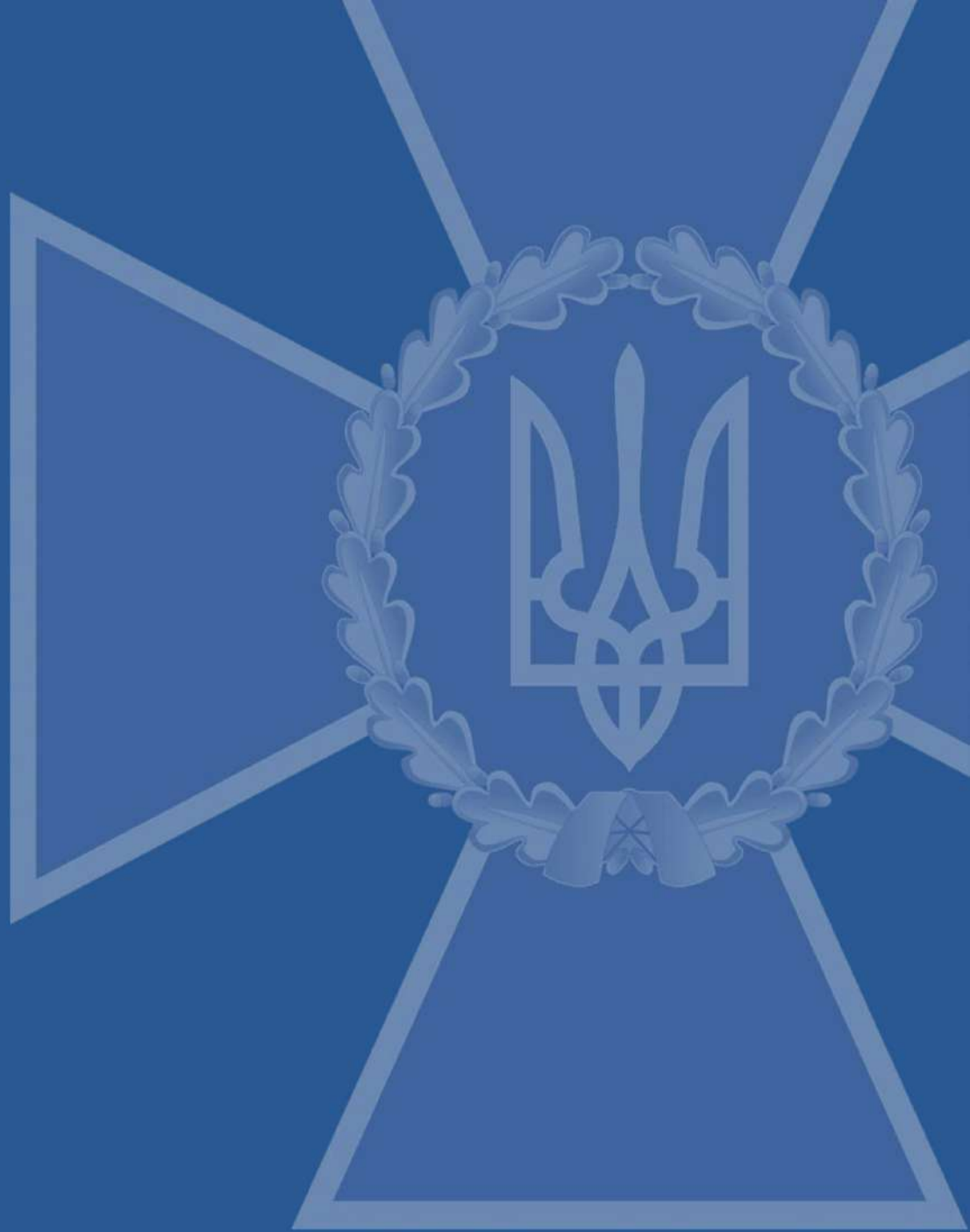


# БЕЗПЕКОВІ рекомендації:

**як не потрапити  
«на гачок» російських  
спецслужб в мережі  
Інтернет**



**ЗАХИЩАЄМО УКРАЇНУ РАЗОМ!**



# Чому дітям слід остерігатися ворожих спецслужб? ДОСВІД СБУ З ПРОТИДІЇ РОЗВІДЦІ РФ



## ОСТЕРІГАЙТЕСЯ СПРОБ ВЕРБУВАННЯ СПЕЦСЛУЖБАМИ ВОРОГА



З перших днів повномасштабного збройного вторгнення росіян в Україну інтенсивність ворожого натиску на український кіберпростір зросла у рази і продовжує залишатися на вкрай високому рівні.

Не маючи можливості перемогти на полі бою, ворог намагається посіяти «зраду» та розхитати українське суспільство у тилу, проводити розвідувальну діяльність, влаштовувати провокації, а також не знаючи правил та моральних бар'єрів, активно використовувати у своїй злочинній діяльності учнів та студентів навчальних закладів для проведення підривної діяльності проти нашої держави.

# Використання дітей ворожими спецслужбами ДО ЯКИХ МЕТОДІВ ВДАЄТЬСЯ ВОРОГ



Фейкові  
замінування



Фіксація  
пересування  
військ



Фото критичної  
інфраструктур  
и



Використання  
смартфон-ігор у  
власних цілях



Виведення з ладу  
критично  
важливих  
магістралей



Розвідка  
військових  
позицій



## Використання смартфон-ігор для вербування дітей ДО ЯКИХ МЕТОДІВ ВДАЄТЬСЯ ВОРОГ

### ВИЯВЛЕНО

Російські спецслужби для того, щоб залучити дітей до підривної діяльності, не рідко вдаються до хитрощів та використовують мобільні додатки, через які у користувачів в ігровій формі виманювали геолокацію та реальні фото стратегічних об'єктів.



### ВИКРИТО

Щоб залучити дітей до підривної діяльності, агресор використовував популярну ігрову програму для смартфонів. За її умовами учасники шукають так звані «коробки» із віртуальними призами, які можна обміняти на електронні гроші.

### ВИКРИТО

Під час проходження маршруту діти здійснюють фотофіксацію місцевості, у тому числі об'єктів військової та критичної інфраструктури на території різних населених пунктів. Усю інформацію з геолокацій учасники квесту завантажують у базу ігрового додатку.

## Використання дітей для розвідки позицій ЗСУ ДО ЯКИХ МЕТОДІВ ВДАЄТЬСЯ ВОРОГ І ДО ЧОГО МОЖЕ ПРИЗВЕСТИ



### ВИЯВЛЕНО

У Харкові окупанти встановили контакт з неповнолітнім хлопцем через Telegram-месенджер. Рашисти обіцяли заплатити гроші за інформацію про позиції ЗСУ на території міста.

Тим часом на Луганщині двоє російських солдат діяли не через месенджер, а напямучу - запропонували 16-ти річному підлітку гроші в обмін на інформацію про місця розташування та маршрути пересування українських військ. Хлопець злякався, проте окупанти його «заспокоїли»: мовляв, ти малолітній, тобі нічого не буде.



В умовах війни, довірливість може призвести до трагедії. Адже окупанти можуть залучати вас до вчинення терактів, диверсій, корегування вогню та інших тяжких злочинів, здатних спричинити загибель багатьох людей.



### ПОПЕРЕДЖЕНО

Завдяки втручання українських силовиків, хлопці не встигли передати інформацію ворогу.

У зв'язку з відсутністю фінансової самостійності підлітків агресор використовує це у своїх цілях



## ЗАФІКСОВАНО

Підлітки отримують завдання на підпал релейної шафи сигнальної установки, через анонімні групи в соціальних мережах, за грошову винагороду.

З метою отримання грошової винагороди весь процес та його наслідки фіксуються на відео, що є обов'язковою умовою замовника.



## НАСЛІДКИ

- 1 Дестабілізація функціонування залізничного транспорту, яка унеможливить доставку вчасної допомоги ЗСУ
- 2 Подальші психологічні маніпуляції з боку ворога
- 3 Притягнення до відповідальності відповідно до чинного законодавства

## НАСЛІДКИ ДО ЯКИХ МОЖУТЬ ПРИЗВЕСТИ «ЛЕГКІ ГРОШІ»



В Тернопільській області станом на 2024 рік зафіксовано один випадок виведення з ладу релейних шаф. В результаті чого це призвело до дестабілізації функціонування залізничного транспорту

Під час проведення пошукових заходів затримано двох мешканців

Тернопільщини, які за завданням спецслужб рф, з метою отримання грошової винагороди здійснили підпал релейних шаф.



**Відповідно до ст. 113 ККУ за вчинення диверсії в умовах воєнного стану «паліям» тепер загрожує п'ятнадцять років або довічне позбавлення волі**

## ФЕЙКОВІ ЗАМІНУВАННЯ

Для здійснення фейкових замінувань країна-агресорка використовує у своїх цілях українських підлітків. Окупанти за допомогою забороненої в Україні соціальної мережі «Вконтакте», підконтрольних Телеграм-каналів та ігрових інтернет-платформах здійснюють вербування дітей.

На цих ресурсах представники спецслужб рф «знайомляться» з юними користувачами і пропонують їм співпрацю. Дуже часто для схилення дітей до підривної діяльності ворог застосовує методи шантажу та психологічних маніпуляцій, а також пропонує «легкі» гроші.



# Що не слід публікувати в мережі Інтернет

## Фото, відео падіння ракети

Окупанти можуть використовувати фото та відео місцевості, де впав снаряд для повторного нанесення удару

## Роботу української ППО

Це може дати ворогу чітку картину, звідки був запуск ракети ППО і нанести ракетний удар

## Заборона «стрімити» ракетні обстріли

Країна-агресор отримає інформацію про ефективність ракетного удару

## Озвучувати та уточнювати дані в коментарях

80% розвідінформації ворог отримує з відкритих джерел



## Відео з ракетами, що летять

Такими кадрами ви допоможете ворогу корегувати вогонь

## Переміщення військ ЗСУ

Будь-які дані про дії та переміщення українських військ та військові об'єкти може становити загрозу для життя наших захисників

## Фото, відео, геолокація військових частин, блокпостів

Цим ви допоможете скерувати ворожі обстріли

## Інша інформація, що може допомогти ворогу

Відео/фото з розпізнавальними знаками: таблички з назвами вулиць, станціями метро, автобусними зупинками, магазинами та супермаркетами, заводами й підприємствами, номери авто.

# НЕ ПРАЦЮЙТЕ КОРИГУВАЛЬНИКАМИ ВОГНЮ У ВОРОГА

ЯКЩО НЕ ХОЧЕТЕ ДОПОМАГАТИ ВОРОГУ ЗНИЩУВАТИ НАШІ МІСТА І СЕЛА ТОДІ:



Не називайте точні цілі і об'єкти враження у соцмережах, у публічних виступах та коментарях для ЗМІ.



Не варто заявляти, що в нас немає ППО на конкретній ділянці і вказувати географічні дані

- ✦ **Не треба говорити чи писати**  
Ракета влучила у школу №7.  
Доцільно заявити – ракета влучила у такому-то населеному пункті в житловий квартал
- ✦ **Не варто говорити** – ракетою цілились у вокзал але потрапили у лікарню, яка знаходиться за нею.
- ✦ **Не треба говорити** – ракета влучила у склад поряд з аеродромом. Бо прилетить друга, третя і вже точно влучить в аеродром.

## ЧОМУ ЦЕ ВАЖЛИВО

80% розвідінформації відпрацьовується з відкритих джерел. І такі повідомлення дозволять ворогу корегувати вогонь по ваших населених пунктах.



Не відповідайте на дописи незнайомців в соцмережах, які просять розповісти, яка ситуація в місті, або уточнюють адресу влучання снарядів – це можуть бути диверсанти.

Російські коригувальники також вдаються до нових тактик – пропонують безкоштовно допомогти з заміною вибитих шибок. «При цьому «добродій» може задавати безліч питань про ваш будинок та все що поруч». Це також може бути коригувальник ворога.

Якщо хтось із користувачів у мережі просить надати **приватну інформацію** (особистий номер телефону чи номер батьків, де батьки працюють, де родина зараз перебуває), інформацію про ситуацію в місті, про родичів-військових, де розміщується військова техніка в місті чи військові об'єкти тощо —

**ТАКУ ІНФОРМАЦІЮ В ЖОДНОМУ РАЗІ НЕ МОЖНА ПЕРЕДАВАТИ.**

Навіть якщо це онлайн-друг, якого ви знаєте в реальному житті.



Адже зараз дуже часто особисті профілі зламують для отримання інформації або створюють фейкові профілі.



## БЕЗПЕКОВІ РЕКОМЕНДАЦІЇ

Якщо вас автоматично додали до невідомих груп, **важливо відписатися від них і заблокувати їх, а також розповісти про це дорослим, яким ви довіряєте.**



Важливо ділитись з дорослими про те, що трапляється в мережі, особливо тоді, коли це викликає у вас неприємні передчуття чи ви не може одразу визначити, як вчинити.

## ЗАБОРОНЕНО

**Розміщувати в соцмережах та месенджерах світлини/відео** родичів які проходять військову службу, за допомогою яких їх можна ідентифікувати. Це може нашкодити вашим рідним, а також ворог може використати цю інформацію для шантажу та погроз.

## УВАГА

Слід **мінімізувати ризик кібератаки на пристрої, якими ви користується** (налаштувати приватність в соцмережі, встановити двофакторну аутентифікацію, не переходити за посиланням на незахищені електронні адреси, не відкривати файли з небезпечним розширенням, адже ці файли або посилання можуть мати небезпечний вміст).

## КУДИ ЗВЕРТАТИСЯ В РАЗІ ВИНИКНЕННЯ ПРОБЛЕМ?



**В разі надходження на мобільні месенджери, особисті акаунти соціальних мереж пропозицій, прохань, погроз від невідомих осіб, давніх друзів здійснених з метою спонукання до:**

- 1** Збору та надсилання даних про розташування (локацій, фото) об'єктів критичної інфраструктури (електропідстанції, мости, газорозподільні вузли тощо), військових частин, правоохоронних органів, органів державної влади, місцевого самоврядування;
- 2** Повідомлення про розміщення та пересування військової техніки;
- 3** Надсилання електронних повідомлень, здійснення телефонних дзвінків із погрозами вчинення вибуху, мінування, захоплення об'єктів;
- 4** Вчинення дій спрямованих на виведення з ладу критично важливих транспортних, електричних, газових магістралей;
- 5** Вчинення інших протиправних дій.

**Негайно ПОВІДОМЛЯЙТЕ класних керівників, адміністрацію навчального закладу, органи СБУ**



**СЛУЖБА  
БЕЗПЕКИ  
УКРАЇНИ**

**+38 (0352) 52-45-42  
+38 (0352) 52-90-00  
usbu\_ter@ssu.gov.ua**



СЛУЖБА БЕЗПЕКИ УКРАЇНИ

**ЗАХИЩАЄМО**

**УКРАЇНУ РАЗОМ!**