2.5. ЦИФРОВІЗАЦІЯ ОСВІТИ

ВЕРБУВАННЯ ПІДЛІТКІВ РОСІЙСЬКИМИ СПЕЦСЛУЖБАМИ ДЛЯ ВЧИНЕННЯ ПРОТИПРАВНИХ ДІЙ: СТАН ПРОБЛЕМИ ТА ШЛЯХИ ПРОТИДІЇ

Світлана ЄФІМЕНКО,

старший викладач кафедри інформаційно-комунікаційних технологій та безпечного освітнього середовища комунального закладу «Кіровоградський обласний інститут післядипломної педагогічної освіти імені Василя Сухомлинського», кандидат педагогічних наук

В умовах повномасштабної війни російські спецслужби активно використовують кіберпростір для вербування українських громадян, зокрема неповнолітніх, з метою вчинення диверсій, терактів та інших протиправних дій. Наслідки таких дій становлять серйозну загрозу національній безпеці нашої країни. І це на сьогодні є надзвичайно актуальною проблемою.

Так, відповідно до досліджень інформаційного ресурсу Dovidka.Info, від початку повномасштабного вторгнення Служба безпеки України (далі – СБУ) зафіксувала понад 600 випадків, коли українців намагалися втягнути в диверсійні дії, 22% завербованих – неповнолітні. Зокрема, в Івано-Франківську група 15-17 річних підлітків на замовлення російських спецслужб готувала серію терактів у місті, унаслідок чого один з них загинув під час транспортування вибухового пристрою, ще одного – госпіталізовано з тяжкими пораненнями. У Києві було затримано 16-річного хлопця за підпал трьох відділень Укрпошти. У Тернополі 14-річна дівчина вчинила теракт біля відділку поліції за допомогою виготовленої власноруч вибухівки, була затримана на місці злочину під час спроби виконати останній етап свого завдання. У Миколаєві було затримано чотирьох підлітків за підготовку теракту в центрі міста, що призвів до загибелі військових. На Черкащині викрито шістьох неповнолітніх підпалювачів релейних шаф Укрзалізниці, які навчалися в одній школі міста Сміли. На Харківщині 15-річний агент загинув після підриву вибухівки біля військової частини Національної гвардії. У Харкові було викрито групу з 15-16-річних осіб, які виконували ворожі завдання із проведення розвідки, передачі координат розташування українських військових та об'єктів критичної інфраструктури, коригування ударів. Окрім цього, в низці міст різних регіонів нашої держави СБУ викривала групи неповнолітніх, які за завданням російських спецслужб здійснювали підпали автівок військових, надсилали анонімні повідомлення про псевдомінування будівель органів державної влади й об’єктів соціальної інфраструктури, вчиняли диверсії на об'єктах соціальної інфраструктури та в місцях дислокації українських військових.

Для вербування українських підлітків російські спецслужби вдаються до різноманітних хитрощів. Один зі шляхів пошуку потенційних виконавців – приватне листування в месенджерах чи соцмережах. Для цього представники російських спецслужб можуть створювати фейкові облікові записи, де видають себе за однолітків, що нібито нещодавно переїхали й шукають друзів та інформацію про населений пункт, включаючи наявність стратегічних об'єктів поблизу «нового місця проживання». Також інформацію військового значення можуть випитувати за допомогою зламаних акаунтів знайомих або родичів, які є військовослужбовцями. До того ж підлітків можуть примушувати, залякувати, шантажувати або спокушати «легким» заробітком, пропонуючи їм виконати спеціальні доручення. Окрім приватного листування, російські спецслужби використовують месенджери (переважно Telegram) та чати ігрових платформ для створення фейкових акаунтів, груп та каналів, що імітують проукраїнські, патріотичні або ігрові спільноти, у яких відбувається неочевидний для учасника спільноти збір стратегічно важливої інформації. Крім такого неочевидного використання, вербування в окремих приватних телеграм-каналах є досить відкритим. Суть цього вербування часто імітує квест, де послідовні завдання для залучених шукачів «легких грошей» поступово ускладнюються: від малювання графіті до створення вибухових пристроїв та вчинення диверсій. Стаття Texty.org.ua «П'ять тисяч доларів за спалення ТЦК. Як російські спецслужби вербують потенційних терористів» наочно ілюструє ці схеми. Журналісти, імітуючи потенційних виконавців, поспілкувались із «рекрутерами» російських спецслужб у приватному телеграм-каналі. Їхнє розслідування почалося зі знайденого графіті з посиланням на цей телеграм-канал, який виявився пропагандистським ресурсом, що підбурював до насильства проти представників ТЦК та української влади. У цьому каналі відкрито публікувався «прайс-лист» на різні акції саботажу та терору. Виявилося, що вербувальники діють за принципами мережевого маркетингу: вони пропонують заповнити анкету, проводять онлайн-співбесіди, з'ясовують рівень готовності учасників, а потім пропонують «стажування», починаючи з таких простих завдань, як розклеювання листівок або виготовлення трафаретів для графіті. У міру «кар'єрного зростання» рівень цих завдань ускладнюється до участі в диверсіях і терористичних актах.

На перших етапах у ланцюжку послідовних дій під час виконання завдань нижчого рівня складності виконавці, дійсно, отримують заробіток. У міру зростання рівня складності й небезпеки спеціального доручення рівень заробітку також зростає. Коли виконавець морально готовий, своїми попередніми діями довів замовникам, що він надійний, а замовники – що вони платоспроможні, наступає завершальний етап – виготовлення за відеоінструкцією вибухівки, диверсія, терористичний акт. Але, на завершальному етапі виконання завдання, за яке пропонують досить великі суми оплати (до кількох тисяч доларів), на виконавця чекає неочікуваний для нього фінал – смерть від вибуху виготовленої

ним же вибухівки, оскільки російські спецслужби дистанційно підривають своїх агентів, позбуваючись їх як зайвих свідків. Є ще один небезпечний та підступний елемент ланцюжка дій в межах виконання спеціальних доручень – використання «в темну» осіб, зокрема неповнолітніх, для перенесення у визначене місце замаскованої вибухівки. СБУ застерігає: «Якщо вам або вашим знайомим пропонують «просто занести пакунок» до ТЦК, поліції чи іншої адмінбудівлі, знайте – вас хочуть вбити».

Чому підлітки потрапляють під вплив російських вербувальників? Ключовим мотиватором вербування є гроші (обіцянки великих грошей за прості дії є дуже привабливими для підлітків, які не усвідомлюють прихованих ризиків та реальної ціни такої «праці»). Проте підлітки можуть вступати в небезпечну онлайн-взаємодію з російськими спецслужбами та погоджуватися на виконання їхніх доручень з багатьох інших причин. Серед них:

- страх (вербувальники часто використовують психологічний тиск, маніпуляції, погрози, залякування та шантаж, аби змусити підлітка співпрацювати, особливо якщо він вже виконав якісь «пробні» завдання і боїться викриття);
- жага до пригод та «гри» (деякі підлітки сприймають ці завдання як небезпечний квест або гру, де можна «перевірити себе» і побачити, «що буде далі», не усвідомлюючи наслідків);
- відсутність патріотичних почуттів та проросійські настрої (вплив російської пропаганди, відсутність міцної проукраїнської ідентичності або навіть прямі проросійські погляди можуть підштовхувати підлітків до співпраці);
- бажання діяти внаслідок ідейної обробки (підлітків можуть вербувати на ідейній основі, використовуючи наративи про «справедливість», «боротьбу з несправедливістю» або «допомогу» певним силам, маніпулюючи їхніми почуттями та незрілістю критичного мислення);
- впевненість в уникненні покарання (неповнолітні часто недооцінюють серйозність своїх дій і вірять, що їх не спіймають, або що через вік вони уникнуть відповідальності, зокрема кримінальної);
- соціальна ізоляція та пошук визнання (деякі підлітки, які почуваються самотніми або не знаходять розуміння у своєму оточенні, мають проблеми в сім'ї чи школі й прагнуть до самоствердження, можуть шукати уваги та відчуття приналежності у спільнотах, створених вербувальниками);
- психологічна вразливість (підлітковий вік, перехідний період, несформована психіка та імпульсивність сприяють схильності неповнолітніх до маніпуляцій та ризикованої поведінки);
- недостатня поінформованість (підлітки можуть не розуміти, що навіть, на перший погляд, несуттєві дії, такі як розклеювання листівок або

фотографування об'єктів, можуть бути частиною диверсійної діяльності та кваліфікуватися як тяжкі злочини).

Наслідками для неповнолітнього виконавця спеціальних завдань в межах вербування є або смерть (від дистанційного підриву вибухівки російськими спецслужбами) або (якщо він залишиться живим) кримінальна відповідальність, що зруйнує його майбутнє та створить проблеми для його сім'ї. Так, відповідно до Кримінального кодексу України, кримінальними правопорушеннями, відповідальність за які наступає з 14-річного віку, є: диверсія (ст. 113 КК), терористичний акт (ст. 258 КК), хуліганство (ст. 296 КК). Кримінальні правопорушення, відповідальність за які наступає з 16-річного віку: колабораційна діяльність (ст. 111^1 КК), пособництво державі-агресору (ст.111^2 КК); несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення ЗСУ чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану (ст. 114^2 КК). До того ж, за ст. 114^2 КК передбачено кримінальну відповідальність за розповсюдження інформації про переміщення, розташування та рух ЗСУ, якщо ця інформація не була опублікована у відкритому доступі. Це може бути стрім, селфі, сторіс, фото чи відео, які містять таку інформацію. Таким чином, неповнолітній інтернет-користувач може допомогти російським військовим, навіть, ненавмисне (наприклад, знявши для TikTok відео про переміщення української військової техніки) і понести за це кримінальну відповідальність.

Розглянемо основні шляхи протидії вербуванню підлітків російськими спецслужбами для вчинення протиправних дій.

Батьківський контроль та відкритість у спілкуванні між членами сім'ї:

- налагодження довірливих стосунків, подолання бар'єрів страху, які можуть стати на заваді дитині зізнатись батькам у підозрілих пропозиціях в інтернет-мережі;
- обговорення ризиків, пояснення дітям небезпеки онлайн-спілкування з незнайомцями, аналіз способів вербування та наслідків злочинних дій, безпечні способи заробітку;
- розвиток навичок відмови (зокрема, пропрацювання фраз, які допоможуть дитині вийти з ризикованої ситуації «Ні, це незаконно», «Я розповім батькам», «Дайте мені спокій» тощо);
- моніторинг активності дитини в інтернеті, зокрема засобами встановленого батьківського контролю на пристроях дитини (наприклад, Google Family Link, Qustodio, Bark), періодичною перевіркою сайтів, які відвідує дитина (за допомогою вкладки «Історія» в браузері) та бесідами про те, з ким і де спілкуються діти (важливо робити це не як контроль, а як турботу про безпеку);
- допомога дитині у встановленні налаштувань приватності та безпеки в облікових записах;

- увага до раптових змін у поведінці дитини та її настрої (наприклад, у дитини з'являються гроші з невідомих джерел, дитина стає замкнутою й агресивною, уникає розмов із рідними, має таємні листування чи розмови по телефону, що супроводжуються підвищеною прихованістю, раптово цікавиться темами армії, політики, об'єктів критичної інфраструктури, регулярно зникає без пояснень, повертається пізно, купує незвичні набори хімікатів, електроніки тощо).

Батькам важливо усвідомлювати, що пильність і відкрите спілкування з дітьми – головна передумова для запобігання їхньому вербуванню.

Освітня та інформаційна робота:

- проведення педагогами у співпраці з психологами та представниками правоохоронних органів (зокрема, офіцером Служби освітньої безпеки) уроків, лекцій, тренінгів, бесід для здобувачів освіти з кібербезпеки, медіаграмотності та правової свідомості, наслідків протиправних дій, механізмів захисту від вербування;
- розвиток у здобувачів освіти патріотичних почуттів, формування ціннісних орієнтирів, національної свідомості;
- налагодження партнерських, довірливих взаємин зі здобувачами освіти (для окремих учнів саме педагог може бути тією людиною, якій вони наважаться зізнатись у тому, що їх намагаються завербувати чи вже завербували);
- спостереження за психологічним станом здобувачів освіти, їхньою поведінкою, змістом розмов та раптовою появою інтересів, які можуть вказувати на залученість дитини до протиправних дій;
- інформування освітянами батьків здобувачів освіти про ризики та можливі ознаки співпраці їхніх дітей з ворожими спецслужбами, способи протидії цьому.

Наразі в межах державної політики щодо протидії вербуванню населення України розроблено низку навчально-методичних матеріалів для освітян, здобувачів освіти та їхніх батьків. Так, командою інформаційно-освітньої кампанії #stop_sextинг (https://stop-sexting.in.ua/) створено кейс освітніх ресурсів, який включає цикл уроків «(Не)безпека в час війни» для різних вікових груп здобувачів освіти, спеціальні брошури й посібники для педагогів, здобувачів освіти та їхніх батьків («Цифрове середовище та воєнні злочини. Діти», «Протидія залучення дітей російськими військовими до протиправної діяльності через інтернет», «Онлайн злочини за участю дітей під час війни» та інші), вебінар «Протидія вербуванню дітей до протиправної діяльності: інструменти для освітян». На вебсторінці «Нова Українська школа» (https://nus.org.ua/) розміщено інформативну статтю «Як росія вербує підлітків для злочинів і як цьому протидіяти», у якій окреслено проблему вербування з юридичного, психологічного та журналістського погляду. На сайті Міністерства освіти і науки

України (далі – МОН) опубліковано національний онлайн-урок для підлітків від МОН, Нацполіції та СБУ «Легкі гроші – смертельні наслідки. Як не потрапити у пастку російських спецслужб» для інформування здобувачів освіти та запобігання випадкам вербування, а також рекомендації «Як розпізнати ознаки вербування дитини? Рекомендації батькам і освітянам». На сайті СБУ оприлюднено поради «Як діяти, якщо вас вербують». СБУ разом із проєктом Dovidka.info Центру стратегічних комунікацій та інформаційної безпеки створили короткий відеоролик «Це не робота. Смертельна пастка», щоб застерегти українців від «легких підробітків», за якими ховається смертельна небезпека. У відео показано реальні методи, які застосовують російські спецслужби, після чого дистанційно підривають виконавця, знищуючи і його, і докази. Телеканали СК1 та Рада, Медіагрупи «Накипіло» й «Ми – Україна» створили просвітницькі відеоматеріали з історіями завербованих підлітків: «Вербування підлітків України: яка відповідальність загрожує за злочини, вчинені на замовлення ворога», «Як російські спецслужби вербують українських підлітків для диверсій», «Розслідування вражає! Історії завербованих підлітків, яких повернули на шлях істини», «Вербування підлітків, воєнні злочини рф і новий закон про захист дітей | Олена Кондратюк». Інформаційний ресурс Dovidka.Info підготував змістовні рекомендації для батьків та освітян щодо запобігання випадкам вербування, інструкції з налаштувань безпеки та конфіденційності облікових записів підлітків, перелік безпечних способів заробітку для підлітків. Також для впровадження в освітній процес нами розроблено два авторські вебквести (автори Єфіменко С.М., Токарь В.В.): «Інформаційна безпека в умовах воєнного стану», «Мінна безпека», у яких частина завдань полягає у вирішенні гравцями проблемних ситуацій, пов'язаних з вербуванням.

На основі аналізу вищезазначених ресурсів систематизуємо головні правила, яких варто дотримуватися підліткам, щоб захистити себе від онлайн-вербування:

- захист облікових записів та налаштування конфіденційності: встановити двофакторну автентифікацію у всіх облікових записах (Google, Facebook, Instagram, TikTok, Telegram, Viber тощо); налаштувати приватність (хто може долучати до груп/спільнот/каналів, хто може надсилати повідомлення, хто може бачити активність онлайн, геолокацію, номер телефону, фото профілю та інші налаштування);
- критичне сприйняття інформації: аналізувати інформацію в інтернет-просторі, вміти розпізнавати маніпуляції та дезінформацію, критично ставитися до «легких» заробітків; не реагувати на заклики про допомогу від незнайомих акаунтів, оскільки це може бути пасткою; не переходити за підозрілими посиланнями від незнайомців та не сканувати невідомі QR-коди на

дошках оголошень/стінах/стовбах, оскільки вони можуть містити шкідливе програмне забезпечення або на телеграм-канали вербувальників;

- поширення інформації: ніколи й за жодних обставин не повідомляти приватну інформацію (номер свого телефону, номери телефонів батьків, місця навчання та проживання, місця роботи батьків тощо); не ділитись інформацією про ситуацію у населеному пункті, про родичів-військових, військові об'єкти чи розміщення військової техніки; пам'ятати про те, що навіть онлайн-друзі, яких підліток знаєте в реальному житті, можуть мати зламані профілі для збору інформаційних даних; не публікувати анонси чи прямі трансляції подій з великим скупченням людей (наприклад, у закладах освіти); не поширювати відео з напрямками польотів ракет; не публікувати фото/відео з українськими військовими, особливо якщо видно їхні шеврони, погони, пов'язки, знаки на техніці чи будь-які інші ідентифікатори; уникати селфі, на яких в кадр потрапляють військові ЗСУ чи стратегічні об'єкти; не вказувати точні координати та геолокацію місць, де тривають бойові дії, і не демонструвати роботу українських військових (ППО, артилерії, авіації); не вести прямих трансляцій (стрімів) з місць прильотів ракет, ворожих обстрілів, поблизу військових баз чи стратегічних об'єктів; не уточнювати інформацію про ці місця в коментарях, чатах чи обговореннях у соцмережах та месенджерах; не публікувати аудіо/відео матеріали про пересування військової техніки Збройних Сил України, місця їх дислокації, ночівлі та укриття тощо;
- реагування на підозрілі пропозиції, що може допомогти не тільки захиститись самому, а й викрити всю мережу вербувальників: не погоджуватись на пропозиції; зробити скриншот листування; заблокувати користувача-адресанта підозрілої пропозиції; вийти з чату/покинути канал; звернутись до батьків/педагога/психолога, зателефонувати за номером 102, звернутись до кіберполіції онлайн за посиланням https://ticket.cyberpolice.gov.ua/ або зателефонувати за номером 0 800 50 51 70, написати в чат-бот СБУ «Спали» ФСБешника» або зателефонувати на гарячу лінію: 0-800-501-482, повідомити інспектора ювенальної превенції або представника Служби освітньої безпеки, якщо такий є в закладі освіти.

Отже, в умовах воєнного стану, коли російські спецслужби активно полюють на українських підлітків в інтернеті, останнім надзвичайно важливо розуміти, як захистити себе, оскільки особиста онлайн-безпека є вагомим внеском у безпеку України. Загалом протидія вербуванню підлітків російськими спецслужбами вимагає комплексного підходу, що включає відповідальність батьків, освітні ініціативи, активну інформаційну роботу та ефективну діяльність правоохоронних органів. Тільки спільними зусиллями можна захистити молоде покоління від злочинних посягань ворога та зберегти наше майбутнє.