бути допустимими протягом дня, та блокування облікових записів користувачів на деякий час. Ці засоби керування, які контролюють спроби входу в систему, призначені

для захисту від спроб отримати несанкціонований доступ до облікових записів користувачів. Зокрема такі тимчасові затримки служать для захисту від атак методом «грубої сили».

Чи знаєте ви?

Повністю автоматизований публічний тест Т'юринга для розрізнення комп'ютерів та людей (CAPTCHA) використовується для запобігання атакам методом «грубої сили». Проте дослідження показало, що малюнки CAPTCHA можна обійти.

Атака «грубою силою» – це використання *скрипта* (тобто комп'ютерної програми) або *робота* для вгадування (методом спроб та помилок) облікових даних користувача (тобто імені користувача та/або пароля/коду доступу). При атаках «грубою силою» використовуються, серед іншого, спільні паролі або зламані облікові дані для входу в систему. У 2018 році було виявлено, що функцію майстер-паролю, яка дозволяла користувачам шифрувати паролі, що зберігаються у браузері Mozilla Firefox (веб-браузер) можна легко зламати з використанням атаки методом «грубої сили».

Паролі або генеруються системою, або створюються користувачем. *Паролі, що генеруються системою* (тобто паролі, створені програмою), є важковідгадуваними і можуть витримати атаки парольних зломщиків (хоча це залежить від довжини паролів). Проблема, пов'язана з паролями, що генеруються системою, полягає у складності їх запам'ятовування. Це призводить до того, що користувачі записують пароль, наприклад, на папір або зберігають його у браузері, програмі або цифровому пристрої. Тому *паролі, створювані користувачем*, є кращими. Однак такі паролі, що генеруються користувачем, також можуть бути складними для запам'ятовування. Системи, програми та онлайн-платформи часто встановлюють складні правила створення паролів, яким повинні дотримуватися користувачі, вимагаючи, щоб паролі відповідали

мінімальній встановленій довжині і включали комбінації літер верхнього та нижнього регістру, цифр та символів. Таким чином, як і паролі, що генеруються системою, більшість паролів, створених користувачами, є важкозапам'ятовуваними.

Користувачам також рекомендується мати різні паролі для кожного облікового запису. Мета цієї рекомендації полягає в мінімізації шкоди, заподіяної користувачам, у разі злому даних для доступу до одного з їхніх облікових записів. У 2017 році одна дослідницька компанія виявила в Інтернеті файл з 1,4 мільярдами імен користувачів та паролів для різних соціальних мереж, ігор, сайтів трансляції телепередач та фільмів та інших сайтів мережі Інтернет. Якщо хтось із цих осіб повторно використовує паролі, такий пролом у системі захисту ставить під загрозу безпеку інших облікових записів в Інтернеті (де використовуються ті ж ім'я користувача та пароль). Хоча використання різних і складних паролів для кожного облікового запису може забезпечити певний рівень безпеки для окремих користувачів, це зрештою негативно впливає на зручність їх використання (тобто їх запам'ятовування). Як справедливо відзначають Адамс, Сасс і Лундт (Adams, Sasse and Lundt), «велика кількість обмежень у механізмах автентифікації створюють велику кількість проблем, пов'язаних із зручністю використання».

Замість паролів пропонується використовувати різні схеми автентифікації. Використання альтернативних схем аутентифікації, таких як техніка біометричної ідентифікації, пов'язане з несприятливими наслідками соціального та правового характеру і навіть наслідками безпеки. Як приклади можна навести смартфони Apple iPhone зі сканерами TouchID, який дозволяє користувачам розблокувати свої пристрої за допомогою відбитка пальця, і FaceID, який за допомогою технології розпізнавання обличчя дозволяє користувачам розблокувати телефони шляхом сканування свого обличчя (алгоритми FaceID сьогодні працюють навіть якщо людина в масці або окулярах). У Сполучених Штатах

працівники системи кримінального правосуддя не мають права примушувати людей надавати свої паролі; такий захист не поширюється на відбитки пальців та інші біометричні дані (наприклад, справа *Virginia v. Baust*, 2014 та справа *State v. Diamond* , 2018, коли суди ухвалили, що особи можуть бути примушені до використання своїх відбитків пальців для розблокування телефону).

Біометрія та право не свідчити проти самого себе

Згідно з п'ятою поправкою до Конституції Сполучених Штатів Америки, «ніхто не повинен притягатися до відповідальності за караний смертю чи іншим чином злочин інакше, як за поданням або обвинувальним висновком Великого журі, за винятком справ, які порушуються у сухопутних чи військово-морських силах, або в ополченні , коли воно покликане на дійсну службу під час війни на період небезпечного для суспільства становища; ніхто не повинен за те саме правопорушення двічі наражатися на загрозу позбавлення життя або порушення тілесної недоторканності; ніхто не повинен змушуватись у кримінальній справі свідчити проти самого себе; ніхто не може бути позбавлений життя, свободи чи власності без належної правової процедури; приватна власність не повинна вилучатись для громадського користування без справедливого відшкодування».

Одним із прав, передбачених п'ятою поправкою, є право не свідчити проти себе (в інших випадках відоме як право на захист від примусу до самозвинувачення). У справі *Schmerber v. California* (1966) суд ухвалив, що «це право захищає обвинуваченого лише від примусу давати свідчення проти самого себе чи іншим чином подавати владі штату докази у формі письмових чи усних свідчень». Однак п'ята поправка до Конституції США «не передбачає жодного захисту від примусу до здавання відбитків пальців, фотографування чи вимірювання росту, явки до суду, предстання перед судом, позування, демонстрації ходи чи певного жестикулювання».

Більше того, суди США можуть зобов'язати підсудних здати зразок крові, слини чи голоси та багато іншого.

Пославшись на справу *United States v. Wade* (1967), суддя у справі *Virginia v. Baust* (2014) дійшов висновку, що оскільки процедура зняття відбитків пальців не вимагає від підсудного надання будь-яких відомостей, вона не підпадає під дію п'ятої поправки – те саме стосується надання ключів і ДНК підсудного. У зв'язку з цим, хоча відомості про паролі захищені відповідно до п'ятої поправки, цей захист не поширюється на відбитки пальців (і, у більш широкому значенні, на інші біометричні дані). Нерозповсюдження п'ятої поправки на біометричні дані було ще раз підтверджено у справі *State v. Diamond* (2018).

Нарешті, у Сполучених Штатах перевірка того, «ким ви є», може бути проведена у примусовому порядку (тобто люди можуть бути примушені до здачі відбитків пальців і, у ширшому розумінні, до сканування обличчя для розблокування смартфонів, у яких використовується технологія розпізнавання осіб), у той час як перевірка того, «що ви знаєте», як правило, не може проводитися примусово відповідно до п'ятої поправки до Конституції США (оскільки це суперечить праву не свідчити проти самого себе). Аналогічно, інші країни (наприклад, Австралія, Нова Зеландія, Індія та багато інших) та суди з прав людини (наприклад, Європейський суд з прав людини) не розглядають примусу до показу особи, здачі відбитків пальців або інших біометричних даних (наприклад, відбитків ніг) як порушення права не свідчити проти себе (наприклад, *Sorby v. Commonwealth* , 1983; Нова Зеландія, *King v. McLellan* , 1974; Індія, *State of UP v. Sunil* , 2017; та *Saunders v. United Kingdom*, 1996).

Люди вважаються найслабшою ланкою в ланцюзі кібербезпеки. Більше того, деякі дослідження показали, що інциденти в галузі кібербезпеки (тобто витоку даних та/або атаки на мережі, системи, послуги

та дані) є результатом людської помилки та нездатності застосувати заходи безпеки. У той час як велика увага приділяється ролі людей в інцидентах в галузі кібербезпеки, заходи кібербезпеки, що діяли в момент настання інциденту, можуть також відігравати певну роль у цьому інциденті. Реальність така, що заходи кібербезпеки (те, що вони фактично здатні зробити) та очікування користувачів щодо ефективності цих заходів безпеки (того, що, на їхню думку, вони роблять) часто не збігаються.

У публікаціях та дослідженнях, присвячених взаємодії людини та комп'ютера, пропонується, щоб заходи забезпечення безпеки цифрових пристроїв, систем, програм, додатків та онлайн-платформ розроблялися з урахуванням фактора користувачів. Така практика, однак, не є загальноприйнятою. Звичайною практикою є розробка систем та подальша модифікація взаємодії користувачів із системою для задоволення потреб у забезпеченні безпеки.

9.2 Ситуаційне попередження злочинності

Ситуаційне попередження злочинності (СПЗ) зосереджене на способах запобігання злочинів і скорочення можливостей їх скоєння. СПЗ вважається важливою частиною Керівництва Економічної та Соціальної Ради ООН (ЕКОСОС) щодо запобігання злочинності (Резолюція 2002/13).

Хоча концепція СПЗ застосовується до запобігання злочинності в реальному світі, вона також може використовуватися як запобігання кіберзлочинності в контексті практики забезпечення кібербезпеки. Стосовно кіберзлочинності заходи СПЗ спрямовані на скорочення та/або запобігання можливостям для вчинення правопорушень та підризу здібностей кіберзлочинців вчиняти злочини. Технічні заходи попередження кіберзлочинності є однією з форм ситуаційного попередження злочинності. Приклади таких технічних заходів включають програми виявлення шкідливих програм, *брандмауери*, які запобігають несанкціонованому доступу шляхом перевірки і блокування трафіку, і *системи виявлення вторгнень*, які дозволяють виявляти кібератаки,

несанкціонований доступ і несанкціоноване використання систем, мереж, даних, послуг.

Виділяють 5 стратегій та 25 методів запобігання та скорочення злочинності (ЗСЗ). П'ять стратегій попередження та/або скорочення злочинності включають: збільшення зусиль, що витрачаються (з боку злочинця) для скоєння злочину; збільшення ризиків виявлення та затримання; скорочення очікуваної нагороди за скоєння злочину; зниження кількості провокацій, які ведуть скоєння злочину; та усунення виправдань для скоєння злочину. Не всі стратегії та методи, перелічені в рамках цих стратегій, застосовуються до всіх видів злочинів. Більше того, методи та стратегії можуть частково збігатися, а деякі методи можуть використовуватися відразу в кількох стратегіях.

Двадцять п'ять методів ситуаційного попередження злочинності: збільшення зусиль зловмисника.

Збільшення зусиль – захист об'єкту, контроль доступу на об'єкті, контроль виходу, пере направлення правопорушників через закриття/перекриття ходів, вулиць тощо, контроль через блокування мобільних пристроїв, обмеження продажу небезпечних речовин тощо.

Збільшення ризиків – посилення охорони, покращення спостережності через покращення освітлення тощо, зниження можливості анонімного доступу до критичних об'єктів, використання керівників на місцях, підсилення формального спостереження.

Зменшення винагороди – приховання об'єктів, видалення об'єктів, ідентифікація власності, контроль (санкціонування) ринків збуту несанкціонованих об'єктів, позбавлення вигоди.

Зниження числа провокацій – зниження стресу через організацію черг і покращення сервісу, недопущення сварок, зниження рівня емоційного напруження, нейтралізація тиску з боку колективу, перешкоджання імітації, використанню неліцензійних виробів і порушенню авторських прав.

Усунення виправдань – введення правил, розміщення вказівних знаків, етикет, сприяння виконанню законів, контроль за вживанням психотропних речовин, таких як алкоголь, наркотики тощо.

Заходи ЗСЗ можуть застосовуватися, застосовувалися раніше та застосовуються в даний час для попередження та скорочення кіберзлочинності. Наприклад, один із методів, перерахованих у запропонованій Корнішем та Кларком (Cornish and Clark, 2003) стратегії ЗСЗ – збільшення ризиків виявлення та затримання – полягає у «використанні керівників на місцях». Стосовно кіберзлочинності, які керують на місцях, які контролюють поведінку в зазначеному місці, можуть бути постачальники Інтернет-послуг. Керівники на місцях використовуються для боротьби з кіберзлочинністю у соціальних мережах. Наприклад, Facebook збільшив кількість модераторів і посилив моніторинг контенту, що пропагує насильство і жорстокість, після того, як Стівен Стівенс (Steven Stephens) вбив людину і транслював це вбивство через FacebookLive. Деякі з цих методів ЗСЗ, що застосовуються для боротьби з кіберзлочинністю, можуть порушувати права людини (наприклад, при блокуванні або видаленні контенту).

Витіснення злочинності відбувається у випадку, коли злочин, який був націлений на один об'єкт, вчиняється щодо іншого об'єкта через чинні заходи безпеки. Всупереч широко поширеній думці, дослідження в першу чергу показують, що ситуаційне попередження злочинності необов'язково веде до витіснення злочинності. Зусилля правоохоронних органів, пов'язані з цими Інтернет-сайтами, не витіснили сутенерів із цих сайтів, які продовжили використовувати їх для реклами сексуальних послуг.

Заходи ЗСЗ зосереджені можливості матеріалізації загроз кібербезпеки у певний час. Таким чином, ці заходи вживаються на підставі припущення про те, що загрози *будуть* матеріалізовані, і тому необхідно вжити відповідних дій. У той час як заходи ЗСЗ переважно (але не виключно) спрямовані на перешкоджання скоєнню злочинів, реальність

така, що навіть після вжиття цих заходів злочин, найімовірніше, буде скоєно. У зв'язку з існуванням такої ймовірності реалізуються заходи, спрямовані на виявлення інцидентів у галузі кібербезпеки, реагування на них та відновлення після них.

9.3 Виявлення інцидентів, реагування на них, відновлення та забезпечення готовності

Виявлення інцидентів є процесом визначення загроз шляхом активного моніторингу активів та виявлення аномальної активності. Відразу після виявлення загрози вживаються відповідні дії для нейтралізації загрози (якщо ця загроза є активною на момент вжиття заходів реагування) та розслідування інциденту. Після вжиття заходів реагування на інцидент першим кроком у процесі відновлення є відновлення доступу та доступності систем, мереж, послуг та даних до стану, що існував до інциденту.

Процес відновлення також включає елемент планування, який вимагає визначення, розробки та остаточної реалізації заходів щодо посилення стійкості та забезпечення можливості відновлення систем, мереж, послуг та даних, які були недоступні, порушені, пошкоджені та/або скомпрометовані під час інциденту. Важливим елементом забезпечення стійкості є наявність сучасного *плану безперервності бізнесу* або *плану дій з врегулювання надзвичайних ситуацій* з викладенням інструкцій, які необхідно дотримуватися, та дій, які необхідно вжити у разі виникнення інциденту в галузі кібербезпеки. Простіше кажучи, цей план включає докладну інформацію про способи реагування на інцидент і відновлення після нього. Усі особи, які беруть участь у вжитті заходів реагування на інциденти в галузі кібербезпеки та відновлення після них, мають бути поінформовані про план дій щодо врегулювання надзвичайних ситуацій. При цьому необхідно організувати тренінги, включаючи навчання, призначені для перевірки ефективності та ефективності цих планів.

Прикладом навчань такого роду є вчення «Кібер-шторм» (Cyber Storm exercises) Міністерства внутрішньої безпеки США за участю представників національних публічних та приватних організацій, а також організацій з інших країн (наприклад, Австралії, Канади, Данії, Фінляндії, Франції, Німеччини, Угорщини, Італії, Японії, Нової Зеландії, Нідерландів, Швеції, Швейцарії та Великобританії), які проводяться з метою перевірки поточної практики обміну інформацією між цими організаціями, а також їх можливостей забезпечення готовності, захисту та реагування на інциденти в галузі кібербезпеки.

Питання для самоперевірки

1. Що таке актив?
2. Що таке загроза?
3. Що таке вразливість?
4. Що таке ризик?
5. Як оцінюється ризик?
6. Якими способами дослідники кібербезпеки виявляють уразливості?
7. Який зв'язок між кібербезпекою та юзабіліті?
8. Що таке ситуаційна профілактика злочинів? Як це можна застосувати до кіберзлочинності?
9. Які заходи кібербезпеки включено до виявлення інцидентів, реагування, відновлення та готовності?

ЛЕКЦІЯ 10

КОНФІДЕНЦІЙНІСТЬ ТА ЗАХИСТ ДАНИХ. НЕДОТОРКАННІСТЬ ПРИВАТНОГО ЖИТТЯ

10.1 Недоторканість приватного життя

10.2 Конфіденційність та безпека

10.3 Карта світу: закони та правила, що стосуються шифрування даних

10.4 Непередбачені ризики для безпеки

10.5 Кіберзлочини, що порушують конфіденційність

10.6 Законодавство про захист даних

10.7 Право на забуття

10.8 Законодавство про повідомлення про пошкодження систем безпеки даних

10.9 Контроль за дотриманням законодавства про захист і конфіденційність даних даних

10.1 Недоторканість приватного життя

Недоторканність приватного життя – одне із основних прав людини. Право на недоторканність приватного життя є абсолютним імперативом для людини і закріплено в міжнародних договорах у галузі прав людини, наприклад, у статті 8 Європейської конвенції з прав людини 1950 року, статті 11 Американської конвенції з прав людини 1969 року, статті 12 Загальної декларації прав людини 1948 року та статті 17 про громадянські та політичні права 1966 року. Це право також визнається у статті 16 Конвенції про права дитини 1989 року, статті 14 Міжнародної конвенції та захисту прав усіх трудящих-мігрантів та членів їх сімей 1990 року, статті 7 Хартії основних прав Європейського союзу 2000 року та статті 22 Конвенції про права інвалідів. Існують різні концепції недоторканності приватного життя, які включають: право на свободу від спостереження; право бути залишеним на самоті; здатність зберігати в таємниці свої думки, переконання, особистість та поведінку; і право

вибирати і контролювати, коли, яка, чому, де, як і кому розкривається особиста інформація, і якою мірою вона розкривається. Остання з перерахованих концепцій недоторканності приватного життя (тобто право обирати та контролювати особисту інформацію) пов'язує конфіденційність із захистом інформації (або даних).

Право на недоторканність приватного життя забезпечує можливість здійснення інших прав людини і тісно пов'язане з цими правами. Недоторканність приватного життя є необхідною умовою для здійснення прав на свободу вираження думок, свободу думки, віросповідання, зборів та об'єднань. Право на недоторканність приватного життя також пов'язане із правом на самовизначення. Стаття 20(1) Африканської хартії правами людини 1981 року говорить: «Усі народи мають право існування. Їм належить безперечне і невід'ємне право самовизначення. Вони вільно визначають свій політичний статус і йдуть у своєму економічному та соціальному розвитку політиці, яку вони вільно обирають». Найважливішим аспектом права на самовизначення є здатність робити вибір і діяти на власний вибір без примусу (*особиста автономія*). Цей вибір поширюється не тільки на фізичні дії, але й на дії Інтернету. Невід'ємним аспектом приватного життя є особиста автономія і право самовизначення. Це право на самовизначення дозволяє людям вести самотнє життя, мати свободу вибору, а також обирати та контролювати, яку інформацію про себе зробити доступною для перегляду, розкриття та обміну.

Примітка

Згідно з Доповіддю Верховного комісара Організації Об'єднаних Націй з прав людини 2018 року, «надмірно широкі норми регулювання в галузі конфіденційності можуть являти собою невиправдані обмеження інших прав, зокрема права на свободу вираження поглядів, коли, наприклад, невідповідні обмеження заважають законній новині

журналістської діяльності, художнього самовираження або наукових досліджень».

Однією з невід'ємних аспектів приватного життя людини є *людська гідність*, спірна концепція, яка відноситься до «почуття власної гідності», яку людина зобов'язана розвивати і поважати в собі і зобов'язана захищати в інших». Людська гідність вважається основою прав людини та включена до преамбулів численних міжнародних договорів у галузі прав людини, включаючи: Загальну декларацію прав людини (ВДПЛ) 1948 року, Міжнародний пакт про громадянські та політичні права (МПГПП) 1966 року, Міжнародний пакт про економічні, соціальні та культурні права (МПЕСКП) 1966 року, Африканську хартію правами людини і народів 1981 року, Конвенцію ООН про права дитини (КООНПР) 1989 року, Декларацію ООН про ліквідацію всіх форм расової дискримінації 1963 року й Конвенцію ООН про ліквідацію всіх форм дискримінації щодо жінок. Хоча концепція людської гідності не знайшла прямого відображення у Європейській конвенції з прав людини 1950 року, у прецедентному праві вона описується як «істотна умова» міжнародних документів у галузі прав людини (*Pretty v. United Kingdom*, 2002). Повага людської гідності також розглядається як найважливіший принцип у конституціях багатьох країн по всьому світу (Shultziner and Carmi, 2014).

10.2 Конфіденційність та безпека

Контроль та вибір щодо розкриття інформації пов'язані з правом особи на свободу ідентифікації своєї особи та своїх дій на свій розсуд та вибір та за власним бажанням. Отже, декларація про недоторканність приватного життя пов'язані з правом не розкривати свою особистість. *Анонімність* дозволяє користувачам займатися діяльністю, не розкриваючи себе та/або своїх дій іншим особам. Завдяки анонімності в Інтернеті «в окремих користувачів та груп в онлайн-овому середовищі з'являється конфіденційний простір, в умовах якого вони можуть дотримуватися тих

чи інших думок та користуватися свободою їх вираження, не побоюючись довільного та незаконного втручання чи посягань». Таким чином, конфіденційність надає користувачам інформаційно-комунікаційних технологій простір, у якому вони можуть не побоюватися залякування, помсти та інших форм примусу чи санкцій за вираження думок, думок, поглядів та ідей без необхідності ідентифікувати свою особистість. Відповідно, «технічні засоби забезпечення безпеки та захисту конфіденційності електронних повідомлень, у тому числі заходи щодо забезпечення анонімності, можуть мати важливе значення для забезпечення здійснення прав людини, зокрема прав на недоторканність приватного життя, вільне вираження думок та свободу мирних зборів та асоціації». У цьому зв'язку «держави не мають перешкоджати використанню таких технічних рішень і мають забезпечувати, щоб будь-які обмеження щодо них відповідали зобов'язанням держав з міжнародного права в галузі прав людини».

Існує думка, що це право не розкривати свою особистість надає деяким людям сміливості адресувати іншим людям грубі, дискримінаційні, расистські, ненависницькі та/або образливі висловлювання, які вони б ніколи не дозволили собі, якби їхні особи були відомі. Хоча ця думка справедлива щодо деяких осіб, зустрічаються й інші люди, яким розкриття своєї особистості надає сміливості, коли вони розповсюджують такі висловлювання. Вони розкривають свою особистість для того, щоб бути впізнаними однодумцями та підштовхнути своїх прихильників до дій. Майло Яннопулос, бывший главный редактор ультраправого издания, специализирующегося на публикации сенсационных новостей (Breitbart), известен своими расистскими, женоненавистническими, антииммигрантскими и антимусульманскими речами, а также тем, что распространял другие ненавистнические высказывания, чтобы завоевать популярность среди членов альтернативных правых и ультраправых движений со сходными взглядами та/або прихильників цих рухів, і

підштовхував інших людей до подібних дій щодо осіб, які були об'єктом його ненависницьких висловлювань.

10.3 Карта світу: закони та правила, що стосуються шифрування даних

Компанія Global Partners Digital опублікувала в мережі інтерактивну глобальну карту законів і правил щодо шифрування даних.

Завдання встановлення особи та її місцезнаходження може виявитися важкоздійсненним через анонімність та використання технологій підвищення конфіденційності, таких як Tor. Ще одним прикладом *технології підвищення конфіденційності* є шифрування. *Шифрування* блокує доступ третіх осіб до інформації та повідомлень користувачів. Уряди багатьох країн світу висловлювалися про необхідність забезпечення доступу до зашифрованих повідомлень та інформації для боротьби з такими серйозними видами злочинності, як тероризм, організована злочинність та сексуальна експлуатація дітей.

Telegram , додаток для зашифрованих повідомлень, яким користуються понад 200 мільйонів осіб, було заблоковано в судовому порядку в деяких країнах, тому що компанія відмовилася надати урядам цих країн ключі дешифрування для відстеження повідомлень користувачів, що надсилаються через цю програму. У деяких країнах було встановлено обов'язкову вимогу про створення бекдорів та надання ключів для дешифрування, в той час як в інших країнах влада звернулася до компаній з проханнями про створення бекдорів та надання ключів для дешифрування для боротьби з серйозними злочинами, такими як тероризм (див., наприклад, спір Apple і ФБР щодо доступу до зашифрованих даних (Apple-FBI debate over encryption)). Однак створення таких бекдорів та надання ключів дешифрування можуть призвести до випадків зловживання доступом до даних (наприклад, дані можуть використовуватися урядами для непередбачених цілей, що виходять за рамки початкового дозволу у будь-якій справі), а також випадків використання цих бекдорів та ключів

злочинцями для отримання доступу до інформації з метою її перегляду, копіювання, видалення та/або зміни.

Чи знаєте ви?

Доступ до зашифрованих повідомлень та інформації можна отримати, якщо на цифрових пристроях увімкнено хмарне сховище. У США розслідування щодо Пола Манафорта, колишнього керівника виборчої кампанії Дональда Трампа, у зв'язку зі звинуваченнями в банківських махінаціях та відмиванні грошей, показало, що прокурори змогли отримати доступ до його зашифрованих повідомлень через Telegram і WhatsApp, які зберігалися в його обліковому записі у хмарному сховищі iCloud.

Навіть незважаючи на те, що шифрування ускладнює завдання притягнення кіберзлочинців до відповідальності і може використовуватися ними для вчинення кіберзлочинів, введення заборони та обмежень на шифрування є невиправданим та юридично необґрунтованим. Пряма заборона на використання технології шифрування невідповідно обмежує право людини на недоторканність приватного життя і, таким чином, суперечить міжнародному праву в галузі прав людини. Міжамериканський суд з прав людини охарактеризував право на недоторканність приватного життя як «свободу та захист від неправомірного та довільного вторгнення чи нападу з боку третіх осіб чи державних органів» і ухвалив, що держави «зобов'язані гарантувати право на недоторканність приватного життя за допомогою позитивних дій, які можуть передбачати, у деяких випадках, вжиття заходів, які забезпечують захист приватного життя від втручання з боку державних органів, а також окремих осіб або приватних установ, включаючи засоби масової інформації».

10.4 Непередбачені ризики для безпеки

Додаток Strava для відстеження фізичної активності дозволяє користувачам обмінюватися даними про маршрути своїх пробіжок з іншими користувачами цих пристроїв. У 2018 році Strava опублікувала на

своєму сайті теплову карту світу із зазначенням маршрутів пересування користувачів. Хоча викладена інформація не могла бути використана для простеження кожного окремого користувача, тепла карта розкрила їх пересування поблизу та навколо військових баз США у зарубіжних країнах. Таким чином, використання цієї програми та інших аналогічних програм на смартфонах, а також використання фітнес-пристроїв, що носяться до Інтернету речей, може бути особливо проблематичним для осіб, що працюють на військових базах і/або в місцях і районах, де їх відстеження може піддати цих осіб, їхню організацію та інших осіб небезпеки.

Заходи, які вживаються у відповідь на загрози безпеці та спричиняють серйозні несприятливі наслідки для здійснення прав людини, породжують почуття незахищеності. Важливо мати на увазі, що безпека та конфіденційність є взаємозалежними поняттями: безпека забезпечує людям свободу вести своє життя, зберігаючи гідність та особисту автономію, та приймати життєво важливі рішення без страху та примусу, а конфіденційність забезпечує людям можливість «для здійснення права на самовизначення та для розвитку своєї особистості без примусу». Таким чином, конфіденційність є засобом досягнення безпеки. Більше того, захист права на недоторканність приватного життя є невід'ємною складовою захисту даних та забезпечення безпеки систем, що містять ці дані, та мереж, через які ці дані переміщуються. Такі заходи захисту та гарантії зводять до мінімуму фактори вразливості до загроз безпеки та зменшують шкоду, заподіяну внаслідок несанкціонованого доступу, збору, видалення, зміни та розкриття даних.

10.5 Кіберзлочини, що порушують конфіденційність

Кіберзлочини порушують право на недоторканність приватного життя людей та безпеку їх персональних даних; до таких кіберзлочинів належать, зокрема, хакерські атаки, шкідливі програми, розкрадання персональних даних, фінансове шахрайство, медичне шахрайство та деякі

злочини щодо осіб, які пов'язані з розкриттям особистої інформації, повідомлень, зображень та відео- та аудіозаписів без згоди чи дозволу цих осіб.

Дані розглядаються як товар у мережі Інтернет та поза мережею - як законно діючими, так і незаконно діючими суб'єктами. Саме тому дані є основною метою кіберзлочинців. Дані також відіграють невід'ємну роль у скоєнні багатьох кіберзлочинів, насамперед тому, що вони не захищені належним чином і можуть бути доступними для незаконного отримання. Випадки витоку даних відбуваються внаслідок втрати або крадіжки зашифрованих флеш-накопичувачів та інших пристроїв зберігання даних (в основному ноутбуків та смартфонів), низького рівня безпеки систем і даних, несанкціонованого доступу до бази даних або перевищення санкціонованого доступу до бази даних, а також випадкового розкриття, розголошення чи публікації даних. Нижче наведено деякі відомі випадки витоку даних:

- Національна централізована база персональних даних уряду Індії (Aadhaar), в якій зберігаються біометричні дані (наприклад, відбитки пальців та фотознімки райдужної оболонки) та ідентифікаційні дані 1,2 мільярда громадян Індії, і яка використовується для перевірки особистості громадян при наданні фінансових, державних, комунальних та інших послуг, в 2018 році зіткнулася з проблемою витоку даних, в результаті якої були скомпрометовані особисті дані, такі як імена доступу, дванадцятизначний ідентифікаційний номер, номери телефонів, адреси електронної пошти та поштові індекси, але не біометричні дані.

- У 2017 році в мережу просочилися дані приблизно 30 мільйонів жителів Південної Африки, включаючи відомості про їх імена, статеву приналежність, дохід, історію працевлаштування, ідентифікаційні номери, номери телефонів і домашні адреси, в результаті витоку даних в одній з провідних ріелторських компаній країни J Holdings.

- У 2013 році були скомпрометовані персональні дані більше трьох мільярдів користувачів Yahoo, включаючи їхні імена, адреси електронної пошти, паролі (з шифруванням, яке можна було легко обійти) та дати народження.
- Deloitte, глобальна консалтингова фірма, зазнала атаки хакерів, які отримали доступ через незахищений обліковий запис до даних про імена користувачів і паролі близько 350 клієнтів.
- Персональні дані (тобто національний ідентифікатор, ім'я, стать, імена батьків, домашня адреса, дата народження та місто народження) понад 49 мільйонів громадян Туреччини у 2016 році були викладені в мережу та стали доступними через базу даних з можливістю пошуку.
- У 2016 році на Філіппінах було скомпрометовано персональні та біометричні дані понад 55 мільйонів виборців після того, як хакери в «чорному капелюсі» отримали несанкціонований доступ до веб-сайту виборчої комісії (COMELEC).

Чи знаєте ви?

Вкрадені паролі можуть завдати шкоди не тільки скомпрометованим обліковим записам, оскільки люди часто повторно використовують одні й ті самі паролі (або частини цих паролів; наприклад, певні номери) на кількох веб-сайтах, в облікових записах електронної пошти, додатках та/або онлайн-платформи.

Крім випадків витоку даних, є випадки, коли медичні, фінансові та інші персональні дані викладаються на спеціалізованих кардинг форумах в мережі (тобто на сайтах, що спеціалізуються на продажу даних дебетових і кредитних карт) і на сайтах в Даркнет .

Поряд із розкриттям таких даних з метою отримання фінансової вигоди, скомпрометовані дані можуть розголошуватися (і розголошуються) для осоромлення людей та викриття їх реальних чи передбачуваних аморальних дій та поведінки. Як приклад можна навести

випадок розміщення особистої інформації (наприклад, імен та адрес електронної пошти) приблизно 37 мільйонів користувачів веб-сайту Ashley Madison, що спеціалізувався на пошуку партнерів для позашлюбних зв'язків.

Тягар забезпечення безпеки даних часто лягає на осіб, дані яких викрадають. Ці люди інформуються про необхідність мінімізації своїх «цифрових слідів» шляхом оновлення налаштувань системи безпеки додатків, веб-сайтів, соціальних мереж та інших онлайн-платформ, а також видалення та/або зменшення обсягу особистих даних, якими вони діляться з іншими особами. Такий підхід, орієнтований на інтереси потерпілого, перекладає відповідальність за захист даних на жертв кіберзлочинів, а не на злочинців та компанії, системи безпеки яких були пошкоджені. Реальність така, що жертви не можуть захистити свої особисті дані, коли вони «зберігаються в базах даних третіх осіб і викрадають із цих баз даних, які знаходяться далеко за межами їх контролю». Крім того, сьогодні завдання мінімізації «цифрових слідів» стає дедалі складнішим. Практично не залишається жодних альтернативних варіантів для людей, які не бажають, щоб їхні дані збиралися, аналізувалися чи використовувалися. Наприклад, особа, яка користується соціальними мережами, вибирає один із двох можливих варіантів: або надати мінімальний обсяг необхідної особистої інформації для отримання права на користування платформою соціальних мереж (по суті, це «плата» за користування послугою), або відмовитися від надання такої інформації та не користуватись платформою. Жодних інших альтернативних варіантів не пропонується. Пристрої, що стосуються Інтернету речей, також вимагають надання особистої інформації, щоб отримати можливість користуватися ними. Все частіше можна спостерігати, що нові пристрої, що з'являються на ринку, - навіть ті, які ніколи раніше не підключалися до Інтернету, такі як побутова техніка, ювелірні вироби, одяг та іграшки, - тепер мають вихід в Інтернет, що залишає споживачам все менше варіантів, якщо вони роблять вибір на

користь придбання пристрою, який не має таких функціональних можливостей.

10.6 Законодавство про захист даних

Захист персональних даних здійснюється відповідно до права на недоторканність приватного життя, передбаченого у міжнародних договорах у галузі прав людини. Наприклад, Європейський суд з прав людини ухвалив, що дані, що стосуються використання телефону, електронної пошти та Інтернету, та дані, що зберігаються на комп'ютерних серверах, підпадають під сферу дії статті 8(1) Європейської конвенції з прав людини. Саме собою зберігання особистих даних може розглядатися як порушення права користувача недоторканність приватного життя. Факт наявності порушення залежить від контексту, в якому дані були отримані, методу їх збору, обробки та використання, а також результатів, які можуть бути при цьому отримані. Більше того, в справі *Tristan Donoso v. Panama and Escher et al. v. Brazil* (2009) Міжамериканський суд з прав людини ухвалив, що дані, зібрані та передані з використанням нових цифрових технологій та Інтернету, підпадають під дію статті 11 Американської конвенції з прав людини 1969 року. Крім того, стаття 8 Конвенції Африканського союзу про кібербезпеку та захист особистих даних 2014 року охоплює право на «захист персональних даних». Нарешті, стаття 8(1) Хартії основних прав Європейського Союзу 2000 року та стаття 16(1) Договору про функціонування Європейського Союзу 1957 року (також відомого як Римський договір) передбачають право на захист персональних даних як один із основних прав людини.

Захист даних поширюється на процеси створення, збирання, зберігання, аналізу, використання особистої інформації та обміну нею. Цей захист поширюється на створення та збирання персональних даних, тому що «право на недоторканність приватного життя зачіпається не тільки в ході аналізу або використання інформації про фізичну особу людиною або

алгоритмом, а й самим фактом підготовки та збору даних, що стосуються особистості, сім'ї та життя конкретної людини.

Бази даних, що містять персональні дані, доступні для запитів, пошуку, редагування, оновлення та перегляду місцевими та зарубіжними державними та приватними організаціями. Процедури управління збором, зберіганням, використанням інформації та обміном нею приватними та державними організаціями варіюють залежно від конкретної країни. Згідно з доповіддю Верховного комісара Організації Об'єднаних Націй з прав людини за 2018 рік, «зростаючий взаємозв'язок між обробкою громадських і особистих даних та накопичений досвід, що свідчить про масові та неодноразові зловживання особистими даними деякими компаніями, підтверджують приватного життя необхідні законодавчі заходи». Особисті дані можуть опрацьовуватися країнами із суворими законами про захист даних, країнами зі слабким законодавством про захист даних або країнами, де немає законів про захист даних. Наприклад, у Гані стаття 60 Закону про захист даних 2012 року дозволяє уряду отримувати доступ до персональних даних без ордеру чи іншого законного розпорядження (наприклад, судового наказу) на користь національної безпеки.

Практичні методи захисту даних також варіюють між різними державними та приватними організаціями. Наприклад, у Сполучених Штатах під дію регламенту підпадають лише деякі типи даних, які збираються, зберігаються, аналізуються та обмінюються приватними компаніями (наприклад, фінансові дані, дані про стан здоров'я, освіти та дані дітей). Крім того, в деяких країнах заходи захисту варіюють залежно від типу даних (наприклад, вмісту електронних повідомлень забезпечується більш високий ступінь захисту, ніж адреса електронної пошти відправника або одержувача). Закони про захист даних різняться з точки зору типів і джерел даних (наприклад, галузеві дані, дані в режимі онлайн, дані в режимі офлайн та конфіденційні дані) та суб'єктів персональних даних (наприклад, дорослі та діти). У Мексиці діють два

закони про захист даних, один з яких регулює приватний сектор - Федеральний закон про захист персональних даних, що знаходяться у розпорядженні приватних компаній 2010 року, - а інший регулює державний сектор - Загальний закон про захист персональних даних, що знаходяться в розпорядженні структур, що зобов'язалися 2017 року. У Мексиці також діють деякі положення у законодавстві, які регулюють приватні дані, пов'язані з хмарними сервісами, та регламентують доступ правоохоронних органів до даних, що зберігаються у хмарних сховищах, та поводження з даними після припинення дії хмарних послуг.

Транскордонний характер Інтернету вимагає ухвалення транснаціонального регламенту захисту даних, що виходить за рамки національних систем і законодавств. Прикладами можуть бути Конвенція Африканського союзу про кібербезпеку та захист особистих даних 2014 року та Додатковий закон A/SA.1/01/10 до закону про захист даних особистого характеру в рамках Економічного співтовариства західноафриканських держав (ЕКОВАС). Прийняття цих регіональних законів та рамкових документів було обумовлено прийняттям Директиви ЄС про захист даних (Директива 1995/46/ЄС). Директива 1995/46/ЄС була замінена Загальним регламентом ЄС із захисту даних (ЗРЗД) від 25 травня 2018 року. Цей єдиний закон про захист даних регламентує обробку, зберігання, використання даних та обмін даними в державах-членах ЄС та інших країнах, установах та приватних організаціях за межами ЄС, які надають товари та послуги ЄС та опрацьовують дані резидентів ЄС. Мета ЗРЗД полягає в уніфікації процесів безпечної обробки, зберігання, використання персональних даних та обміну ними. Цей регламент зводить до мінімуму обсяг цифрових слідів користувачів та способи, за допомогою яких додатки, технології, Інтернет-сервіси та платформи використовують ці сліди у своїх інтересах. ЗРЗД зміцнює права фізичних осіб на недоторканність приватного життя та сприяє вільному потоку персональних даних через кордони завдяки уніфікації практики захисту

даних. ЗРЗД вніс ясність щодо того, що являють собою персональні дані, встановив правила поводження з даними, чітко визначив ролі та обов'язки тих, хто контролює та обробляє персональні дані, встановив суворіші заходи покарання за недотримання вимог та ввів обов'язкову вимогу щодо повідомлення про витік персональних даних протягом 72 годин після інциденту.

Цей регламент встановлює нові зобов'язання для контролерів даних (тобто організацій, які визначають обґрунтування для обробки даних та методи, що використовуються для обробки даних), та для осіб, які обробляють дані (тобто організацій, які відповідають за обробку даних на основі методів, визначених контролером даних). ЗРЗД регулює доступ до даних, їх виправлення, видалення, прозорість контролерів даних та осіб, які обробляють дані; передбачає право на заперечення проти формування профілю; накладає зобов'язання щодо забезпечення безпеки даних на компанії, що обробляють дані; та надає розширені повноваження органам захисту даних та сприяє координації та співробітництву в галузі обробки та захисту даних. Цей регламент також передбачає великі штрафи та покарання за недотримання вимог.

Чи знаєте ви?

У справі *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González* (2014) Європейський Суд визначив операторів пошукових систем, таких як Google, як контролери даних, оскільки вони контролюють персональні дані, що знаходяться на веб-сайтах третіх сторін, роблячи ці веб-сайти доступними для інших осіб і приймаючи рішення про способи надання доступу до цих веб-сайтів.

Користувачі мають право на отримання інформації щодо обробки даних; право на доступ до оброблених даних; право на виправлення оброблених даних; право на видалення даних («право на забуття»; суб'єкт даних має право вимагати видалення своїх даних з журналів контролерів даних, а також не допускати подальшого використання та передачі

персональних даних суб'єкта даних третіми особами); право на заперечення проти обробки даних; декларація про обмеження обробки даних; право на переносимість даних (тобто суб'єкт даних має право отримати свої персональні дані, які він надав контролеру, та передати ці дані іншому контролеру); та право на заперечення проти автоматизованого процесу ухвалення рішення (наприклад, формування профілю).

10.7 Право на забуття

У справі *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González* (2014) Європейський суд витлумачив Директиву 1995/46/ЕС як таку, що дозволяє користувачам вимагати припинення індексації їх персональних даних у пошукових системах та браузерях. Зокрема, суд ухвалив, що фізичні особи мають право вимагати, щоб контролери даних (наприклад, оператори браузерів та пошукових систем, таких як Google) видалили посилання на сторонні веб-сайти, які містять невірні, неповні, неактуальні, застарілі або недійсні відомості про них. Наприклад, фізична особа може вимагати, щоб посилання, які з'являються в результаті пошуку імені користувача в цьому контенті, були видалені. Таке припинення індексації обмежується контентом, індексованим під ім'ям користувача. Припинення індексації не припиняє доступність цього контенту, індексованого під іншими пошуковими запитам, що базується на контенті, публікації або іншому джерелі або видавцеві або авторі контенту.

ОРЗД поширюється на установи ЄС, які ширше тлумачаться Європейським судом як організації, які обробляють дані в контексті своєї діяльності, навіть якщо така діяльність є мінімальною (*Weltimmo v. NAIH*, 2014). Якщо такий процес обробки даних здійснюється в контексті певної домовленості, яка діє в Європейському союзі, то він підпадає під дію ОРЗД. Організації, які мають свої контори в ЄС, а також організації, які просувають або продають маркетингові чи рекламні послуги, орієнтовані на резидентів ЄС, також підпадають під дію ГРЗД. Дія ОРЗД поширюється

навіть на організації, не засновані в ЄС, якщо вони обробляють персональні дані з метою пропозиції товарів та послуг резидентам ЄС та моніторингу поведінки споживачів до ЄС для складання профілю споживачів, визначення тенденцій та прогнозування особистих переваг споживачів.

ЗРЗД не поширюється на обробку персональних даних у рамках діяльності, пов'язаної з національною безпекою, а також діяльності, що стосується спільної зовнішньої та безпекової політики ЄС (тобто питань, пов'язаних з обороною та безпекою). ЗРЗД також не поширюється на дані, що опрацьовуються установами ЄС, які регулюються Регламентом (ЄС) №.45/2001 Європейського парламенту та Ради від 18 грудня 2000 року «Про захист фізичних осіб при обробці персональних даних, що здійснюється інститутами та органами Співтовариства, та про вільне зверненні таких даних». Крім того, ЗРЗД не поширюється на дані, що опрацьовуються державними органами з метою попередження, виявлення, розслідування злочинів та судового переслідування винних, які регулюються Директивою (ЄС) 2016/680 Європейського парламенту та Ради від 27 квітня 2016 року «Про захист фізичних осіб при обробці персональних даних компетентними органами з метою попередження, розслідування, виявлення кримінальних злочинів або притягнення до відповідальності, або виконання кримінальних покарань, та про вільний рух таких даних».

Конвенція Ради Європи про захист фізичних осіб при автоматизованій обробці персональних даних 1981 року (ETS №.108) є міжнародним договором про захист даних, що юридично зобов'язує. Додатковий факультативний протокол до цієї конвенції - Додатковий протокол до Конвенції про захист фізичних осіб при автоматизованій обробці персональних даних щодо наглядових органів та транскордонних потоків даних, 2001 року - містить заклик до створення наглядових органів для забезпечення захисту даних та недоторканності приватного життя під

час обміну даними. Ще один протокол (CETS No . 223) вніс зміни та доповнення до Конвенції 1981 р. (а саме Протокол про внесення змін до Конвенції Ради Європи щодо захисту фізичних осіб під час автоматизованої обробки даних 2018 року. Згідно з заявою Ради Європи (дата не вказана), модернізація конвенції «має дві основні цілі: вирішити проблеми, що породжуються використанням нових інформаційних та комунікаційних технологій, та посилити механізми конвенції для забезпечення її ефективного здійснення»

На додаток до національних, регіональних та міжнародних законів про захист даних існують керівні вказівки та принципи, які були розроблені країнами та міжурядовими організаціями та реалізовані установами державного та приватного секторів по всьому світу, такі як Посібник із захисту недоторканності приватного життя та транскордонної передачі персональних даних Організації економічного співробітництва та розвитку (ОЕСР) (1980; 2013).

У Посібнику з захисту недоторканності приватного життя та транскордонній передачі персональних даних 2013 року викладено такі принципи захисту даних та недоторканності приватного життя:

Принцип обмеження обсягу даних, що збираються

Обсяг персональних даних, що збираються, повинен мати певні межі; всі ці дані повинні бути отримані законним та чесним чином - якщо можливо, то за відома чи згоди суб'єкта даних.

Принцип якості даних

Персональні дані повинні відповідати цілям, у яких вони використовуватимуться; тією мірою, якою це необхідно відповідно до згаданих цілей, персональні дані мають бути точними, повними та регулярно оновлюваними.

Принцип конкретизації цілей

Цілі, в яких збираються персональні дані, повинні бути конкретизовані не пізніше моменту збору зазначених даних, а їхнє

подальше використання повинно обмежуватися досягненням згаданих або подібних (сумісних) цілей, які повинні вказуватися щоразу, коли ці цілі переглядаються.

Принцип обмеження використання даних

Персональні дані не повинні розголошуватися, надаватися в користування або іншим чином використовуватися з іншою метою, ніж ті, що перераховані в пункті 9, за винятком випадків, коли:

- а) суб'єкт даних дає свою згоду; або
- б) це дозволено законом.

Принцип обмеження використання даних

Персональні дані повинні бути забезпечені належними механізмами захисту від ризиків, пов'язаних із втратою, несанкціонованим доступом, знищенням, використанням, зміною або розголошенням даних.

Принцип відкритості

Повинна існувати загальна політика відкритості у сфері практики та політик щодо персональних даних. У постійній готовності повинні бути кошти для встановлення факту наявності та характеру персональних даних, основних цілей їх використання, а також особистості та звичайного місцезнаходження розпорядника даних.

Принцип персональної участі

Кожен суб'єкт даних (індивід) повинен мати такі права:

- одержувати від розпорядника даних, чи іншим чином, підтвердження того, чи є у цього розпорядника даних персональні дані, що належать до згаданого суб'єкта даних;
- одержувати персональні дані, що належать до нього/ній, у розумні терміни; у разі стягнення плати - за тарифом, який не є надмірним; в рамках розумної та необтяжливої процедури; та у зручній для розуміння формі;

- у разі відмови від задоволення заявки на надання інформації, поданої відповідно до пунктів (а) та (b), отримувати роз'яснення про мотиви відмови та опротестовувати таку відмову; а також
- опротестовувати дані, що відносяться до нього; у разі задоволення протесту вимагати, щоб такі дані були знищені, виправлені чи доповнені.

Принцип підзвітності

Розпорядник даних повинен нести відповідальність за вжиття заходів, що забезпечують дотримання перерахованих вище принципів.

Такі принципи було прийнято у національному законодавстві деяких країн. наприклад, *Закон Нової Зеландії про недоторканність приватного життя* 1993 року та *Закон Австралії Закон про недоторканність приватного життя* 1988 року.

10.8 Законодавство про повідомлення про пошкодження систем безпеки даних

Незважаючи на те, що в багатьох країнах діють закони, що вимагають надсилання повідомлень про витік даних (наприклад, Філіппіни: Закон про конфіденційність даних 2012 року; Катар: Закон №.(13) від 2016 року про захист особистих даних; та Індонезія: Положення № .82 від 2012 року «Про електронні системи та угоди» та постанову про реалізацію цього положення - Положення №.20 від 2016 року «Про захист персональних даних в електронній системі»), у більшості країн такі повідомлення є необов'язковими (наприклад, в Аргентині, Білорусі, Коста-Ріці, Єгипті, Японії, Макао, Малайзії, Мадагаскарі, Маврикії, Панамі, Росії та Саудівської Аравії) та/або є обов'язковими для приватного сектору, але не для державного сектору в інших країнах, або тільки для певних секторів суспільства (наприклад, в Анголі та Сербії). В Аргентині, хоча повідомлення про витік даних не є обов'язковим, установи зобов'язані

вести облік випадків витоку даних та подавати звіт на першу вимогу під час проведення розслідування або аудиторської перевірки.

Чи знаєте ви?

Компанія DLA Piper склала інтерактивну глобальну карту законів про захист даних, а також базу даних національних законів щодо захисту даних та повідомлень про пошкодження систем безпеки даних з можливістю пошуку: DLA Piper.

Закони про повідомлення про витік даних включають положення щодо застосування цих законів; наприклад, перераховуються особи, установи та/або органи, на яких поширюються ці закони, і що, згідно з цими законами, підпадає під визначення витоку даних. Відповідно до цих законів, організації, в яких стався витік даних (і які підпадають під дію закону), зобов'язані зв'язатися із суб'єктами цих даних та іншими відповідними сторонами та інформувати їх про інцидент.

У цих законах, зокрема, описуються способи надсилання повідомлення, термін повідомлення, а також особи, установи та/або органи, яких необхідно інформувати про витік даних. Наприклад, ЗРЗД передбачає зобов'язання про повідомлення у разі несанкціонованого доступу до систем та даних, використання та розповсюдження даних протягом 72 годин (стаття 33). Особи, які обробляють дані, зобов'язані повідомляти контролерів даних протягом 72 годин після витоку, а контролери даних протягом такого ж терміну зобов'язані повідомляти орган нагляду із захисту даних у відповідній державі-члені ЄС.

Закони про повідомлення про витік даних також передбачають винятки з вимоги про повідомлення. Наприклад, згідно з ЗРЗД повідомлення суб'єкта даних залежить від серйозності випадку витоку даних (стаття 34). Деякі закони про повідомлення про витік даних не вимагають повідомлення суб'єктів даних, якщо буде встановлено, що витік, найімовірніше, не завдасть їм шкоди. В інших законах повідомлення є обов'язковим, коли масштаб витоку даних досягає певного порога. У

Сполучених Штатах Америки Закон про спадковість страхування та звітності в галузі охорони здоров'я (HIPAA) вимагає сповіщення порушених сторін протягом 60 днів з моменту витоку. Однак у випадках, коли витік даних про здоров'я торкається понад 500 осіб, необхідно повідомляти Управління з цивільних прав Міністерства охорони здоров'я та соціальних служб та засоби масової інформації протягом 60 днів з моменту витоку, у той час як у випадках, коли витік особистих даних про здоров'я торкається менше 500 осіб, немає необхідності повідомляти про це засоби масової інформації, а Управління з цивільних прав Міністерства охорони здоров'я та соціальних служб має бути повідомлено про це не пізніше ніж через 60 днів після початку наступного календарного року (HIPRA Journal , 2015).

В інших країнах законодавство про повідомлення про витік даних також вимагає від організацій, які обробляють персональні дані, вживати заходів безпеки для захисту даних та/або здійснювати дії від імені особи, порушеної витоком даних, для виправлення ситуації та/або усунення збитків (наприклад, Канада , Індонезія та Сполучені Штати).

10.9 Контроль за дотриманням законодавства про конфіденційність та захист даних

Як правило, проблеми, з якими стикаються країни при застосуванні заходів щодо забезпечення належного дотримання законів про захист даних, включають проблеми фінансування, нездатність належним чином забезпечити виконання цих законів (наприклад, через обмежені людські та технічні ресурси), неадекватну інфраструктуру ІКТ , а також нездатність або небажання виконувати обробку транскордонних запитів на передачу даних.

Заходи щодо забезпечення дотримання принципів та законів, що стосуються конфіденційності та захисту даних, різняться між державним та приватним секторами, між окремими країнами та всередині країн. Наприклад, ЗРЗД було прийнято з метою гармонізації та зміцнення

повноважень органів захисту даних для забезпечення ефективної реалізації законодавства. На додаток до законів про захист даних, з метою сприяння зусиллям захисту даних міжнародні та регіональні організації розробили та ухвалили регламенти захисту даних. Наприклад, Азіатсько-Тихоокеанське економічне співробітництво (АТЕС) розробило Рамкову угоду щодо захисту персональних даних, яка включає в себе принципи та керівні вказівки для захисту даних таким чином, щоб уникнути перешкод, що ускладнюють потоки інформації між країнами-учасницями, а також Правила транскордонної передачі персональних даних – добровільний механізм саморегулювання, який встановлює стандарти захисту даних для транскордонного обміну даними між країнами-учасницями. Важливо відзначити, що національне законодавство про конфіденційність та захист даних має переважну силу порівняно з цими правилами.

Чи знаєте ви?

Таблиця з описом подібностей та відмінностей між Рамковою угодою АТЕС щодо захисту персональних даних та ЗРЗД з точки зору таких аспектів, як мета, матеріальна сфера дії, територіальна сфера дії, особиста інформація, контролер даних, особи, що обробляють дані, загальнодоступна інформація, допустимі відхилення для країн-учасниць (дерогація), принцип попередження шкоди, повідомлення, обмеження на збір, обмеження на використання, вибір та згода, цілісність даних, гарантії безпеки, доступ та виправлення, підзвітність, передача персональних даних іншій особі чи країні, визначення витоку даних, повідомлення про витік даних та пом'якшення наслідків витоку даних, була опублікована Міжнародною асоціацією фахівців у галузі захисту недоторканності приватного життя (IAPP).

На додаток до заходів щодо забезпечення дотримання цих правил, які вживаються органами влади, захист даних також можуть забезпечувати технології. Як приклад можна навести технологію підвищення

конфіденційності. Мета таких технологій полягає у захисті та збереженні недоторканності приватного життя окремих осіб. Тому технології підвищення конфіденційності можуть використовуватися для реалізації та дотримання законів про захист даних. Ці технології в першу чергу використовуються для захисту конфіденційності (тобто дані захищені, і тільки авторизовані користувачі можуть отримати до них доступ) та цілісності даних (тобто дані не змінені і є тим, як вони заявлені). Одним із прикладів технології підвищення конфіденційності є шифрування. Іншим прикладом є *управління обліковими даними*, яке відноситься до процесу автентифікації ідентифікаційних даних користувачів, ідентифікації відповідних привілеїв та надання доступу користувачам на основі цих привілеїв. Керування обліковими даними підтримує принципи безпеки та пропорційності захисту даних шляхом введення обмеження на доступ та використання даних.

Виконання законів про захист даних також може забезпечуватись шляхом застосування принципу *захисту даних на основі продуманих дій*. Стаття 25 ЗРЗД встановлює вимогу про «захист даних на основі продуманих дій», відповідно до якої контролери даних та особи, що обробляють дані, повинні впроваджувати технології підвищення конфіденційності та передбачати інші заходи щодо забезпечення конфіденційності персональних даних при розробці систем та технологій. Ці конструктивні особливості вимагають вжиття технічних та організаційних заходів контролю та політики для захисту персональних даних, а також заходів безпеки, спрямованих на забезпечення конфіденційності, цілісності та доступності (тобто доступності на вимогу) систем, мереж, сервісів та даних (наприклад, управління доступом, шифрування, брандмауери, моніторинг використання комп'ютерів та принципи інформаційної безпеки).

Ще один захід захисту даних на основі продуманих дій (або *конфіденційності на основі продуманих дій*) передбачає приховування інформації, що ідентифікує, шляхом *анонімізації* або *псевдонімізації*.

Відповідно до статті 4(5) ЗРЗД, під терміном «псевдонімізація» розуміється «обробка персональних даних таким чином, що персональні дані не можуть бути більше віднесені до певного суб'єкта даних без використання додаткової інформації, за умови, що додаткова інформація зберігається окремо та підлягає застосуванню технічних та організаційних заходів, які гарантують, що персональні дані не віднесені до ідентифікованої або ідентифікованої фізичної особи». Псевдонімізація відбувається, коли ідентифікуючі дані запису замінюються штучними ідентифікаторами. Вона є однією з форм *маскування даних*, оскільки захищає конфіденційність даних для запобігання ідентифікації суб'єкта даних. На додаток до заходів захисту даних на основі продуманих дій можуть застосовуватися заходи захисту *даних за умовчанням*. Прикладом такого заходу є практика обробки лише тих персональних даних, які необхідні досягнення конкретної заявленої мети обробки (з дотриманням принципу *мінімізації даних* і цільового обмеження).

Питання для самоперевірки

Чому конфіденційність важлива? Як би ви описали зв'язок між конфіденційністю та безпекою? Яким чином кіберзлочинність впливає на конфіденційність?

Як би ви описали правове середовище захисту даних? Чи належним чином захищені дані в межах країни та/або коли вони передаються за кордон? Будь ласка, обґрунтуйте свою відповідь.

Чи сповіщення про порушення даних є обов'язковими в більшості країн? Якщо ні, то повинні бути? Чому ти так думаєш?

Якими способами можна забезпечити захист даних? Не забудьте включити у відповідь як юридичні, так і технічні заходи.

ЛЕКЦІЯ 11. ЗЛОЧИНИ У СФЕРІ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ, ЗДІЙСНЮВАНІ ЗА ДОПОМОГОЮ КІБЕРТЕХНОЛОГІЙ

11.1 Види інтелектуальної власності

11.2 Причини, підстави та передбачувані мотиви правопорушень, що стосуються авторських прав та товарних знаків, що скоюються за допомогою кібертехнологій

11.3 Зусилля із захисту та профілактики

Всесвітня організація інтелектуальної власності (ВОІВ) дає таке визначення *інтелектуальної власності*: «результат творення людського розуму. До об'єктів ІВ відносяться винаходи, літературні та художні твори, символіка, назви та зображення, які використовуються в комерційних цілях». Права на інновації, твори, оригінальне вираження ідей та секретні методи та процеси ведення бізнесу охороняються національним та міжнародним законодавством про інтелектуальну власність. Відповідно до статті 2 Конвенції, яка започатковує Всесвітню організацію інтелектуальної власності 1967 року (змінена у 1979 році), ці права належать до: ... літературних, художніх та наукових творів, ... виконавчої діяльності артистів, звукозапису, радіо та телевізійних передач, ... винаходів у всіх галузях людської діяльності; ... наукових відкриттів; ...промислових зразків; ... товарних знаків, знаків обслуговування, фірмових найменувань та комерційних позначень; ... захисту проти недобросовісної конкуренції, а також усіх інших прав, що стосуються інтелектуальної діяльності у виробничій, науковій, літературній та художній галузях.

Доступ до інтелектуальної власності, її розповсюдження та/або використання без попереднього дозволу та/або після закінчення строку дії такого дозволу та порушення прав власника або власників інтелектуальної власності вважається злочином у сфері інтелектуальної власності (також називається *крадіжкою інтелектуальної власності*). Оскільки права

інтелектуальної власності визнаються як особисті майнові права (Guan, 2014), злочини у сфері інтелектуальної власності розглядається як форма крадіжки особистого майна, навіть якщо вона не відповідає загальноприйнятому уявленню про крадіжку (тобто позбавлення володіння). Наприклад, якщо в людини викрадено ювелірні вироби, вона позбавляється свого (матеріального) майна, оскільки вона більше не має доступу до цих ювелірних виробів. Однак у разі інтелектуальної власності, навіть якщо майно «викрадено» (тобто використовується та споживається без дозволу), власника інтелектуальної власності *не* позбавляють його власності, оскільки вона все ще перебуває у його володінні. Все, що він втрачає, – це контроль, управління та економічна вигода, яка могла бути отримана від подальшого використання його інтелектуальної власності. Позбавлення винагороди за працю (тобто за створення інтелектуальної власності) є негативним стимулом для створення об'єктів інтелектуальної власності, які мають найважливіше значення для зростання національної економіки. У цьому зв'язку ВОІВ «за допомогою збалансованої та ефективної системи інтелектуальної власності сприяє інноваційній та творчій діяльності на користь соціально-економічного та культурного розвитку всіх країн».

З метою захисту прав інтелектуальної власності було введено в дію кілька міжнародних конвенцій, угод та договорів (далі – договори). Прикладом може бути Бернська конвенція з охорони літературних і мистецьких творів 1886 року (з поправками, внесеними 1979 року), у якій встановлюється зобов'язання держав захисту інтелектуальної власності і визначаються мінімальні стандарти захисту інтелектуальної власності. У зв'язку із занепокоєнням щодо забезпечення дотримання Бернської конвенції, Світова організація торгівлі (СОТ) прийняла Угоду з торгових аспектів прав інтелектуальної власності (ТАПІВ) 1994 року (яка набула чинності у 1995 році). Угода ТАПІВ вимагає, щоб країни-члени СОТ виконували свої зобов'язання, ухвалені в рамках Бернської конвенції та

інших договорів. Світова організація торгівлі здійснює нагляд за виконанням Угоди ТАПВ і, серед іншого, встановлює стандарти для політики, законів, положень, що стосуються інтелектуальної власності, а також механізмів контролю за виконанням зобов'язань щодо захисту прав інтелектуальної власності.

Чи знаєте ви?

Міжнародні конвенції щодо захисту авторських прав можуть вплинути на національні закони у сфері регулювання Інтернет-середовища. Наприклад, «виключне право дозволяти будь-яке повідомлення своїх творів для загального відомості про проводи або засоби бездротового зв'язку» відноситься до «Права на повідомлення для загального відомості», яке охороняється статтею 8 Договору ВОІВ з авторського права. Виходячи з цього, право на доведення творів до загальної інформації за допомогою інформаційних мереж було включено до статті 10(12) Закону Китайської Народної Республіки «Про авторське право» (зі змінами, внесеними у 2010 році) та Положення про захист права на доведення творів до загального відомості за допомогою інформаційних мереж (переглянуто у 2013 році).

На додаток до міжнародних договорів, національні закони (наприклад, В'єтнам: Закон №.36/2009/QН12 від 19 червня 2009 року, що вносить зміни до Закону про інтелектуальну власність; Азербайджан: *Закон Азербайджанської Республіки «Про забезпечення прав інтелектуальної власності та боротьбу з піратством»*) 2012 року, Коста-Ріка: Закон № 8686 від 21 листопада 2008 року про зміни, доповнення та анулювання різних правил, що регулюють питання права інтелектуальної власності, Екваторіальна Гвінея: Закон від 10 січня 1879 року «Про інтелектуальну власність», та Сальвадор: указ №.611 від 15 лютого 2017 року про внесення поправок до Закону про інтелектуальну власність тощо) та регіональні договори (наприклад, Асоціація держав Південно-Східної Азії (АСЕАН): Рамкова угода про співробітництво у сфері інтелектуальної власності 1995 року); та Співдружність Незалежних Держав (СНД): Угода

про співпрацю в галузі правової охорони та захисту інтелектуальної власності та створення Міждержавної ради з питань правової охорони та захисту інтелектуальної власності 2011 року) вводяться в дію з метою уніфікації політики, законів та практики в галузі інтелектуальної власності у державах-учасниках цих договорів.

Чи знаєте ви?

BOIV підтримує онлайн базу даних з можливістю пошуку, що включає національні та регіональні закони та міжнародні договори у сфері інтелектуальної власності (Відвідайте базу даних [WIPO Lex](#)).

11.1 Види інтелектуальної власності

Інтелектуальна власність включає авторські права, товарні знаки, патенти і промислові секрети. Кожен із цих видів інтелектуальної власності докладніше розглядається нижче.

Авторські права

Авторські права містять у собі права на «літературні та художні твори», які визначаються у статті 2(1) *Бернської конвенції* з охорони літературних та художніх творів 1886 наступним чином:

Термін «літературні та художні твори» охоплює всі твори в галузі літератури, науки і мистецтва, хоч би яким чином і в якій формі вони не були виражені, як-то: книги, брошури та інші письмові твори; лекції, звернення, проповіді та інші подібні твори; драматичні та музично-драматичні твори; хореографічні твори та пантоміми; музичні твори з або без тексту; кінематографічні твори, до яких прирівнюються твори, виражені способом, аналогічним кінематографії; малюнки, твори живопису, архітектури, скульптури, графіки та літографії; фотографічні твори, до яких прирівнюються твори, виражені способом, аналогічним фотографії; твори прикладного мистецтва; ілюстрації, географічні карти, плани, ескізи та пластичні твори, що стосуються географії, топографії, архітектури або наук

Крім Бернської конвенції, Міжнародна конвенція про охорону прав виконавців, виробників фонограм та мовних організацій 1961 року (Римська конвенція про охорону суміжних прав) також захищає авторські права та визначає права власників авторських прав. Всесвітня організація інтелектуальної власності (ВОІВ), Міжнародна організація праці (МОП) та Організація Об'єднаних Націй з питань освіти, науки та культури (ЮНЕСКО) спільно здійснюють контроль за виконанням цієї конвенції. ВОІВ, МОП та ЮНЕСКО також спільно контролюють виконання Конвенції про охорону інтересів виробників фонограм від незаконного відтворення їх фонограм 1971 року (Женевська конвенція з фонограм). «Визнаючи глибокий вплив розвитку та зближення інформаційних та комунікаційних технологій на виробництво та використання виконавств та фонограм», Договір ВОІВ з виконавств та фонограм 1996 року регулює права «виконавців (акторів, співаків, музикантів тощо); та ...виробників фонограм (фізичних чи юридичних осіб, які беруть на себе ініціативу та несуть відповідальність за запис звуків)» «у цифровому середовищі». Крім того, Договір ВОІВ з авторського права 1996 року, «спеціальна угода, укладена в рамках Бернської конвенції, стосується охорони творів і прав їх авторів у цифровому середовищі, включно з комп'ютерними програмами, незалежно від способу або форми їх вираження; ... та ... компіляції даних або іншої інформації («бази даних»)) (ВОІВ, *«Договір ВОІВ з авторського права»*). Також існують національні закони (наприклад, Бурунді: Закон № 1/021 від 30 грудня 2005 року «Про охорону авторського права та суміжних прав Бурунді») та регіональні договори, що забезпечують охорону авторських прав (наприклад, Міжамериканська конвенція про авторське право на літературні, наукові та художні твори 1947 року Організації американських держав (ОАД).

Порушення авторських прав в Інтернеті називається *цифровим піратством*, яке передбачає викладання, передачу, завантаження творів, що охороняються авторським правом, та обмін ними (наприклад, книг,

музики та фільмів) без отримання передбаченого законом дозволу на доступ, використання та розповсюдження. Як приклад можна навести Napster, онлайн-платформу, яка забезпечила можливість для незаконного розповсюдження музики через систему обміну файлами однорангових мереж (*A&M Records, Inc. v. Napster, Inc.*, 2001). Порухення авторських прав також має місце на інших однорангових файлообмінниках та торрент-сайтах (таких як Kazaa, Limewire та PirateBay) та криптолокерах (тобто сайтах, які надають послуги хмарного зберігання та обміну файлами для клієнтів; наприклад, Megaupload) (Drath, 2012). Як і інші види злочинів у сфері інтелектуальної власності, скоєних за допомогою кібертехнологій, цифрове піратство позбавляє авторів і видавців творів прибутку, які вони могли б отримати від своїх творів, власності та праці. Наприклад, НВО (американський кабельний канал, який стягує з глядачів плату за перегляд контенту) втратив мільйони доларів у вигляді неотриманого виторгу, коли епізоди одного з його серіалів, *«Гри престолів»*, просочилися в Інтернет і стали доступними для безкоштовного перегляду (Denham, 2015). Сценарії епізодів *«Гри престолів»* і епізоди телевізійних шоу НВО, що ще не вийшли в ефір, також були викладені в Інтернет після витоку даних, що стався в НВО в 2017 році (Gibbs, 2017).

Цифрове піратство: гендерний кіберзлочин?

Результати емпіричних досліджень зв'язків між цифровим піратством та гендерною приналежністю є неоднозначними. Деякі дослідження показали, що чоловіки здійснюють дії, що стосуються цифрового піратства, та/або повідомляють про випадки цифрового піратства частіше, ніж жінки (Hinduja, 2001; Ingram and Hinduja, 2008; Skinner and Fream, 1997). У той час як в одних дослідженнях гендерна приналежність була визнана статистично значущим прогностичним фактором цифрового піратства (Gopal et al., 2004; Hinduja, 2007; Ingram and Hinduja, 2008), в інших дослідженнях статистично значимих гендерних відмінностей цього

виду Cheung, 2013; Higgins, 2005; Higgins and Makin, 2004; Morris and Higgins, 2009).

Товарні знаки

Товарні знаки – це ідентифікатори, які дозволяють відрізнити товари чи послуги одних джерел від інших. Таким джерелом може бути підприємство, фізична особа або географічне розташування. Товарні знаки можуть включати, зокрема, логотипи, символи, малюнки, назви та слогани, які є складовою частиною товарів, послуг і брендів і дають можливість відрізнити їх між собою. Ідентифікатори, з яких складаються товарні знаки, набувають цінності завдяки праці, грошам, знанням та навичкам власників товарних знаків. Така набута цінність ґрунтується на характеристиках, якості та/або надійності товару чи послуги. Товарні знаки захищають їх власників від практики недобросовісної конкуренції, мета якої полягає у спробі отримати вигоду від інвестицій власника товарного знака у розробку та/або розповсюдження товару чи послуги (WIPO, 1993). Товарні знаки також захищають споживачів, допомагаючи їм розпізнавати джерело товару чи послуги.

Чи знаєте ви?

В окремих країнах, таких як Сполучені Штати Америки, деякі знаменитості мають можливість офіційно зареєструвати своє ім'я як товарний знак.

Географічні вказівки (або найменування місць походження) також є формою інтелектуальної власності, що охороняється. Географічні вказівки, які «зазвичай використовуються щодо сільськогосподарської продукції, продуктів харчування, вин та міцних спиртних напоїв, ремісничих та промислових виробів» (ВОІВ, без дати), не можна використовувати, крім випадків, коли продукт був розроблений у цьому регіоні відповідно до загальноприйнятої стандартною практикою. У статті 2(1) Лісабонської угоди про охорону найменувань місць походження та їх міжнародної

реєстрації 1958 року «вказівка місця походження» визначається як «географічна назва країни, району або місцевості, що використовується для позначення виробу, що відбувається звідти, якість і властивості якого визначаються виключно або в значною мірою географічним середовищем, включаючи природні та етнографічні фактори». Вказівка географічного місця походження виробу є символом його якості та репутацією місця його створення (стаття 2(2) *Лісабонської угоди про охорону найменувань місць походження та їх міжнародну реєстрацію* 1958 року). Тому географічна вказівка розглядається як одна з форм інтелектуальної власності.

Для товарних знаків розробляються міжнародні системи класифікації. Зокрема, міжнародна система класифікації (Ніццька класифікація) була розроблена для товарних знаків відповідно до Ніццької угоди про Міжнародну класифікацію товарів та послуг для реєстрації знаків 1957 року. Міжнародна система товарних знаків (також відома як Мадридська система) була створена як централізована система реєстрації товарних знаків та управління ними, щоб забезпечити можливість фізичним особам подавати одну заявку на реєстрацію товарних знаків та оплачувати один набір мит, що дозволить їм питати охорону їхніх товарних знаків у Мадридському союзі. За даними ВОІВ, Мадридський союз складається зі 117 договірних сторін Мадридської угоди про міжнародну реєстрацію знаків 1891 року (з наступними змінами та поправками) та Мадридського протоколу до Мадридської угоди про міжнародну реєстрацію знаків 1989 року (з наступними поправками). Більш того, Міжнародна система найменувань місць походження, централізована система, що забезпечує можливість оформлення однієї реєстрації та сплати одного набору мит, була створена з метою охорони найменувань місць походження у 28 сторонах Лісабонської угоди про охорону найменувань місць походження та їх міжнародної *реєстрації* 1958 року .

Міжнародні договори, такі як Договір про закони щодо товарних знаків 1994 року, забезпечили гармонізацію процедур подання заявок на реєстрацію товарних знаків та їх реєстрацію в країнах-учасниках договорів. Відповідно до Сінгапурського договору про закони щодо товарних знаків 2006 року було внесено поправки та зміни до Договору про закони щодо товарних знаків 1994 року, які, зокрема, дозволили подавати заявки на реєстрацію товарних знаків в електронному вигляді (Maras, 2016). Так само, як і у випадку з авторськими правами, охорону товарних знаків забезпечують національні закони (наприклад, Афганістан: Закон про реєстрацію товарних знаків 2009 року; Андорра: Закон про торгові знаки 1995 року; Куба: Декрет-закон №.228 «Про географічні вказівки» 2002 року та Куба: Декрет-закон №.203 «Про торгові марки та інші відмітні знаки» 1999 року) та регіональні договори (наприклад, Співдружність Незалежних Держав: Угода про заходи щодо запобігання та припинення використання неправдивих товарних знаків та географічних вказівок) 1999 року та Організація американських держав: Загальна міжамериканська конвенція про охорону товарних знаків та торгівлі 1930 року).

Підrobка товарних знаків (коли товар або послуга маркований товарним знаком його законного власника, але не є справжнім товаром або послугою законного власника товарного знака) є загальносвітовою глобальною проблемою, і висловлюються побоювання з приводу того, що така форма контрафакції фінансує організовану злочинність, тероризм та інші серйозні злочини. Товари з підробленими товарними знаками включають ювелірні вироби, аксесуари, одяг, взуття, електроніку, іграшки, побутову техніку, виробничі деталі, продукти харчування та (алкогольні та безалкогольні) напої, косметику та засоби особистої гігієни, лікарські препарати і т.д. Ці контрафактні товари викликають серйозні проблеми для здоров'я, безпеки, охорони праці та довкілля (UNODC, 2014). Продукція з підробленими товарними знаками купується та продається в особистому порядку та через Інтернет. Навіть логотипи, упаковку та інші

ідентифікуючі промислові зразки контрафактних товарів можна придбати в Інтернеті та за межами мережі (Albanese, 2018).

Патенти

Патент – це право на нові та унікальні витвори, новаторські розробки та винаходи, зареєстровані в органі виконавчої влади, яке може забезпечити їхню охорону на національному та/або міжнародному рівні. Патенти дозволяють забороняти використання та експлуатацію нововведень без дозволу (тобто явно вираженої згоди або схвалення) власника патенту. Патенти на зразки (або *промислові зразки*) також є формою інтелектуальної власності, що охороняється. Промислові зразки вважаються однією з форм інтелектуальної власності, оскільки ці зразки створюються з метою бути естетично привабливими для споживачів і впливають на вибір споживачів між товарами. Отже, промислові зразки впливають на конкурентоспроможність та комерційну цінність товару (WIPO, 2006).

Чи знаєте ви?

Існують *патентні тролі*, які нічого не створюють і не винаходять. Тролі такого типу просто купують патенти, видають ліцензії іншим особам, а потім судяться з будь-якою особою, групою чи організацією, які порушують їхні набуті патентні права.

Так само, як у товарних знаків, міжнародні системи класифікації розробляються й у патентів. Зокрема, міжнародна система класифікації (Локарнська класифікація) для реєстрації промислових зразків була введена в дію відповідно до Локарнської угоди про заснування Міжнародної класифікації промислових зразків 1968 року. Також була розроблена міжнародна система класифікації (Міжнародна патентна класифікація) для патентів відповідно до Страсбурзької угоди про Міжнародну патентну класифікацію 1971 року. Міжнародна система зразків (тобто. Гаазька система міжнародної реєстрації промислових зразків), централізована система реєстрації, розроблена відповідно до

Гаазької угоди про міжнародну реєстрацію промислових зразків 1925 року та її актами (Гаазький акт 1960 року та Женевський акт 1999 року), дозволяє компаніям реєструвати до 100 зразків та запитувати їхню охорону на території 68 країн-учасниць угоди.

Міжнародні договори, такі як Паризька конвенція з охорони промислової власності 1883 року (у редакції 1979 року) та подальші поправки до неї, основними цілями яких є «охорона промислової власності, об'єктами якої є патенти на винаходи, корисні моделі, промислові зразки, товарні знаки, знаки обслуговування, фірмові найменування та вказівки походження чи найменування місця походження, а також припинення недобросовісної конкуренції», поширюються «на всі продукти промислового чи природного походження, як, наприклад: вино, зерно, тютюновий лист, фрукти, худобу, копалини, мінеральні води, пиво, квіти, мука» (стаття 1). Крім того, Договір про патентну кооперацію 1970 року та Договір про патентне право 2000 року були введені в дію з метою уніфікації процедур подачі патентних заявок та реєстрації на територіях Договірних Держав, щоб дозволити особам подавати одну патентну заявку та вимагати патентну охорону винаходу на території 15 держав. Крім того, охорона патентів також забезпечується регіональними договорами, такими як Європейська конвенція щодо формальностей, необхідних для оформлення заявок на патенти 1955 року, Конвенція про видачу європейських патентів (Європейська патентна конвенція) 1973 року, Європейська патентна конвенція 1994 року, які прийняті Радою Європи з метою зміцнення співробітництва в галузі патентної охорони та у договірних державах, а також національними законами (наприклад, Кіпр: Закон «Про патенти» 1998 року; Непал: Закон №.2022 «Про патенти, промислові зразки та торговельні знаки» 1965 року; Киргизстан: Закон Киргизької Республіки №.8 від 14 січня 1998 року «Патентний закон» (у редакції Закону №76 від 10 квітня 2015 року).

Патенти та громадська охорона здоров'я

Існують протиріччя між інтелектуальною власністю, інноваціями та громадською охороною здоров'я, особливо у частині, що стосується інновацій у фармацевтичній галузі (наприклад, антиретровірусні препарати для лікування ВІЛ/СНІДу) та права на отримання недорогої та доступної медичної допомоги (див., наприклад, Fisher and Ri 2005 для отримання інформації про патентні бар'єри при отриманні антиретровірусних препаратів проти ВІЛ/СНІДу в Південній Африці). У Дохінській декларації «Угода щодо ТРІПС та громадська охорона здоров'я» 2001 року ці протиріччя були усунуті шляхом застосування гнучких положень Угоди ТРІПС для вирішення проблем у галузі охорони здоров'я в країнах, що розвиваються і найменш розвинених, та підтвердження того, що Угода ТРІПС не заважає і не заважає, спрямовані на охорону здоров'я населення (WHO, WIPO та WTO, 2015).

Промислові секрети

Промислові секрети є цінною інформацією про бізнес-процеси та ділову практику, які є секретними і захищають конкурентні переваги компанії. Промислові секрети можуть включати в себе секретні стратегії, методи, процеси і формули, які дозволяють підприємствам зберігати конкурентну перевагу, такі як будь-які типи фінансової, ділової, наукової, технічної, економічної та інженерної інформації, включаючи інформацію про пристрій, плани, набір даних, програмних пристроях, формулах, дизайнах, прототипах, методах, технологіях, процесах, процедурах, програмах або кодах як відчутну, так і невлловиму незалежно від того, як вони зберігаються, чи істематизовані вони, чи збережені вони фізично, в електронному вигляді, графічно, на фотографії чи письмово.

На відміну від інших форм інтелектуальної власності, «промислові секрети охороняються без реєстрації» (тобто «без будь-якої формальної процедури») і таким чином можуть «охоронятися необмежений період часу» (ВОІВ, «Як охороняються промислові секрети? »). Критерії та стандарти охорони промислових секретів (або захисту закритої інформації)

наведено у статті 39 Угоди ТРІПС. Зокрема, відповідно до статті 39(2), Фізичним та юридичним особам надається можливість перешкоджати тому, щоб інформація, що правомірно перебуває під їх контролем, без їх згоди була розкрита, отримана або використана іншими особами у спосіб, що суперечить чесній комерційній практиці, за умови , що така інформація:

(а) є секретною в тому сенсі, що вона в цілому або в певній конфігурації та доборі її компонентів не є загальновідомою та легко доступною особам у тих колах, які зазвичай мають справу з такою інформацією;

(b) через свою таємність має комерційну цінність; і

(с) є предметом належних у цих обставин заходів, спрямованих на збереження її таємності, з боку особи, яка правомірно контролює цю інформацію.

Крім того, захист промислових секретів забезпечують деякі регіональні договори (наприклад, Директива Європейського союзу щодо захисту комерційної таємниці 2016 року) та національні закони (наприклад, Сполучені Штати Америки, Закон про захист комерційної таємниці 2016 року). Промислові секрети охороняються на національному, регіональному та міжнародному рівнях, оскільки вони мають життєво важливе значення для економічної та національної безпеки країни. Суб'єкти підприємницької діяльності також захищають свої промислові секрети, оскільки розкриття цієї інформації третій стороні (наприклад, приватній особі, групі, компанії або іноземному уряду) без дозволу може завдати їм економічної шкоди. Крадіжка комерційної таємниці може відбуватися поза мережею Інтернет (*економічний шпигунство*) або з використанням Інтернету та Інтернет-технологій (різновид економічно мотивованого *кібершпигунства*). У 2018 році колишнім співробітникам компанії Jawbone, яка нині припинила своє існування, займалася продажем фітнес-браслетів, було пред'явлено звинувачення у володінні

комерційними секретами Jawbone (які містилися в «захищених внутрішніх комп'ютерних системах Jawbone і хмарному сховищі ») після того, як вони погодилися почати працювати в компанії Fitbit, яка була конкурентом Jawbone (US Department of Justice, 2018).

Мета крадіжки комерційної таємниці офлайн та/або онлайн полягає у отриманні несправедливої конкурентної переваги. Несанкціоноване розкриття комерційної таємниці іноземному уряду, іноземному агенту (тобто «посадовій особі, працівнику, довірній особі, службовцю, посланцю або представнику іноземного уряду»; параграф 1839(2) титулу 18 Зводу законів США) або іноземній структурі (т. е.). "будь-якому агентству, бюро, міністерству, підрозділу, установі, асоціації або будь-якій юридичній, комерційній або діловій організації, корпорації, фірмі або суб'єкту, які значною мірою належать, контролюються, фінансуються, керуються урядом іноземної держави; параграф 1839(1) титулу 18 Зведення законів США) також може завдати шкоди національній економічній безпеці.

11.2 Причини, підстави та передбачувані мотиви правопорушень, що стосуються авторських прав та товарних знаків, що скоюються за допомогою кібертехнологій

Як можливі пояснення злочинів у сфері інтелектуальної власності, що скоюються за допомогою кібертехнологій, пропонуються різні кримінологічні, соціологічні, психологічні та економічні теорії (для отримання інформації про застосування цих та інших теорій до злочинів у сфері інтелектуальної власності, що скоюються за допомогою кібертехнологій). Одні дослідження показують, що на показники злочинності, пов'язаної з цифровим піратством, впливають соціокультурні норми, групова поведінка та групова динаміка (Gopal and Sanders, 1998; Shinet et al., 2004; Hinduja and Ingram, 2009; Higgins and Wilson, 2 and Makin, 2004; Higgins et al., 2012). Результати інших досліджень свідчать про те, що цифрове піратство є поведінкою, запозиченою від інших (Akers,

2009; Higgins, Fell, and Wilson, 2007; Hinduja and Ingram, 2008; Hinduja and Ingram, 2009; Skinner and Fream, 1997; Higgins Fell and Wilson, 2006).

Вважається, що особисті якості, такі як самовладання, «впливають... на ймовірність того, що людина буде залучена до незаконної діяльності, а також на частоту та масштаби зайняття нею такою незаконною діяльністю». Дослідження показали, що низький рівень самовладання (зокрема потреба в отриманні миттєвого задоволення), а також стреси, з якими стикаються люди (наприклад, нездатність заплатити гроші за твори, що охороняються авторським правом, або отримати до них доступ) (Hinduja, 2012); Hohn, Muftic, and Wolf, 2006) впливають на показники злочинності у сфері цифрового піратства (Higgins, 2004; Higgins and Wilson, 2006; Higgins and Makin, 2004; Higgins et al., 2008; Higgins, Fell, Malin and Fowers, 2009; Higgins, Fell, and Wilson, 2006; Hinduja and Ingram, 2008; Hinduja, 2012). Проте результати досліджень зв'язків між стресом, самовладанням та цифровим піратством неоднозначні. В інших дослідженнях були виявлені лише слабкі або незначні підтвердження зв'язку між стресом та цифровим піратством (Morris and Higgins, 2009) та між самоволодінням та цифровим піратством (Higgins and Wilson, 2006; Higgins, Wolfe, та Marcum, 2008; Hinduja, 2).

Було також встановлено, що виконавці злочинів у сфері інтелектуальної власності, скоєних за допомогою кібертехнологій, використовують певні методи (*техніку нейтралізації*), щоб «подолати почуття докору совісті або провини за поведінку, що суперечить загальноприйнятим нормам, цінностям і переконанням суспільства», і від загальноприйнятих обмежень шляхом виправдання чи обґрунтування своєї незаконної поведінки». Використовувані види техніки нейтралізації (*заперечення відповідальності; заперечення жертви; заперечення шкоди; засудження засуджуваних; і звернення до вищих цінностей*; Sykes and Matza, 1957) у сфері цифрового піратства бувають різними (Hinduja, 2007; Hinduja, 2007; and Marcum, 2008; Moore and McMullan, 2009; Morris and

Higgins, 2009; Ingram and Hinduja, 2008; Smallridge and Roberts, 2013; Siponen and Vance 2010). Ще одне дослідження показало, що цифрова асиметрія (наприклад, відсутність безпосереднього контролю за діями в Інтернеті) може сприяти поступовому «відхиленню» людей у цифрову девіантну поведінку та отриманню ними доступу до інформації/ресурсів, які підтримують або стандартизують протизаконні дії, такі як піратство (Brewer and Goldsmith, 2015; Dolliver and Love, 2015).

Антипідприємницькі настрої та (реальна та/або сприйнята) висока вартість творів, що охороняються авторським правом, сприяють злочинам у сфері інтелектуальної власності, що скоюються за допомогою кібертехнологій (Chaudhry et al., 2011; Maras, 2016). Оскільки для споживачів важливе значення мають справедливість та співвідношення між ціною та споживчою цінністю (Zeithaml, 1998; Seale et al., 1998), люди залучаються до дій (наприклад, купує товар та послуги або обмінюються ними), якщо вони розуміють, що вони «одержують рівні (або справедливі) відповідні результати від таких взаємин» (Glass and Wood, 1996, p. 1191). Якщо споживачі вважають, що існує несправедлива невідповідність між споживчою цінністю, якістю та ціною, вони шукають альтернативні способи одержання товару (за більш низькою ціною або за допомогою *піратства*, несанкціонованого придбання, доступу та/або використання чужої інтелектуальної власності). Дослідники також висунули припущення про те, що різке зростання показників цифрового піратства наприкінці 1990-х та на початку 2000-х рр. в. став результатом реакції громадськості на законодавчі перегини у сфері охорони інтелектуальної власності (Lessig, 2004; Lessig, 2008; Burkhardt, 2011).

Загалом, незважаючи на існування кількох теорій, застосовних до злочинів у сфері інтелектуальної власності, які здійснюються за допомогою кібертехнологій, результати застосування цих теорій для пояснення причин, підстав та мотивів цих злочинів у мережі Інтернет та поза мережею були суперечливими та неоднозначними.

11.3 Зусилля із захисту та профілактики

Запропоновані рішення проблеми злочинів у сфері інтелектуальної власності, що здійснюються за допомогою кібертехнологій, включають заходи кримінально-правового характеру, технічні рішення щодо обмеження несанкціонованого доступу до об'єктів інтелектуальної власності та просвітницькі кампанії. Заходи профілактики, що вживаються в галузі кримінального правосуддя, включають: моніторинг Інтернет-сайтів, на яких публікуються твори, що охороняються авторським правом; таємні розслідування щодо осіб, залучених до різних форм злочинів у сфері інтелектуальної власності, які здійснюються за допомогою кібертехнологій (наприклад, *Операція Fastlink*, в якій брали участь численні агентства США, які проводили кілька таємних операцій одночасно для ідентифікації і, зрештою, арешту осіб, відповідальних за незаконне поширення в Інтернеті творів, що охороняються авторським правом, таких як ігри, програмне забезпечення, музика, фільми; Department of Justice, 2004); закриття сайтів, які явно розповсюджують об'єкти інтелектуальної власності (наприклад, *Megaupload*); та судові переслідування осіб, залучених до злочинів у сфері інтелектуальної власності, які здійснюються за допомогою кібертехнологій (наприклад, учасників та адміністраторів онлайн-платформ, на яких розміщуються твори, що охороняються авторським правом). Більше того, такі компанії, як *Canada Goose* та *Chanel*, які стали жертвами злочинів у сфері інтелектуальної власності, що скоюються за допомогою кібертехнологій, подали до суду на торгові майданчики в Інтернеті через порушення прав на товарні знаки за продаж контрафактних версій своїх товарів (WIPR, 2018; ТВО, 2018).

Чи знаєте ви?

У різних країнах (наприклад, у Великій Британії та Малайзії) веб-сайти, що розміщують викрадені об'єкти інтелектуальної власності, публічно ідентифікуються та включаються до переліку сайтів-порушників

(IWL) (Muhamading, 2017). Перелік IWL, ведення якого є частиною програми Operation Creative Відділу британської поліції по боротьбі зі злочинністю у сфері інтелектуальної власності (PIPCU), використовується для ідентифікації піратських веб-сайтів з метою позбавлення їх доступу до рекламних доходів та/або їх значного скорочення шляхом інформування підприємств та компаній-рекламодавців про те, що їх реклама розміщується на незаконних сайтах, та проведення серед цих підприємств та компаній роз'яснювальної роботи, розповідаючи їм про можливу шкоду їхньому бренду від розміщення реклами на цих сайтах (City of London Police, 2016).

Заходи кримінального покарання також активно застосовуються як спосіб демонстрації того, що порушення прав інтелектуальної власності є серйозними та караються відповідно до чинного законодавства. Покарання за злочини у сфері інтелектуальної власності, які здійснюються за допомогою кібертехнологій, призначаються з метою стримування. Для того, щоб такий засіб *стримування* був ефективним, заходи покарання повинні бути: *суворими* (тобто шкода від покарання має переважувати вигоди від злочину); *певними* (тобто особа, яка вчиняє злочин, має каратися за скоєння цього злочину); і *невідкладними* (тобто особа карається недовзі після скоєння злочину). Заходи кримінального покарання порушення прав інтелектуальної власності орієнтовані *конкретне стримування* (тобто. особа, яке понесло покарання, припиняє подальші протиправні дії, якщо отримане покарання переважує вигоди від скоєння злочину), і *загальне стримування* (тобто. посиляють сигнал всім іншим, що подібна поведінка спричинить подібне суворе покарання). Однак сьогоdnішній характер Інтернету серйозно обмежує практичну здійсненність стримування, оскільки масштаб і частота випадків піратства значно перевершують можливості вживання будь-яких заходів протидії у відповідь (Dolliver and Love, 2015).

Крім заходів, спрямованих на виконавців злочинів у сфері інтелектуальної власності, що здійснюються за допомогою кібертехнологій, уряди здійснюють заходи до громадського осуду країн, які не захищають інтелектуальну власність, як того вимагають міжнародні, регіональні та національні закони. Наприклад, Офіс торгового представника США, який здійснює моніторинг стану справ у сфері охорони інтелектуальної власності США по всьому світу, складає щорічний звіт, в якому «зазначаються іноземні держави та перераховуються закони, принципи та практика, які не забезпечують адекватну та ефективну охорону та застосування прав ІВ для американських винахідників, творців, брендів, виробників та постачальників послуг, і визначаються торгові партнери в зарубіжних країнах, де умови охорони та застосування прав ІВ погіршилися або залишилися на колишньому неадекватному рівні, і де громадяни США, які розраховують на охорону їх права ІВ, відчують складнощі у отриманні справедливого та рівноправного доступу до ринків» (United States Trade Representative, 2018, p. 5).

Для боротьби з крадіжкою інтелектуальної власності також реалізуються технологічні рішення, такі як зашифрована передача інтелектуальної власності та використання спеціальних кодів та/або паролів для забезпечення доступу до інтелектуальної власності. Одним із таких технологічних рішень є технологія цифрових водяних знаків (тобто вбудований ідентифікаційний код, що включає інформацію про авторське право) (Chaudhry et al., 2011). Ще одним технологічним вирішенням проблеми злочинів у сфері інтелектуальної власності є технологія блокчейн (тобто надійні та автентичні транзакції, захищені криптографією), яку пропонується використовувати як безпечний реєстр об'єктів ІС (Clark, 2018).

Також вживаються заходи забезпечення кібербезпеки захисту даних, і навіть систем, у яких цей контент зберігається, і якими він

переміщається. Крім того, для запобігання несанкціонованому доступу до об'єктів інтелектуальної власності та їх використання реалізуються технічні заходи. Прикладами таких заходів є методи блокування та фільтрації (лекція 3).

Примітка

Довільне блокування або фільтрація контенту заборонено міжнародним правом у галузі прав людини (див. модуль 3 Серії модулів з кіберзлочинності: «Правова база та права людини» для отримання додаткової інформації).

Що стосується просвітницьких кампаній, ВОІВ проводить різноманітні щорічні заходи щодо підвищення обізнаності країн, організацій, підприємств та споживачів щодо охорони прав інтелектуальної власності та наслідків крадіжки об'єктів інтелектуальної власності. Цілі цих заходів та інших просвітницьких кампаній полягають у тому, щоб підвищити поінформованість про проблеми, пов'язані з крадіжкою інтелектуальної власності, та необхідність охорони інтелектуальної власності, а також зміцнити повагу до інтелектуальної власності шляхом зміни існуючих переконань та ставлення до інтелектуальної власності. Ці ініціативи орієнтовані на дітей та дорослих. Наприклад, інформаційно-просвітницька кампанія ВОІВ, орієнтована на молодь, *Повага інтелектуальної власності*, проводиться з метою поширення інформації для підвищення поінформованості про інтелектуальну власність та передбачає використання ресурсів та інтерактивних занять та засобів для дітей, а також вчителів, які цікавляться цим питанням, бажають викладати або зараз викладають цей предмет або хочуть дізнатися більше з цієї теми. ВОІВ також надає посилання на анімаційні відеоролики для дітей, в яких розповідається про те, що являють собою авторські права, товарні знаки та патенти.

Також проводяться національні просвітницькі кампанії з інтелектуальної власності. Наприклад, Міжнародна асоціація з товарних

знаків (INTA) та Група з заохочення прав інтелектуальної власності та управління ними (CIPAM) у 2017 році ініціювали просвітницьку кампанію з питань прав інтелектуальної власності у школах Індії, яка включала інтерактивну презентацію та ігри). Крім того, Відомство інтелектуальної власності Великобританії надає загальнодоступну інформацію про освітні ресурси, уроки, засоби та інтерактивні заняття для поширення знань про інтелектуальну власність, її важливість та права для учнів різних рівнів системи освіти (див., наприклад, Cracking Ideas (Відмінні ідеї)) .

Інформаційно-просвітницькі кампанії, що стосуються творів, що охороняються авторським правом, докладно інформують про проблеми негативного впливу порушень авторських прав на економіку та робочі місця в кіноіндустрії, книжковій справі, музичному бізнесі та індустрії програмного забезпечення. Просвітницькі кампанії, що належать до товарних знаків, спрямовані на інформування громадськості про шкоду, яку завдає контрафактна продукція. Як приклад можна навести Інформаційну кампанію УНП ООН «Контрафакт: не купуй продукцію злочинців» , яка була розроблена з метою підвищення поінформованості споживачів про підробку товарних знаків та її негативні особисті, соціальні та екологічні наслідки (UNODC, 2014b).

Висновок

Використовуючи Інтернет та інші цифрові технології, будь-яка людина може отримати доступ до контенту, що охороняється, миттєво переглядати і повторно поширити його по всьому світу. Як розв'язання проблеми злочинів у сфері інтелектуальної власності, що здійснюються за допомогою кібертехнологій, пропонуються заходи в галузі кримінального правосуддя, технологічні рішення щодо обмеження несанкціонованого доступу до інтелектуальної власності та інформаційно-просвітницькі кампанії. Незважаючи на вживані на національному, регіональному та міжнародному рівнях заходи нормативно-правового характеру, простота, легкість та дешевизна тиражування, зберігання, поширення та/або іншого

способу забезпечення доступності об'єктів інтелектуальної власності роблять зусилля щодо розслідування цих кіберзлочинів, їх запобігання та переслідування осіб, у їх скоєнні, дуже скрутними для відповідних органів та установ у всьому світі.

Питання для самоперевірки

1. Чому захист інтелектуальної власності важливий?
2. Які існують види інтелектуальної власності?
3. Назвіть два приклади міжнародних та регіональних документів, що захищають інтелектуальну власність. Які типи інтелектуальної власності вони захищають?
4. Які теорії використовувалися для пояснення порушень авторського права та/або торговельних марок у кібернетичному режимі?
5. Які національні, регіональні та міжнародні заходи захисту та запобігання вжито для захисту інтелектуальної власності?

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Steve Anson. Applied incident response. Wiley. Computer science books. 2021y. 437pp.
2. Джерело: (2001). Семінар для судових експертів із цифрових злочинів [Digital Forensic Research Workshop (DFRWS)].
3. Хейєс, Д., Сафарі та О'Рейлі Медіа Компані [Hayes, D., & Safari, an O'Reilly Media Company]. (2020). *Практичні керівні настанови щодо розслідувань кримінальних правопорушень у цифровій сфері [A Practical Guide to Digital Forensics Investigations]*, 2 видання (1 видання, ред.).
4. Чау, К., Шеной, С. [Chow, K., & Sheno, S.] (2010). Досягнення в галузі цифрової криміналістики, VI Міжнародна конференція з цифрової криміналістики IFIP [Advances in Digital Forensics VI Sixth IFIP WG 11.9 International Conference on Digital Forensics], Гонконг, Китай, 04-06 січня 2010 року, Відредаговані відібрані статті (1 видання, ред. 2010 року, «Досягнення інформаційних та комунікаційних технологій» IFIP, 337 с. [Revised Selected Papers (1st ed. 2010. ed., IFIP Advances in Information and Communication Technology, 337)]).
5. Петерсон, Гілберт (Peterson, Gilbert,) та Шеной, Суджит (Sujeet, Sheno). *Досягнення в галузі цифрової криміналістики, V міжнародна конференція з цифрової криміналістики IFIP WG 11.9 [Advances in Digital Forensics V Fifth IFIP WG 11.9 International Conference on Digital Forensics]*, м. Орlando, штат Флорида, США, 26-28 січня 2009 року, Відредаговані відібрані статті. 1 видання, ред. 2009 року. мм. Берлін, Гайдельберг: Видавництво «Springer Berlin Heidelberg», 2009. Вебресурс
6. Г. Портокалідіс (дата публікації відсутня). CS 695 – Вступ до криміналістики хостів. Технологічний інститут ім. Стівенса
7. Д. Бем та Е. Губенер (2007). Криміналістичний аналіз комп'ютерів у віртуальних середовищах. Міжнародний журнал цифрових доказів. Том 6, випуск 2.

8. Лей Жанг, Донг Жанг та Лянхай Ванг «Цифрове дослідження віртуальних машин наживо», *Міжнародна конференція з комп'ютерних програм та системного моделювання 2010 р. (ICCASM 2010)*, 2010, ст. V4-328-V4-332, ідентифікатор цифрового об'єкта (doi): 10.1109/ICCASM.2010.5620364.

9. С. Лайлс, 2016. Атрибуція кіберзлочинів. Sveoti. <https://sveoti.net/?p=6791>.

10. К. Ческі, 2015. Хто був по той бік екрану? Атрибуція винних у розслідуваннях цифрових доказів. Міжнародний журнал цифрових доказів, том 4 (1), с. 1-12.

11. Б. Керіер, 2003. Визначення засобів цифрової криміналістичної експертизи й аналізу з використанням шарів абстракції. *Міжнародний журнал цифрових доказів, том 1 (4), с. 1-12*.

12. Палмер, Г. Л. (2002) Криміналістична експертиза у цифровому світі: некомерційна організація MITRE Corporation. Міжнародний журнал цифрових доказів, 1.

13. Ф. Коен (2006). Виклики при роботі з цифровими криміналістичними доказами. Нью Хейвен, Фред Коен та партнери.

14. Кобозєва А.А., Зоріло В.В. Метод виявлення фальсифікації цифрового зображення в умовах збурних дій. Збірник наукових праць Військового інституту Київського національного університету ім.Т.Шевченка. 2009. Вип.№20. С.147-154.

15. ITU Global Cybersecurity Index 2020, 4th edition Weightage Recommendations. URL: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>

16. NirSoft. Утиліти для цифрової криміналістики. URL: nirsoft.net