ТЕМА 3

ПОНЯТТЯ КІБЕРЗЛОЧИНІВ ТА ЇХ КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА

1.Поняття кіберзлочинності та її ознаки. Співвідношення з поняттями «злочинність у сфері використання електронно-обчислювальних машин», «комп'ютерна злочинність», «злочинність у віртуальному просторі», «злочинність у сфері інформаційних технологій», «злочинність у сфері IT - технологій» тощо.

2. Класифікація кіберзлочинів.

3. Кримінологічна характеристика кіберзлочинів: динаміка, рівень, географія, тенденції, ціна кіберзлочинності.

4. Кримінологічна характеристика особи кіберзлочинця.

5. Ціна кіберзлочинності

1. Поняття **кіберзлочинності** визначено на національному рівні в ЗУ «Про основні засади кібербезпеки України» - як **сукупність кіберзлочинів (комп'ютерних злочинів).**

Комп'ютерний злочин (комп'ютерне кримінальне правопорушення) – суспільно-небезпечне винне діяння у кіберпросторі та/ або з його використанням, відповідальність за яке передбачена Кримінальним кодексом України та/або яке визнано злочином міжнародними договорами.

«злочинність у сфері використання електронно-обчислювальних машин», «комп'ютерна злочинність», «злочинність у віртуальному просторі», «злочинність у сфері інформаційних технологій», «злочинність у сфері IT – технологій».

Універсальним та найбільшим розповсюдженим є термін кіберзлочин (cibercrime), саме цей термін використовується на міжнародному рівні і згадується в Конвенції РЄ «Про кіберзлочинність» та ЗУ «Про основні засади кібербезпеки»

В Кримінальному кодексі України є Розділ XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» ст. 361-363.

- В основу належності кримінального правопорушення до кіберзлочину (комп’ютерного кримінального правопорушення) закладають, зокрема, такі критерії:
- комп’ютерними називають ті кримінальні правопорушення, які законодавець об’єднав у Розділі XVI Особливої частини КК. Ознакою, яка відрізняє кіберзлочини від інших та об’єднує їх у певну групу є родовий об’єкт цих кримінальних правопорушень;
- комп’ютерним є кримінальне правопорушення, яке вчиняється з використанням ЕОМ, телекомунікаційних систем, комп’ютерних мереж і мереж електрозв’язку (знаряддя кримінального правопорушення)

- комп’ютерним є кримінальне правопорушення, предметом якого є комп’ютерна інформація, що обробляється в ЕОМ, АС, комп’ютерних мережах чи мережах електрозв’язку;
- кіберзлочином є кримінальне правопорушення, в якому комп’ютер є або предметом або знаряддям або способом вчинення кримінального правопорушення;
- кіберзлочини – це кримінальне правопорушення, в яких кіберпростір є середовищем, предметом (метою) посягання та/або способом його вчинення

- спільною, інтегруючою та, одночасно, найбільш істотною ознакою проявів кримінально протиправної поведінки які належать до кіберзлочинів, є те, що у процесі їх вчинення задіяні інформаційні (комп'ютерні) системи. Ці системи є або **об'єктом** кримінально протиправної поведінки, тим, проти чого спрямоване конкретне діяння винного, або використовуються у процесі кримінально протиправної діяльності, як, зокрема, **знаряддя**, **засіб**, **місце**, **спосіб** вчинення суспільно небезпечного діяння. Ця ознака відрізняє їх від інших видів кримінально протиправної поведінки, та, відповідно, дозволяє виділити цю групу кримінально протиправної поведінки в окремий вид злочинності – кіберзлочинність. Тобто у процесі вчинення (скоєння) кіберзлочину злочинець використовує особливі можливості, властивості, якими наділені інформаційні (комп'ютерні) системи

У міжнародній доктрині поняттями кіберзлочини, кіберзлочинність охоплюються різні види правопорушень. У п. 14 Доповіді Комітету II Десятого Конгресу ООН 2000 року по попередженню злочинності і поводженню з правопорушниками було зазначено, що існує дві категорії кіберзлочинів:

1) кіберзлочини у вузькому розумінні («комп'ютерні злочини»): будь-яке протиправне діяння, здійснюване шляхом електронних операцій, метою якого є подолання захисту комп'ютерних систем і оброблюваних ними даних;

2) кіберзлочини в широкому розумінні («злочини, пов'язані з використанням комп'ютерів»): будь-яке протиправне діяння, яке вчиняється шляхом або в зв'язку з комп'ютерною системою або мережею, включаючи такі злочини, як незаконне зберігання, пропонування або розповсюдження інформації через комп'ютерні системи або мережі

Найбільш поширена класифікація кіберзлочинів в даний час ґрунтується на структурі Конвенції Ради Європи про кіберзлочинність від 23.11.2001 року. За конвенцією Ради Європи про кіберзлочинність існує чотири основних групи кіберзлочинів.

До першої групи належать правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем: незаконний доступ (ст. 2), нелегальне перехоплення (ст. 3), втручання у дані (ст. 4), втручання у систему (ст. 5), зловживання пристроями (ст. 6).

До другої групи входять правопорушення, пов'язані з комп'ютерами: підробка та шахрайство, пов'язані з комп'ютерами (статті 7, 8).

Третю група: правопорушення, пов'язані з дитячою порнографією (ст. 9) (пов’язані зі змістом).

Четверта група: правопорушення, пов'язані з порушенням авторських та суміжних прав (ст. 10)

П’ята група - злочини, зафіксовані в окремому протоколі (акти расизму та ксенофобії, вчинені за доромогою комп’ютерних мереж)

Залежно від **об’єкту посягання** кіберзлочини (комп’ютерні злочини) класифікують за такими видами:

(1)

Злочини, вчинені у кіберпросторі та/або з його використанням, відповідальність за які передбачена різними розділами КК України. Такі злочини посягають на різні об’єкти кримінально-правової охорони: основи національної безпеки, громадську безпеку, відносини у сфері охорони права на об’єкти інтелектуальної власності, власність, господарські відносини, права та свободи тощо. Ознакою віднесення цих злочинів до кіберзлочинів є те, що вони вчиняються з використанням сучасних інформаційних технологій і засобів комп’ютерної техніки.

Наприклад:

викрадення реквізитів платіжних карток (фішинг, вішинг, шиммінг, скимінґ);

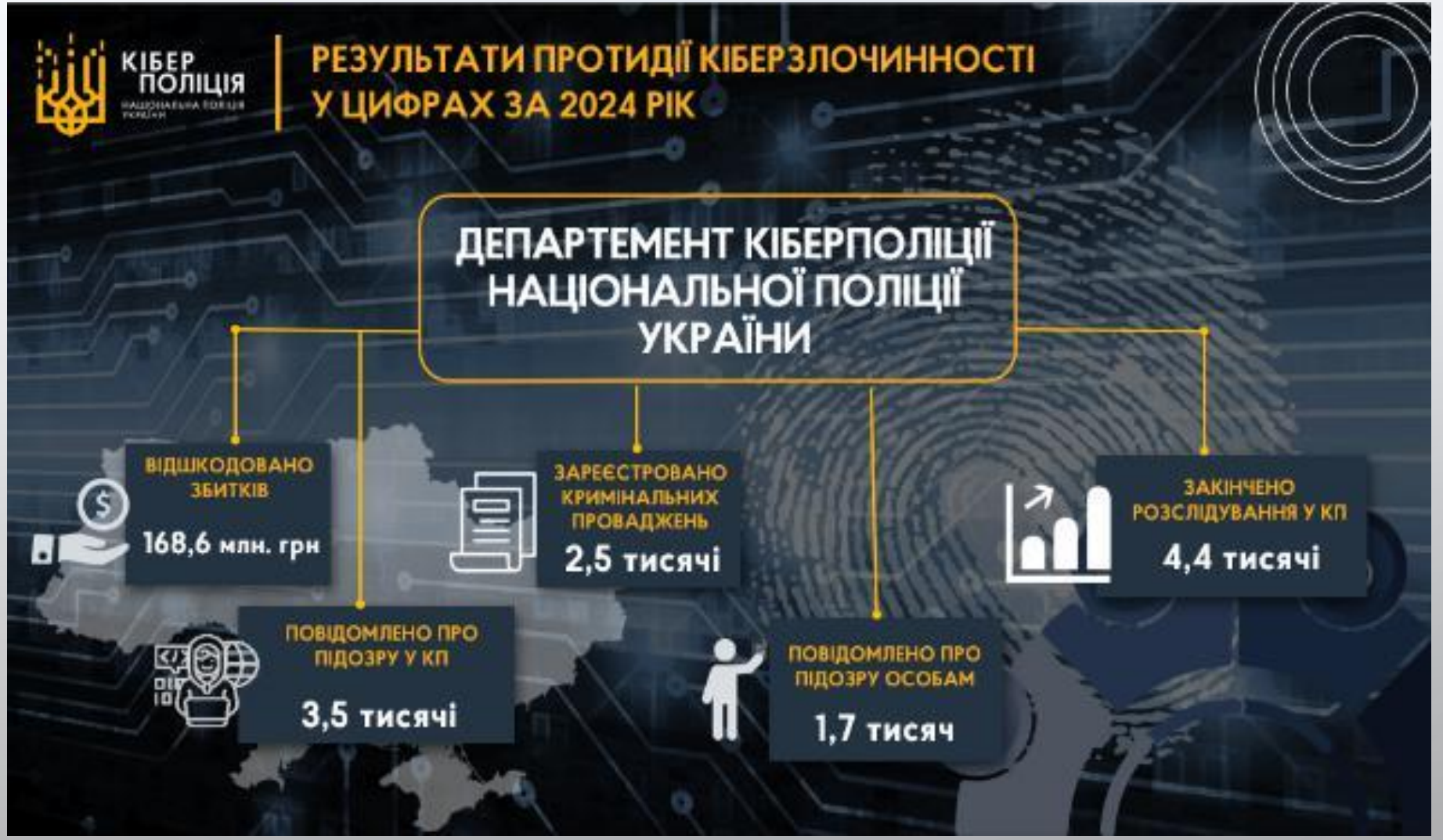
незаконні фінансові операції з використанням платіжних карток або їх реквізитів, які не ініційовані або не підтверджені її власником (кардінг); заволодіння коштами через фіктивні інтернет-магазини, інтернет-аукціони, сайти та інші засоби телекомунікації (онлайн–шахрайство);

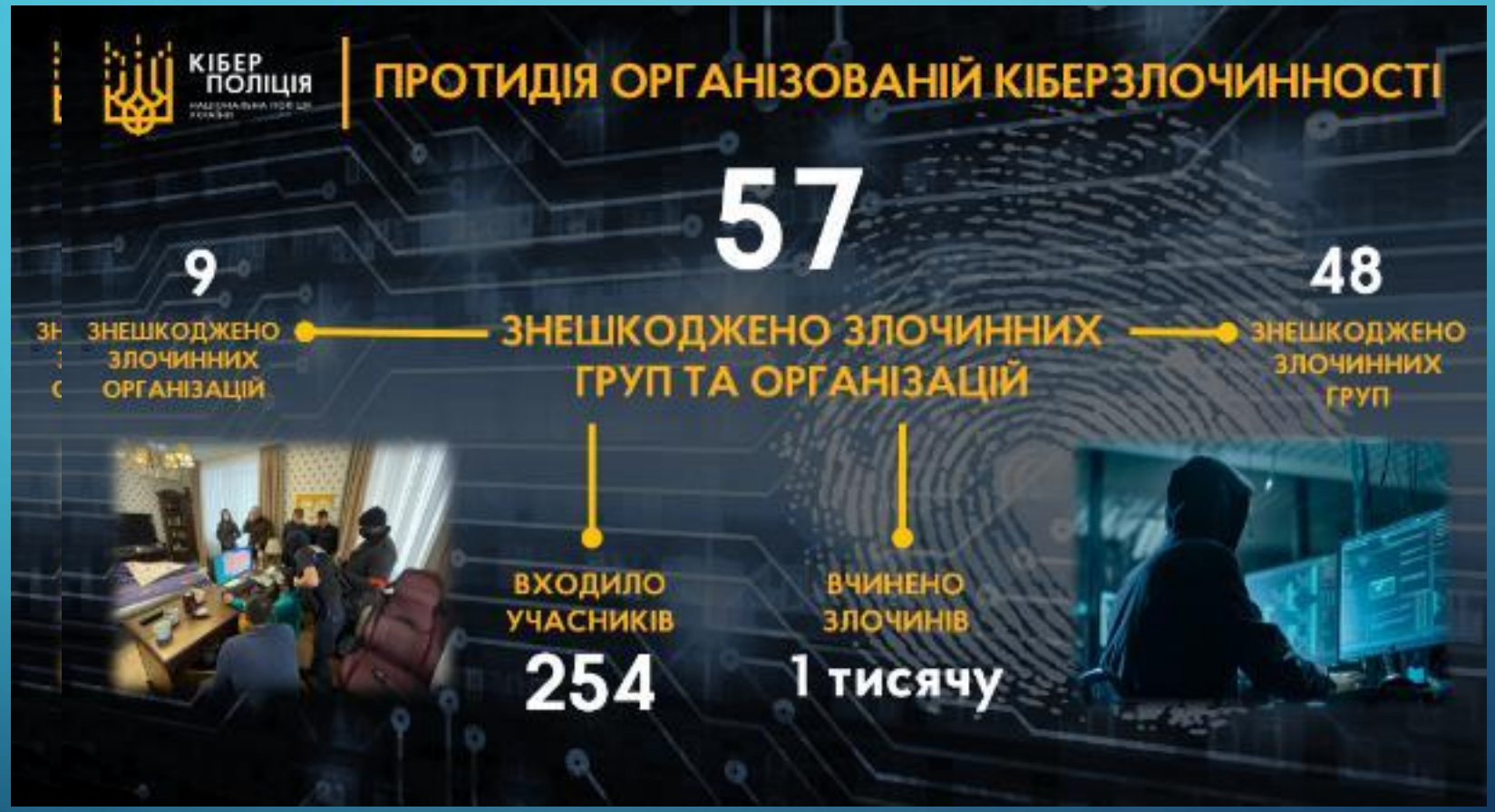
порушення авторського права і суміжних прав шляхом незаконного розповсюдження програмних продуктів через комп'ютерні мережі (піратство) тощо.

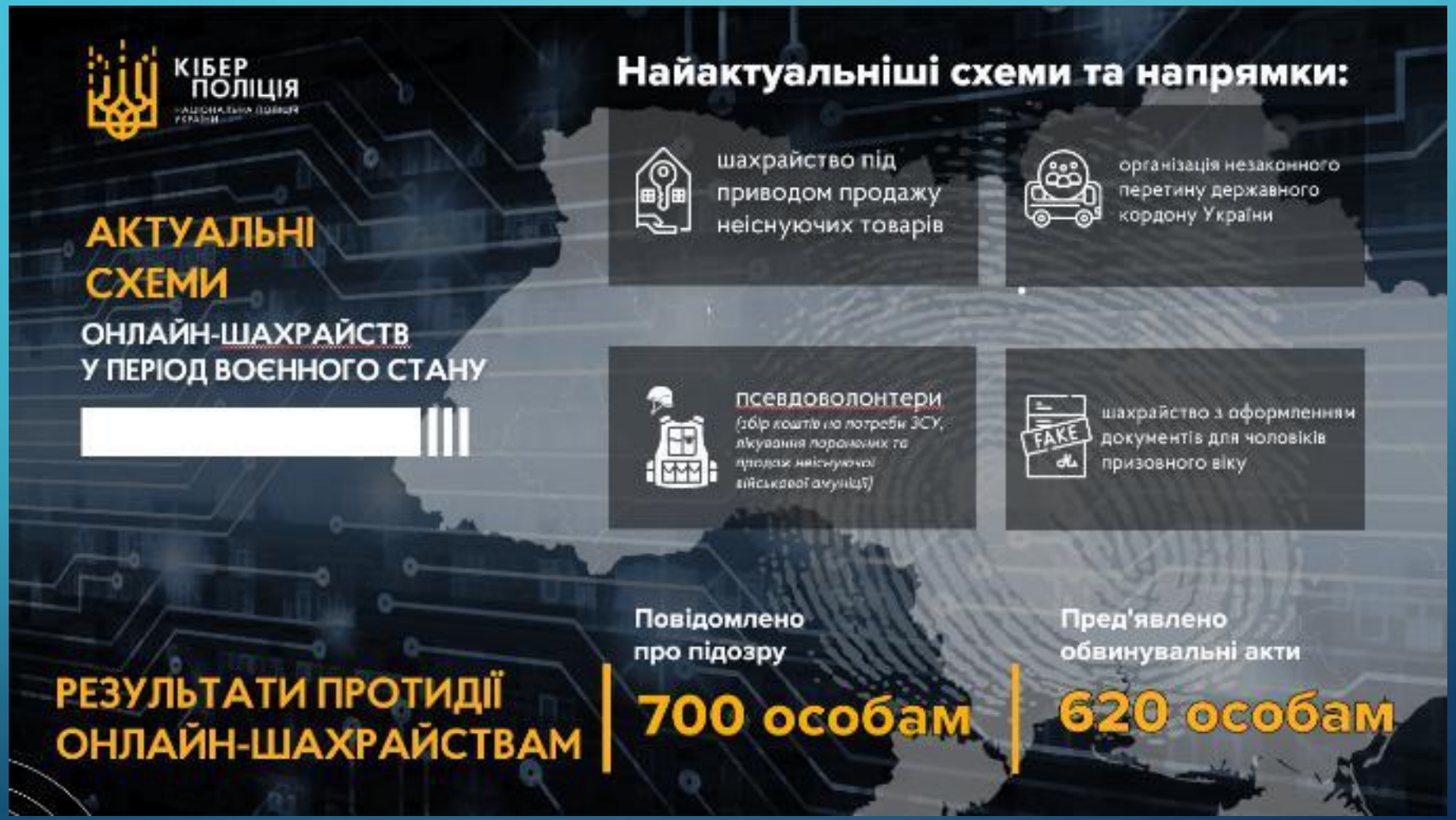
Залежно від **об’єкту посягання** кіберзлочини (комп’ютерні злочини) класифікують за такими видами:

(2)

Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж, що передбачені Розділом XVI КК України. Ознакою віднесення цих злочинів до комп’ютерних є те, що вони посягають на відносини, що виникають у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку.


КІБЕР ПОЛІЦІЯ
РЕЗУЛЬТАТИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ У ЦИФРАХ ЗА 2024 РІК
ДЕПАРТЕМЕНТ КІБЕРПОЛІЦІЇ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ
ВІДШКОДОВАНО ЗБИТКІВ
168,6 млн. грн
ЗАРЕЄСТРОВАНО КРИМІНАЛЬНИХ ПРОВАДЖЕНЬ
2,5 тисячі
ЗАКІНЧЕНО РОЗСЛІДУВАННЯ У КП
4,4 тисячі
ПОВІДОМЛЕНО ПРО ПІДОЗРУ У КП
3,5 тисячі
ПОВІДОМЛЕНО ПРО ПІДОЗРУ ОСОБАМ
1,7 тисяч


КІБЕР ПОЛІЦІЯ
ПРОТИДІЯ ОРГАНІЗОВАНІЙ КІБЕРЗЛОЧИННОСТІ
57
ЗНЕШКОДЖЕНО ЗЛОЧИННИХ ГРУП ТА ОРГАНІЗАЦІЙ
9
ЗНЕШКОДЖЕНО ЗЛОЧИННИХ ОРГАНІЗАЦІЙ
48
ЗНЕШКОДЖЕНО ЗЛОЧИННИХ ГРУП
ВХОДИЛО УЧАСНИКІВ
254
ВЧИНЕНО ЗЛОЧИНІВ
1 тисячу


КІБЕР ПОЛІЦІЯ
НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ
АКТУАЛЬНІ СХЕМИ
ОНЛАЙН-ШАХРАЙСТВ
У ПЕРІОД ВОЄННОГО СТАНУ
Найактуальніші схеми та напрямки:
шахрайство під приводом продажу неіснуючих товарів
організація незаконного перетину державного кордону України
псевдоволонтери
(збір коштів на потреби ЗСУ, лікування поранених та продаж неіснуючої військової амуніції)
FAKE
шахрайство з оформленням документів для чоловіків призовного віку
РЕЗУЛЬТАТИ ПРОТИДІЇ ОНЛАЙН-ШАХРАЙСТВАМ
Повідомлено про підозру
700 особам
Пред'явлено обвинувальні акти
620 особам

учасники міжнародного злочинного угрупування (всього нараховується понад 200 учасників), використовуючи мережу Інтернет та електронно-обчислювальну техніку, займались викраденням безготівкових коштів з банківських карт громадян країн Європи, зокрема Чехії, Польщі, Франції, Іспанії, Португалії. Відповідно до відведених ролей у вчиненні злочинів, члени міжнародного угрупування, котрі проживали та здійснювали свою діяльність на території України, займались розробленням фішингових сайтів з метою створення шахрайських посилань з купівлі-продажу товарів та послуг, внаслідок чого, отримували доступ до електронних гаманців потерпілих осіб задля подальшого заволодіння та виведення їхніх грошових коштів. Інші учасники відповідали за створення банківських рахунків і акаунтів на підставних осіб, через здійснювалося виведення безготівкових коштів у готівку. Від протиправних дій міжнародного злочинного угрупування потерпілим завдано шкоди в еквіваленті понад 160 млн грн

*злочинна організація у складі **13-ти осіб**, які з метою розповсюдження шкідливих програмних і технічних засобів, призначених для несанкціонованого втручання в роботу системи «Клієнт-Банк», здійснювали перевипуск SIM-картки номеру мобільного телефону та надсилали шкідливий програмний засіб на поштову скриньку, таким чином отримували доступ до персонального комп'ютера, на якому інстальована система «Клієнт-Банк». У підсумку шляхом проведення ряду транзакцій заволоділи коштами в сумі близько **11 млн грн;***

*злочинна організація у складі **8-ми осіб**, з використанням електронно-обчислювальної техніки, спеціалізуючись на розроблені фішингових-повідомлень, які імітували офіційні урядові та банківські вебсайти України, пропонували громадянам України та особам, які постраждали внаслідок військових дій на території України, отримання грошової допомоги від Президента України, ООН, «UNICEF» та ін. Фішингові посилання надавали змогу учасникам злочинної організації отримати доступ до електронного кабінету онлайн-банкінгу. Після чого зловмисники проводили заміну фінансового номеру в обліковому записі та прив'язування банківської картки до інших облікових записів, з метою подальшого заволодіння і виведенням коштів постраждалих осіб за допомогою платіжних сервісів. Від протиправних дій злочинної організації було завдано шкоди на загальну суму **700 тис. грн.***

ОЗНАКИ КІБЕРЗЛОЧИННОСТІ:
ПОШИРЮЄТЬСЯ НА СЕРЕДОВИЩЕ, ЩО НАДАЄ МОЖЛИВОСТІ ДЛЯ ЗДІЙСНЕННЯ КОМУНІКАЦІЙ ТА/АБО РЕАЛІЗАЦІЇ СУСПІЛЬНИХ ВІДНОСИН; ВЧИНЯЄТЬСЯ У ВІРТУАЛЬНОМУ ПРОСТОРІ В МЕЖАХ МЕРЕЖІ ІНТЕРНЕТ ТА/АБО ІНШИХ ГЛОБАЛЬНИХ МЕРЕЖ ПЕРЕДАЧІ ДАНИХ; ВЧИНЯЮТЬСЯ ЗА ДОПОМОГОЮ КОМП'ЮТЕРНИХ СИСТЕМ АБО ШЛЯХОМ ВИКОРИСТАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ ТА ІНШИХ ЗАСОБІВ ДОСТУПУ ДО ВІРТУАЛЬНОГО ПРОСТОРУ, А ТАКОЖ ПРОТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

У 1991 році кодифікатор Інтерполу був інтегрований в автоматизовану систему пошуку і в даний час доступний більш ніж у 100 країнах. Усі коди, що характеризують комп'ютерні злочини, мають ідентифікатор, що починається з букви Q. Для характеристики злочину можуть використовуватися до п'яти кодів, розташованих у порядку убування значимості скоєного. · QA - Несанкціонований доступ і перехоплення · QAH - комп'ютерний абордаж · QAI - перехоплення · QAT - крадіжка часу · QAZ - інші види несанкціонованого доступу і перехоплення · QD - Зміна комп'ютерних даних · QUL - логічна бомба · QDT - троянський кінь · QDV - комп'ютерний вірус · QDW - комп'ютерний черв · QDZ - інші види зміни даних · QF - Комп'ютерне шахрайство · QFC - шахрайство з банкоматами · QFF - комп'ютерна підробка · QFG - шахрайство з ігровими автоматами · QFM - маніпуляції з програмами введення-висновку · QFP - шахрайства з платіжними засобами · QFT - телефонне шахрайство · QFZ - інші комп'ютерні шахрайства · QR - Незаконне копіювання · QRG - комп'ютерні ігри · QRS - інше програмне забезпечення · QRT - топографія напівпровідникових виробів · QRZ - інше незаконне копіювання · QS - Комп'ютерний саботаж · QSH - з апаратним забезпеченням · QSS - із програмним забезпеченням · QSZ - інші види саботажу · QZ - Інші комп'ютерні злочини · QZB - з використанням комп'ютерних дощок оголошень · QZE - розкрадання інформації, що складає комерційну таємницю · QZS - передача інформації конфіденційного характеру · QZZ - інші комп'ютерні злочини

Розділ XVI

КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ

Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж

Стаття 361^{-1}. Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут

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

Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї

Стаття 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється

Стаття 363^{-1}. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку

Ч.4 ст. 190 КК - Шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки

Стаття 158. Надання неправдивих відомостей до органу ведення Державного реєстру виборців або інше несанкціоноване втручання в роботу Державного реєстру виборців

Стаття 163. Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер

Стаття 176. Порушення авторського права і суміжних прав

Стаття 200. Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення

Стаття 301^{-1}. Одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження

Стаття 376^{-1}. Незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя

Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж

https://zakon.rada.gov.ua/laws/show/2341-14?find=1&text=182#Text

Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж

карається штрафом від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян або пробаційним наглядом на строк до трьох років, або обмеженням волі на той самий строк

Ч. 3 ст. 361 КК передбачає відповідальність за дії, передбачені частиною першою або другою цієї статті, якщо вони призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації

- **Несанкціоноване втручання в роботу ЕОМ**, систем або комп'ютерних мереж – зміна режиму роботи ЕОМ, системи або комп'ютерної мережі, вчинена шляхом впливу на носікомп'ютерної інформації або засоби її автоматизованого опрацювання, з порушенням установленого відповідно до законодавства порядку доступу до інформації, що заподіює шкодусуспільним відносинам власності на ком'пютерну інформацію.
- **ВИТІК** комп'ютерної інформації – це результат дій, унаслідок яких інформація в системі стає відомою чи доступною фізичним/юридичним особам, які не мають права доступу до неї
- **ВТРАТА** комп'ютерної інформації – це такий вплив на носій комп'ютерної інформації, унаслідок якого вона перестає існувати у формі, яка дозволяє опрацьовувати її за допомогою комп'ютерної техніки

- **ПІДРОБКА** комп'ютерної інформації – порушення такого повноваження власника, як користування, адже через підробку власник повністю або частково втрачає можливість реалізовувати свою інформаційну потребу.
- **БЛОКУВАННЯ** комп'ютерної інформації – відсутність у власника можливості використовувати інформацію для задоволення інформаційної потреби, за умови, що її не втрачено і не підроблено
- **СПОТВОРЕННЯ ПРОЦЕСУ ОБРОБКИ** комп'ютерної інформації – це отримання під час операцій з комп'ютерною інформацією, які здійснювалися за допомогою технічних чи програмних засобів, результатів, що не відповідають характеристикам технічних засобів або алгоритму комп'ьютерної програми
- **ПОРУШЕННЯ ВСТАНОВЛЕНОГО ПОРЯДКУ МАРШРУТИЗАЦІЇ** комп'ютерної інформації – ненадходження комп'ютерної інформації, що передається за допомогою комп'ютерної мережі конкретному абонентові (абонентам), або здійснення доступу до певних мережевих ресурсів з порушенням встановленого порядку

- Такі дії караються штрафом від семи тисяч (119000 грн) до десяти тисяч (170000 грн) неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від трьох до восьми років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого

https://reyestr.court.gov.ua/Review/114884775

Стаття 361^{-1}. Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут

Створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж

караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на строк до трьох років

ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду

караються позбавленням волі на строк до п’яти років

- Брак чіткого визначення терміна «шкідливий програмний засіб» (**ШПЗ**) унеможливлює формування єдиного підходу до кваліфікації протиправного діяння, пов'язаного з його використанням, пошуку та фіксації, а також проведення комп'ютерно-технічних експертиз.
- У жодному чинному нормативному акті не запропоновано дефініцію поняття ШПЗ, не схарактеризовано криміналістичні ознаки та критерії віднесення їх до категорії шкідливих.

Шкідливий програмний засіб має відповідати критеріям, що визначають цільове призначення ШПЗ, зокрема це несанкціоноване втручання в роботу в електронно-обчислювальну техніку (**ЕОТ**). Отже, ШПЗ можна вважати будь-який програмний засіб, що має приховану деструктивну властивість, за таких умов:

1) призначений для несанкціонованого втручання, зміни, модифікації, блокування, копіювання або знищення інформації, споживання технічних ресурсів ЕОТ, використовує спеціально для цього розроблений програмний код (сигнатуру, модуль), що заздалегідь визначений розробником;

2) наявність середовища, через яке здійснено проникнення (локально, через Інтернет, окремі оптичні, магнітні носії або конкретна команда на ЕОТ);

3) наявність певної події яка передувала проникненню ШПЗ, або системного алгоритму, завдяки якому почав діяти ШПЗ (наприклад, встановлений клієнт-банк, Інтернет-гаманець електронних грошей тощо);

4) самодостатність програмного коду ШПЗ для втілення задуму розробника;

5) достатня стійкість ШПЗ до подолання систем захисту ЕОТ.

- Судова практика засвідчує, що програмні засоби можуть бути шкідливими, якщо вони за своїми ознаками здатні несанкціоновано порушити конфіденційність, доступність і цілісність інформації, яку опрацьовують через автоматизовану систему або передають мережами електрозв’язку [9].
- Саме прихованість, деструктивність і несанкціонованість є визначальними ознаками ШПЗ. Тобто для віднесення програмного засобу до категорії шкідливих спеціаліст, експерт мають, насамперед, визначити саме такі його риси.

- Щоб констатувати приналежність програмного засобу до категорії шкідливих, він має відповідати одночасно всім окресленим критеріям. Для встановлення їх наявності потрібні спеціальні знання, тому для аналізу ШПЗ призначають судову комп'ютерно-технічну експертизу [11], різновидом якої є програмно-комп'ютерна експертиза [12].

Дії, передбачені ч.1-ч.4 ст. 361 КК, не вважаються несанкціонованим втручанням в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, якщо вони були вчинені відповідно до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж

- Будь-який програмний засіб, якщо в ньому міститься хоча б одна деструктивна (шкідлива) або прихована функція, що діє без згоди користувача або оператора, становить суспільну небезпеку. Наприклад, легальне програмне забезпечення, що містить приховану функцію надання віддаленого доступу до комп'ютера користувача та здійснення такого несанкціонованого втручання без згоди його власника або користувача, на думку фахівців, необхідно визнавати як ШПЗ.
- Неоднозначними є питання кваліфікації програмних засобів, які за низкою ознак належать до категорії шкідливих, однак такими не є. Це, зокрема, програмні засоби, які хоч і розроблен для несанкціонованого втручання в роботу ЕОТ, однак мають спеціальне призначення – їх застосовують працівники правоохоронних органів для документування протиправної діяльності (перехоплення електронної пошти, паролів, закриття доступу до протиправного контенту, військового, лабораторного чи дослідницького призначення).
- Також такими програмними засобами користується спеціаліст, який перевіряє (проводить аудит) ступеня захищеності ЕОТ від несанкціонованого втручання. Такі програмні засоби за своїм призначенням, конструктивними особливостями та дією схожі на ШПЗ.

- До цієї категорії програмних засобів відносять і шкідливі програмні засоби, які спеціально для цього створені, однак їх використовують з дозволу керівництва суб'єкта господарювання для стеження за підлеглими з метою профілактики вчинення ними протиправних дій або неефективного використання робочого часу. Працівників попереджають про встановлення на ЕОТ, якими вони користуються, таких ШПЗ. Такі програмні засоби, здебільшого, проходять реєстрацію, мають необхідну ліцензію, їх використання в кожному конкретному випадку санкціоноване відповідними державними органами або керівництвом суб'єкта господарювання, хоча використання їх є негласним.
- Якщо правопорушник, який створив, заволодів або мав намір використати нефункціональне ШПЗ, помилково вважаючи його цілком функціональним і таким, що може бути використаний за протиправним призначенням, його дії слід кваліфікувати як замах на вчинення злочину за ст. 15 і відповідною частиною ст. 361-1 КК України.
- https://reyestr.court.gov.ua/Review/115837971

- ОСОБА_4 , будучи обізнаним про принципи дії шкідливих програмних засобів та наслідки їх використання, заборону розповсюдження шкідливого програмного забезпечення, використовуючи належний йому персональний комп`ютер з магнітним жорстким диском «Hitachi», модель «HDT722525DLA380», об`ємом 250 Гб, серійний номер «T8DT06DH», у невстановлені досудовим розслідуванні спосіб, місці та часі, але не пізніше 20.06.2023 року, отримав файл «12345.exe», що міститься в архіві з назвою «12345.rar». У подальшому, ОСОБА_4 , перебуваючи за адресою свого проживання (АДРЕСА_1),використовуючи IP адреси НОМЕР_1 , НОМЕР_2 , надані інтернет-провайдером ТОВ «Нетворк Львів», код ЄДРПОУ 43905581, зареєстрованого за адресою: м. Львів, вул. Перфецького, 21, офіс 37, діючи з прямим умислом, з метою подальшого несанкціонованого втручання в роботу інформаційно-комунікаційних систем невизначеного кола користувачів, розповсюдив шляхом завантаження у загальний доступ мережі інтернет, а саме на сервіс файлобмінника mediafire.com, 20.06.2023 о 14:16 год (згідно налаштувань часу на серверному обладнанні) файл «12345.exe», що міститься в архіві з назвою «12345.rar», який згідно висновку експерта відноситься до сімейства шкідливого програмного забезпечення шпигунських програм з загальною назвою Trojan-Spy, які використовуються для крадіжки інформації користувачів різних платіжних онлайн і банківських систем.

- також, ОСОБА_4 20.06.2023 року та 23.06.2023 року розповсюдив шкідливі програмні засоби шляхом завантаження їх у загальний доступ мережі інтернет, а саме на сервіс файлобмінника mediafire.com, та очікував, щоб будь-хто завантажив та виконав файл із шкідливим програмним засобом, відтак вчинив усі дії, які вважав за необхідне для подальшого несанкціонованого втручання в роботу інформаційно-комунікаційних систем будь-яких осіб, хто завантажить вказане шкідливе програмне забезпечення.
- Так, 02.07.2023 року ОСОБА_6 , перебуваючи за адресою свого проживання, а саме: АДРЕСА_2 , за допомогою свого персонального комп`ютера перейшов за посиланням на файл, який був розміщений на сервісі файлобмінника mediafire.com, та завантажив на свій персональний комп`ютер архів із, як він вважав, патчем (модифікацією) до гри « GTA5 online », який насправді був шкідливим програмним засобом. Після завершення процесу розархівування, близько 11:16 год. 02.07.2023 року ОСОБА_6 запустив вказаний файл, що розпочав передачу даних на належний ОСОБА_4 персональний комп`ютер з магнітним жорстким диском «Hitachi», модель «HDT722525DLA380», об`ємом 250 Гб, серійний номер «T8DT06DH», однак антивірус, що встановлений на персональному комп`ютері ОСОБА_6 , сповістив останнього про шкідливість зазначеного файлу та припинив його роботу.

Характерні приклади:
направлено до суду обвинувальний акт у кримінальному провадженні за ч.2, 4 ст. 27,
Ч.3 ст. 28, частиною 5 ст. 190, ч.2 ст. 361, ч. 1,2 ст. 255 КК
стосовно учасників злочинної організації, які за допомогою Інтернету (соціальні мережі, месенджери)
розповсюдження фішингових посилань щодо виплат грошової допомоги від Президента України, ООН, UNICEF та інших видів допомоги, що в подальшому давало змогу отримати доступ до електронного кабінету онлайн-банкінгу потерпілих.
З метою заволодіння коштами громадян фігуранти здійснювали телефонні дзвінки потерпілим, у ході яких представлися працівниками служб безпеки банківських установ для підтвердження безпечності проведення фінансових транзакцій потерпілими. Крім того, учасники злочинної організації контролювали систему функціонування так званих «дропів», які з метою подальшого виведення коштів, здобутих протиправним шляхом, створили оголошення (ордери) щодо купівлі криптовалюти шляхом p2p-транзакцій у спеціалізованому криптоботі в месенджері «Т» під назвою «С». Від протиправних дій злочинної організації 13 потерпілим завдано
шкоди на загальну суму близько 1,8 млн грн. Накладено арешт на майно фігурантів на суму 2 млн грн.

Список літератури:

Амелін О. Визначення кіберзлочинів у національному законодавстві. Науковий часопис Національної академії прокуратури України. 2016. № 3. С. 1–10

Юртаєва К. В. Визначення місця вчинення злочинів з використанням комп'ютерних технологій. Форум права. 2009. № 2. С. 434–441.

Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку. http://www.scourt.gov.ua/clients/vsu/vsu.nsf/(print)/AFB1E90622E4446FC2257B7C00499C02

Про судову експертизу : Закон України від 25 лют. 1994 р. № 4038-XII. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/4038-12.

Парфило О. А. Актуальні питання судово-експертного дослідження шкідливих програмних засобів у межах протидії кібертероризму. Криміналістичний вісник. 2016. № 1 (25). С. 78–84.

Волков О.О. Поняття шкідливого програмного засобу призначеного для несанкціонованого втручання в роботу електронно-обчислювальної техніки. *Науковий вісник Національної академії внутрішніх справ. 2018. № 1 (106). С. 217.231.*