ПРОБЛЕМИ ЗАСТОСУВАННЯ ОКРЕМИХ СТАТЕЙ КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ В КОНТЕКСТІ ХАКТИВІСТСЬКОЇ ДІЯЛЬНОСТІ

Протягом останніх 4-х років спостерігався помітне зростання ролі волонтерських та громадських структур, які допомагали державі в різних аспектах національної безпеки. Ця допомога набула особливого значення в перші роки конфлікту на сході України із російсько-терористичними військами.

Не стала виключенням і кіберсфера. Проукраїнські хактивісти (зокрема, «Українські кібер війська», «Кіберсотня», «FalconsFlame», «Trinity», «RUH8» та інші) здійснювали:

- злами комп'ютерних систем як терористів, так і їх російських кураторів;
- отримували доступ до поштових скриньок осіб, які задіяні в організації та реалізації російської агресії проти України;
- відслідковували аккаунти в соціальних мережах та мережі інтернет через які терористичні угрупування вели свою агітацію та збирали кошти;
- блокували окремі електронні гаманці фінансистів терористів;
- допомагали у ідентифікації осіб, які приймають участь у збройному протистоянні на сході України проти сил АТО та багато іншого.

Вочевидь для класифікації їх діяльності найбільш доцільно використовувати концепцію кольорових «капелюхів» (hat)[1], що вже стала звичною практикою при характеристиці дій хакерських (чи просто IT-експертних) угрупувань. «Білі капелюхи» (White hat) зазвичай є повністю легальними IT-фахівцями, що здійснюють свою діяльність законно і частіше за все – на комерційній основі. Основна їх мета – вдосконалення систем кібербезпеки тих чи інших структур (державних чи приватних), в тому числі

[1] Традиція поділяти хакерів за капелюхами походить з жанру американського кіно вестерну, де позитивні герої традиційно носили білі шляпи, в той час як злодії та негативні персонажі – чорні.

через пошук недоліків коду тих інформаційних систем, які використовують ці структури. Основний інструмент – пентест[2]. Важливим є те, що ці дії вони застосовують на запит самої організації та за чіткою попередньою домовленістю з нею.

Іншим полюсом є «чорні капелюхи» (Black hat), які більшою мірою є традиційними кіберзлочинцями, що здійснюють свою діяльність заради особистого зиску використовуючи будь-які методи зламу. Водночас послугами таких груп все частіше користуються військові та розвідувальні структури задля досягнення своїх військово-політичних цілей, але мінімізуючи при цьому юридичні наслідки від такого втручання (неможливості визнання відповідальності держав за такі атаки). В таких випадках «чорні капелюхи» виступають як своєрідні «проксі-групи», аналогічні за своєю суттю до різноманітних форм найманців, що здійснюють свою діяльність проти України з територій «ДНР/ЛНР».

Водночас українські хактивісти швидше підпадають під третю класифікаційну групу – «сірих капелюхів» (Grey hat). До них відносяться хакери чи фахівці з комп'ютерної безпеки, які почасти порушують законодавство чи типові етичні норми, але не здійснюють деструктивного впливу на зламану систему, що є типовим для «чорних шляп». Така характеристика проукраїнських хакерських груп меншою мірою стосується їх діяльності проти інформаційних ресурсів «ДНР» та «ЛНР», а також російських інформаційних ресурсів, щодо яких вони діють саме як «чорні шляпи».

Останнім часом їх безпосередня активність все частіше спрямовується на внутрішні інформаційні системи (передусім – державних органів та об'єктів критичної інфраструктури) щодо яких вони проводять несанкціоновані пентести, скачуючи при цьому окремі документи (які не мають грифів обмеження доступу) для підтвердження наявності уразливості.

[2] Пентест (penetration test, pentest) - оцінювання захищеності комп'ютерної системи чи мережі шляхом часткового моделювання дій зовнішніх зловмисників з проникнення у неї

Незважаючи на те, що ці дії здійснюються ними в інтересах забезпечення більшої кібербезпеки держави в умовах агресії (принаймні така мета ними публічно декларується), але відповідно до чинного законодавства вони частіше за все є порушенням українського законодавства.

Показовим в цьому сенсі був випадок із українським програмістом О. Моховим, який у 2013 році помітив уразливість в системі «Приват-24»[3], та здійснивши декілька тестів уразливості звернувся до Служби безпеки Приват-банку. Однак фактично експлуатація цієї уразливості можна було кваліфікувати як порушення законодавства (про що і заявила тоді прес-служба банку[4]), в т.ч. – статті 361 КК України. В подальшому ситуація була вирішена, однак при цьому принципова проблема не зникла.

Ще більш виразно проблема своєрідної «негнучкості» українського законодавства щодо діяльності у кіберпросторі проявилась у історії навколо акції[5] (флешмобу) «Ukrainian Cyber Alliance» під загальним хештегом #F*ckResponsibleDisclosure[6] який розпочався у листопаді 2017 року. За словами організаторів його мета - «*громадська акція для підвищеня рівня IT-гігієни*» (за суттю акція є формою краудсорсингового пентесту державних інформаційних систем). В межах «флешмобу» були знайдені уразливості в комп'ютерних системах щонайменше 10 ЦОВВ (в т.ч. – правоохоронних органів), декількох облрад, мінімум 5 об'єктів, які можна віднести до критичної інфраструктури держави, низки наукових та комунальних закладів.

Щонайменше одна з атакованих структур звернулась до поліції[7] із заявою щодо незаконного вторгнення в локальну комп'ютерну мережу облради.

---

[3] http://kpishnik.com/mohov-privat24/
[4] https://habrahabr.ru/post/193204/
[5] https://petrimazepa.com/disclosure.html
[6] Responsible Disclosure – форма пошуку уразливостей інформаційних систем, за якою першою про її наявність повідомляється власник системи (для того, щоб він міг її виправити) і лише з певним часовим проміжком про цю уразливість повідомляють громадськості. Концепція «Full disclosure» не передбачає паузи для інформування власника системи. Більш докладно про сутність поняття «Responsible Disclosure» та небажання авторів флешмобу його дотримуватись - у матеріалі за посиланням «https://www.facebook.com/vstyran/posts/10155958884177372»
[7] За даними офіційного повідомлення на сайті установи

Слід визнати, що з погляду чинного законодавства дії «Ukrainian Cyber Alliance» дійсно порушують тією чи іншою мірою статтю 361 Кримінального Кодексу України: «*несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку*»[8]. Фактично згадана стаття розглядає будь-яке втручання (в т.ч. те, яке не нанесло безпосередньої шкоди) до автоматизованої системі чи комп'ютерної мережі як злочин, адже внаслідок дій «Ukrainian Cyber Alliance» відбувся витік інформації. Формулювання зазначеної статті КК фактично унеможливлює діяльність некомерційних пентестерів, якщо ці тести заздалегідь не погоджені із об'єктами атаки.

Вочевидь діяльність груп на кшталт «Ukrainian Cyber Alliance» із виявлення вразливостей в інформаційних системах (в т.ч. – органів державної влади) є важливою і цілком підпадає під сутнісні ознаки державно-приватного партнерства, однак потребує свого повноцінного законодавчого вирішення. Передусім - задля виведення таких хактивістів з під дії статей КК України та здійснення їх діяльності у легальний спосіб, який би не наносив шкоду державним ресурсам і не створював передумови для застосування правоохоронними органами статті 361.

Одним з варіантів вирішення проблеми є уточнення статті 361 додатковим пунктом 3, у спосіб, яким сформульовано статтю 111 КК «Державна зрада», в якій вказано, що «*звільняється від кримінальної відповідальності громадянин України, якщо він на виконання злочинного завдання іноземної держави, іноземної організації або їх представників ніяких дій не вчинив і добровільно заявив органам державної влади про свій зв'язок з ними та про отримане завдання*». Таким чином мова йде про форму попередження відповідальних органів державної влади, про дії, які можуть бути трактовані як злочин у відповідності до положень статті КК.

[8] http://zakon3.rada.gov.ua/laws/show/2341-14/print

Крім того, слід визнати, що діяльність «Ukrainian Cyber Alliance» та схожих на них хактивістів (які відрізняються від комерційних пентестерів які узгоджують свої дії із структурою, щодо якої проводиться пентест), вочевидь частково підпадає під формулювання «*негласна перевірка готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів*», що відповідно до Закону України «Про основні засади забезпечення кібербезпеки України»[9] покладено на Службу безпеки України. При цьому стаття 361 КК України підвідомча Національній поліції, відтак дії таких хактивістів мають бути узгоджені як з Національною поліцією (профільним департаментом), так і зі Службою безпеки України.

Важливо відмітити, що «*негласна перевірка…*» є складовою оперативно-розшукової діяльності, яка у Законі України «Про оперативно-розшукову діяльність» визначена як «*система гласних і негласних пошукових, розвідувальних та контррозвідувальних заходів, що здійснюються із застосуванням оперативних та оперативно-технічних засобів*», а відповідно до українського законодавства і Служба безпеки України, і Національна поліція України є суб'єктами проведення оперативно-розшукової діяльності.

Неоднозначним видається і пошук практичного механізму співпраці – швидше за все, це актуалізує принаймні ще дві проблеми, які стануть фоном для дискусії з цього приводу.

По-перше – сам механізм та необхідність активістів узгоджувати свої дії із правоохоронними/контр розвідувальними структурами можуть стати питанням складних перемовин. Не у всіх випадках неурядові структури бажають узгоджувати свої дії із правоохоронними/контррозвідувальними органами, часто вбачаючи в цьому обмеження своїх прав та можливостей, а також незалежності дій. Крім того, публічне артикулювання фактів такого співробітництва може мати негативні іміджеві наслідки для таких структур. Відтак пошук практичного механізму співпраці має базуватись на

[9] http://zakon3.rada.gov.ua/laws/show/2163-19/print

гарантуванні нерозголошення інформації про таку співпрацю та мінімально необхідних бюрократичних процедурах для ініціювання перевірки.

По-друге – вирішення проблеми з врахуванням результатів такого тестування для безпосереднього поліпшення кібербезпеки протестованих структур. Останнє особливо важливо для хактивістів, оскільки одна з основних їх претензій та обґрунтувань формату проведення «флешмобу» полягала у системному ігноруванні установами інформації про уразливості в інформаційній системі тієї чи іншої державної структури, які надавались хактивістами.

Важливо відмітити ще один аспект: відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» суб'єкти кібербезпеки реалізують свої повноваження передусім щодо об'єктів критичної інфраструктури. Сайти ж органів державної влади, їх внутрішні комп'ютерні мережі швидше за все не підпадуть під ознаки об'єктів критичної інфраструктури. Відтак потрібно або уточнити положення зазначеного Закону, або ж передбачити можливість використання механізму співпраці з активістами і для цієї сфери в інших законах України.

ВИСНОВКИ

1. Участь волонтерських та неурядових структур у протидії агресії РФ шляхом атак на комп'ютерні системи і російсько-терористичних, а також проти комп'ютерних систем на території РФ дійсно надало важливу допомогу у протидії російській агресії та допомогло зробити публічними докази активної включеності РФ в конфлікт на сході України.

2. Українські активістські групи більшою мірою діють проти комп'ютерних систем РФ як «чорні капелюхи», в той час як їх дії проти українських комп'ютерних мереж (у вигляді несанкціонованого пентесту) більше характерні для «сірих капелюхів».

3. В межах чинного законодавства, така діяльність має протизаконний характер і може бути кваліфікована у відповідності до ст.361 КК України. Ця

проблема з'являлась і до російської агресії 2014 року, але була особливо актуалізована після неї. Без юридичного вирішення цієї проблеми буде істотно ускладнено ефективне державно-приватне партнерство, зважаючи на те, що до діяльності таких активістських груп залучено чимало висококласних та високомотивованих ІТ-фахівців.

4. Акція «Ukrainian Cyber Alliance» з листопада по грудень 2017 року найбільш рельєфно проявила цю проблему і обумовлює необхідність швидкого пошуку її рішення. Найбільш доцільним вбачається уточнення положень ст.361 КК України для створення чіткого механізму який би вивів дії таких хактивістів з під дії КК.

РЕКОМЕНДАЦІЇ

суб'єктам національної системи кібербезпеки

1. Для вирішення актуальних питань державно-приватного партнерства в сфері кібербезпеки важливим є ініціювання дискусії щодо модифікації українського законодавства (в т.ч. – Кримінального кодексу України) для легалізації пентестової діяльності хактивстів в інтересах перевірки готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів. З цією метою пропонується уточнити формулювання статті 361 КК України, доповнивши її новим пунктом у наступній редакції: «*звільняється від кримінальної відповідальності громадянин України, якщо таке втручання здійснювалось за погодженням із суб'єктами національної системи кібербезпеки, що мають право на здійснення оперативно-розшукової діяльності*».

2. Важливим є напрацювання реального механізму згаданого погодження, зробивши його максимально дебюрократизованим та із гарантуванням нерозголошення інформації про таку співпрацю. Вбачається доцільним утворення на базі Національного координаційного центру кібербезпеки постійно діючої робочої групи з особливих питань державно-приватного партнерства у складі працівників Служби безпеки України,

Департаменту кіберполіції Національної поліції України та Державної служби спеціального зв’язку та захисту інформації

3. Для функціонування групи має буде сформовано окреме положення, в якому чітко визначити механізм надання дозволу на здійснення пентесту систем, а також граничні показники такого пентесту, за межами якого на заявника більше не буде поширюватись дозвіл. Крім того, це ж положення має чітко регламентувати і вичерпні причини, чому такий дозвіл може не бути надано з боку суб’єктів національної системи кібербезпеки. Розробку відповідного положення доцільно проводити спільно із представниками українського ІТ-співтовариства, передусім тими, які спеціалізуються на комерційному здійсненні пентестів.

4. Передбачити, що робота таких пентестових груп може здійснюватись виключно за принципом «Responsible disclosure», де суб’єктом отримання відомостей є саме правоохоронні/контррозвідувальні органи. В межах роботи такої Групи передбачити чіткий механізм донесення результатів такої перевірки до тих відомств, які були піддані негласному пентесту, а також контролю за їх усуненням.

5. Розглянути можливість проведення Центром щонайменше одного засідання на рік присвяченого питанням стану реалізації державно-приватного партнерства (можливо – із залученням представників недержавного сектору).

Дубов Д.В.
Відділ інформаційної безпеки та
розвитку інформаційного суспільства
Національного інституту стратегічних досліджень