

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

**ІТ-ПРАВО
ПІД ЧАС ГІБРИДНОЇ ВІЙНИ:
ВІД ПОШУКУ ПАРАДИГМИ
ДО ПРАГМАТИЧНИХ РІШЕНЬ**

Колективна монографія

*За редакцією
Є. Харитонова, О. Харитонової, І. Давидової*

Одеса
Фенікс
2025

*Рекомендовано рішенням вченої ради
Національного університету «Одеська юридична академія»
(протокол № 9 від 30 червня 2025 р.)*

Рецензенти:

Майданик Р. А. – академік НАПрН України, доктор юридичних наук, професор, професор кафедри цивільного процесу Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка;

Соколов А. В. – доктор технічних наук, професор, професор кафедри кібербезпеки Національного університету «Одеська юридична академія»;

Маковій В. П. – кандидат юридичних наук, професор, завідувач кафедри цивільно-правових дисциплін Одеського державного університету внутрішніх справ.

I-87 **ІТ-право під час гібридної війни: від пошуку парадигми до практичних рішень** : кол. монографія / за заг. ред. проф.: Є. Харитонова, О. Харитонової, І. Давидової. – Одеса : Фенікс, 2025. – 588 с.
ISBN 978-617-8430-70-2

Монографія є продовженням циклу праць колективу кафедри цивільного права Національного університету «Одеська юридична академія», присвячених результатам досліджень цивілістичних шкіл університету від часу їхнього формування до гібридної війни, що триває нині. У третьому томі аналізуються в контексті гібридної війни: проблеми визначення концепту «ІТ-право», особливості правового регулювання відносин, що виникають у зв'язку з використанням інформаційних технологій, особливості механізму цивільно-правового регулювання у сфері ІТ, чинник симулякру, значення та роль інформаційного середовища як стратегічного ресурсу, правові рамки для цифрових активів і перспективи цифрової власності, ІТ-правочини, порушення прав інтелектуальної власності в Інтернет, протидія кіберзагрозам у гібридній кібервійні, загрози вербування неповнолітніх через соцмережі та месенджери та юридичні заходи запобігання таким загрозам, правове регулювання стартапів, е-кредитування, цивільно-правова відповідальність за шкоду, завдану кібератаками, забезпечення інформаційної безпеки електронного судочинства в умовах гібридної війни в Україні та ін.

Авторський колектив концентрував увагу на обґрунтуванні необхідності комплексного вирішення практичних питань впорядкування інформаційно-технологічні відносини в умовах гібридної російсько-української війни. Автори прагнули розкрити особливості правового регулювання цих відносин і запропонувати власне бачення шляхів вирішення проблем, що виникають у цій сфері. Усвідомлюючи спірність низки висновків і пропозицій, автори розраховують на продовження плідних дискусій з проблем правового регулювання інформаційних технологій, зокрема в умовах гібридної війни.

Монографія може бути цікавою науковцям, практикуючим юристам, викладачам, аспірантам, здобувачам вищої освіти, а також широкому загалу небайдужих українців, які цікавляться проблемами правового регулювання у сфері ІТ, зокрема під час гібридної війни.

УДК 340:004:327:355

ЗМІСТ

Авторський колектив	5
Розділ 1. Прагматична (соціологічна) школа «ІТ-права» – відповідь цивілістики на виклики інформаційного суспільства (Євген Харитонов, Олена Харитонova, Ірина Давидова)	7
Розділ 2. Концепт ІТ-права (Євген Харитонов, Олена Харитонova)	30
Розділ 3. Гібридна інформаційна війна та інформаційні технології (Євген Харитонов, Олена Харитонova)	65
Розділ 4. ШІ як бінарна категорія ІТ (Євген Харитонов, Олена Харитонova)	93
Розділ 5. Симулякр, гібридна (інформаційна) війна і потенціал ІТ (Євген Харитонов, Олена Харитонova)	119
Розділ 6. Інформаційне середовище як стратегічний ресурс у гібридних конфліктах (Оксана Калітенко)	143
Розділ 7. Правові рамки для цифрових активів: перспективи цифрової власності (Катерина Некіт)	175
Розділ 8. Захист немайнових прав у медіапросторі в період гібридної війни (Алла Кирилюк, Лариса Галупова)	203
Розділ 9. ІТ-правочини в умовах гібридної війни (Ірина Давидова)	250
Розділ 10. Порушення прав інтелектуальної власності в мережі інтернет під час гібридної агресії в умовах воєнного стану (Наталія Бааджи)	279
Розділ 11. Кіберзагрози у гібридній кібервійні: дія і протидія (Євген Харитонов, Олена Харитонova)	323
Розділ 12. Етико-юридичні аспекти використання штучного інтелекту в мережі інтернет в умовах гібридної війни (Олександр Омельчук)	351
Розділ 13. Застосування систем автоматизованого прийняття рішень під час збройного конфлікту (Віра Токарева)	378

Розділ 14. Гібридна війна і кіберзброя (Євген Харитонов, Олена Харитонova)	388
Розділ 15. Вербування неповнолітніх через соцмережі та месенджери в умовах гібридної війни: загрози, механізми та заходи запобігання (Вікторія Рябченко).	420
Розділ 16. Правове регулювання діяльності стартапів в умовах гібридної війни: виклики, можливості та перспективи (Дмитро Розумейко).	435
Розділ 17. Е-кредитування у період воєнного стану (Олена Берназ-Лукавецька)	453
Розділ 18. Цивільно-правова відповідальність за шкоду, завдану кібератаками (Богдан Фасій)	483
Розділ 19. Сімейні правовідносини в сфері інформаційних технологій в умовах гібридної війни (Оксана Сафончик)	514
Розділ 20. Забезпечення інформаційної безпеки електронного судочинства в умовах гібридної війни в Україні (Крістіна Дрогозюк)	545
Розділ 21. Кіберспортивна дипломатія: перспективи для України (Максим Ткалич, Юлія Толмачевська)	557
Список основних праць представників школи	565

Авторський колектив

Харитонов Євген (ORCID ID: 0000-0001-5521-0839), доктор юридичних наук, професор, член-кореспондент НАПрН України, зав. кафедри цивільного права НУ «ОЮА»: розділ 1 (у співав. з О. Харитоновою, І. Давидовою); розділ 2 (у співав. з О. Харитоновою); розділ 3 (у співав. з О. Харитоновою); розділ 4 (у співав. з О. Харитоновою); розділ 5 (у співав. з О. Харитоновою); розділ 11 (у співав. з О. Харитоновою); розділ 14 (у співав. з О. Харитоновою);

Харитонova Олена (ORCID ID: 0000-0002-9681-9605), докторка юридичних наук, професорка, членкиня-кореспондент НАПрН України, зав. кафедри права інтелектуальної власності і патентної юстиції НУ «ОЮА»: розділ 1 (у співав. з Є. Харитоновим, І. Давидовою); розділ 2 (у співав. з Є. Харитоновим); розділ 3 (у співав. з Є. Харитоновим); розділ 4 (у співав. з Є. Харитоновим); розділ 5 (у співав. з Є. Харитоновим); розділ 11 (у співав. з Є. Харитоновим); розділ 14 (у співав. з Є. Харитоновим);

Давидова Ірина (ORCID ID: 0000-0001-5622-671X), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 1 (у співав. з Є. Харитоновим, О. Харитоновою); розділ 9;

Некіт Катерина (ORCID ID: 0000-0002-3540-350X), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 7;

Сафончик Оксана (ORCID ID: 0000-0001-6781-8219), докторка юридичних наук, професорка, професорка кафедри цивільного права НУ «ОЮА»: розділ 19;

Бааджи Наталія (ORCID ID: 0000-0002-9889-4879), кандидатка юридичних наук, доцента, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 10;

Берназ-Лукавецька Олена (ORCID ID: 0000-0002-2133-1672), кандидатка юридичних наук, доцента, доцентка кафедри цивільного права НУ «ОЮА»: розділ 17;

Галупова Лариса (ORCID ID: 0000-0001-6263-2773), кандидатка юридичних наук, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 8 (у співав. з А. Кирилюк);

Дрогозюк Крістіна (ORCID ID: 0000-0001-9254-9575), кандидатка юридичних наук, доцента, доцентка кафедри цивільного, нотаріального та виконавчого процесу НУ «ОЮА»: розділ 20;

Калітенко Оксана (ORCID ID: 0000-0003-1001-3561), кандидатка юридичних наук, доцентка, професорка кафедри цивільного права НУ «ОЮА»: розділ 6;

Кирилюк Алла (ORCID ID: 0000-0002-3051-6599), кандидатка юридичних наук, доцентка, доцентка кафедри права інтелектуальної власності та патентної юстиції НУ «ОЮА»: розділ 8 (у співав. з Л. Галуповою);

Омельчук Олександр (ORCID ID: 0000-0002-0082-3619), кандидат юридичних наук, доцент, доцент кафедри цивільного права НУ «ОЮА»: розділ 12;

Ткалич Максим (ORCID ID: 0000-0003-4224-7231), кандидат юридичних наук, доцент, доцент кафедри цивільного права Запорізького національного університету: розділ 21 (у співав. з Ю. Толмачевською);

Токарева Віра (ORCID ID: 0000-0002-8409-1477), кандидатка юридичних наук, доцентка, доцентка кафедри цивільного права НУ «ОЮА»: розділ 13;

Толмачевська Юлія (ORCID ID: 0000-0002-7964-8875), докторка філософії (081 право): розділ 21 (у співав. з О. Ткаличем);

Фасій Богдан (ORCID ID: 0000-0002-8715-930X), кандидат юридичних наук, доцент, декан факультету судового та міжнародного права НУ «ОЮА»: розділ 18;

Розумейко Дмитро (ORCID ID: 0000-0001-8206-1031), аспірант кафедри цивільного права НУ «ОЮА»: розділ 16;

Рябченко Вікторія (ORCID ID: 0009-0007-1542-6492), аспірантка кафедри цивільного права НУ «ОЮА»: розділ 15.

Розділ 15

ВЕРБУВАННЯ НЕПОВНОЛІТНІХ ЧЕРЕЗ СОЦМЕРЕЖІ ТА МЕСЕНДЖЕРИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ: ЗАГРОЗИ, МЕХАНІЗМИ ТА ЗАХОДИ ЗАПОБІГАННЯ

DOI

Вікторія Рябченко
аспірантка

Вступ. Сучасний світ переживає епоху активного розвитку цифрових технологій, які значно змінюють способи взаємодії між людьми, формування інформаційних потоків та доступу до контенту. Віртуальний простір став невід'ємною частиною життя молодого покоління, як наслідок, зростає занепокоєння щодо нових форм руйнівного впливу на дітей.

Нові інформаційні технології та засоби зв'язку суттєво впливають на реалізацію прав дитини, закріплених у міжнародних документах, таких як Конвенція про права дитини (ратифікована 27.02.1991), Європейська Конвенція з прав людини (ратифікована 17.07.1997) та Європейська соціальна хартія (ратифікована із заявами 14.09.2006). Всі діти мають право на безпечний доступ до інформаційно-комунікаційних технологій та цифрових засобів масової інформації. Це право передбачає можливість повноцінно брати участь у суспільному житті, вільно висловлювати свої думки, шукати необхідну інформацію та користуватися усіма правами, гарантованими КПП ООН та її факультативними протоколами, без дискримінації.

Відповідно до статті 9 Закону України «Про охорону дитинства», кожна дитина має право на вільне висловлювання особистої думки, формування власних поглядів та розвиток громадської активності. Це право також передбачає свободу шукати, отримувати, використовувати, поширювати та зберігати інформацію будь-яким чином, зокрема через інтернет. Для забезпечення здорового фізичного, психічного, соціального, духовного та морального розвитку

дитини їй гарантується доступ до інформації з національних та міжнародних джерел¹.

Однак важливо враховувати, що доступ до цифрових технологій повинен бути безпечним і захищеним від будь-яких загроз, які можуть порушити права дитини. Технологічний прогрес, хоча і надає нові можливості для розвитку та самоствердження молоді, також створює ризики.

Соціальні мережі та месенджери, які спочатку були створені для комунікації, освіти та розваг, поступово перетворилися на інструменти маніпуляції свідомістю, зокрема, неповнолітніх. Країна-агресор активно використовує інтернет-платформи для розпалювання суспільного розколу, поширення страху та вербування молоді для здійснення деструктивних дій. Починаючи з ігор типу «Синій кит» (інші назви – «Тихий дім», «Розбуди мене о 4:20», «Море китів», «Чумацький шлях», «U19», «F57») та «Двері розуму» (інша назва – «Червоні двері, жовті двері»), завершуючи сучасними методами вербування неповнолітніх для терористичних актів: підпалів та підривів, ця стратегія є частиною ширшої гібридної війни, спрямованої на дестабілізацію суспільства.

Ці явища не лише демонструють новий рівень маніпуляції свідомістю, але й ставлять перед суспільством ряд важливих питань. По-перше, як саме організатори таких ігор та вербувальники використовують механізми для впливу на неповнолітніх? По-друге, які фактори роблять молодь особливо вразливою до такого роду впливу? По-третє, які інструменти можуть бути застосовані для запобігання та протидії таким явищам?

Стан опрацювання. Різні аспекти захисту прав та інтересів неповнолітніх були предметом аналізу у багатьох наукових працях провідних вчених, таких як *О. В. Мельник, Глиняної К. М., Т. В. Боднар, І. В. Жилінкової, Л. В. Красицької, М. В. Менджул, О. В. Розгон, З. В. Ромовської, О. І. Сафончик, Є. О. Харитонова*. Окрім того, є окремі праці, що стосуються заборони участі дітей під час воєнних дій та у збройних конфліктах (*Глушко М. В., Лесько Н. В.* та ін.). Водночас проблематика впливу російських спецслужб через соцмережі та месенджери, зокрема телеграм, на неповнолітніх є достатньо новою,

¹ Про охорону дитинства: Закон України від 26.04.2001 № 2402-III: станом на 1 січ. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/2402-14#Text>

тому проблеми захисту молоді України у цьому випадку досліджені фрагментарно.

Це підкреслює *актуальність* подальших досліджень для запобігання вербуванню неповнолітніх, формування ефективних механізмів захисту та забезпечення безпеки молоді в умовах гібридної війни. Потреба у комплексному вивченні цього питання обумовлена не лише загрозами для окремих осіб, а й ризиками для стабільності суспільства в цілому.

Виклад основного матеріалу. Гра «Синій кит» є одним із найбільш тривожних феноменів сучасного цифрового суспільства, який набув широкого поширення на платформі соціальної мережі «ВКонтакте» (стосовно якої у 2017 році Президент України своїм указом встановив вимогу блокування доступу на території України), а потім і телеграм у період 2016–2018 років. Її походження пов'язане з росією, де вперше були зареєстровані випадки участі неповнолітніх у грі та її трагічних наслідків.

Ця інтернет-гра спрямована на маніпуляцію свідомістю неповнолітніх через серію завдань, які поступово поглиблюють психологічний тиск і закінчуються інструкцією до самогубства. Гра «Синій кит» представляє собою серію завдань, які користувачі повинні виконувати протягом 50 днів. Завдання починаються з невинних дій, таких як перегляд фільмів жахів або прослуховування депресивної музики і поступово переходять до більш радикальних дій, наприклад, самопошкодження, порізів шкіри. Останнє завдання полягає у стрибку з високої будівлі або іншому способі самогубства.

Організатори гри, як правило, виступають у ролі «кураторів» (або ще вони себе називають «куратори смерті»), які контролюють виконання завдань через месенджери, соціальні мережі або закриті онлайн-чати. Вони використовують психологічний тиск, загрози та шантаж для того, щоб примусити учасників продовжувати гру. Так, за перші 7 місяців 2018 року діти здійснили 156 спроб суїцидів. З них у 58 випадках неповнолітні загинули. За даними ЄРДР, у 2020 році вчинили самогубство 123 підлітки, а вже на початку березня 2021 року органами Національної поліції було зафіксовано 25 випадків самогубств і 91 спробу вчинити такі дії¹.

¹ В Україні торік вчинили самогубство 123 підлітки – МВС. *УКРІНФОРМ*. URL: <https://www.ukrinform.ua/rubric-society/3213177-v-ukraini-torik-vcinili-samogubstvo-123-pidlitki-mvs.html>

Гра «Синій кит» використовує ряд психологічних механізмів, які сприяють формуванню залежності та втраті критичного мислення, зокрема, прогресивне зростання складності, тобто завдання у грі поступово ускладнюються, що створює ефект «просування до мети». Гравець втрачає здатність критично оцінювати наслідки своїх дій. Організатори гри часто використовують загрози, шантаж або обіцянки «відкриття нового світу» для того, щоб примусити гравців продовжувати участь. Ізолювання, оскільки гра створює ілюзію особистого зв'язку з «куратором», що призводить до соціальної ізоляції гравця від родини та друзів. Штучне створення страху, власне «куратори» використовують загрози розкриття секретів або залякування для того, щоб утримати гравця у грі.

Участь у даній грі може мати серйозні наслідки для неповнолітніх: перш за все, наслідком тривалого психологічного тиску та втрати контролю над своїми діями стає самогубство. Багато завдань у грі вимагають само пошкодження (наприклад, порізи, опіки), що може призвести до фізичних травм, які потребують медичної допомоги. Гравці часто стикаються з тривожністю, депресією, параноєю та іншими психічними розладами. Постійний тиск та стресові ситуації можуть призвести до довготривалого впливу на психічний стан. Учасники гри часто віддаляються від родини, друзів та суспільства, що призводить до соціальної маргіналізації та погіршення якості життя.

З початком повномасштабного вторгнення країна-агресор «в темну» використовувала українську молодь для збору даних про місцезнаходження стратегічно важливих об'єктів. На початку 2022 року стали відомі декілька фактів вербування українських неповнолітніх спецслужбами російської федерації, для цього останні використовують смартфон-ігри. Одна з таких ігор пропонує користувачам шукати «коробки» з віртуальними призами, які можна обміняти на електронні гроші. Під час цього процесу діти, не усвідомлюючи наслідків, фотографують місцевість, включаючи об'єкти військової та критичної інфраструктури у різних населених пунктах. Усі дані включно з геопозицією потім зберігаються в базі додатку і потім можуть бути використані для розвідки або планування диверсій.

У 2025 році Національна соціальна сервісна служба України повідомила, що серед неповнолітніх почав поширюватися новий небезпечний тренд – гра «Червоні двері, жовті двері», також відома як

«Двері розуму», що передбачає введення гравця у трансopodobний стан. Ця гра є своєрідним онлайн-ритуалом або челенджем, який зазвичай відбувається в реальному житті під керівництвом іншої особи. Учасник лягає на підлогу, а інша людина здійснює ритмічні масажні рухи його скронь, одночасно повторюючи фразу «Червоні двері, жовті двері». Після досягнення певного стану, учасник нібито потрапляє до уявного коридору з безліччю дверей різних кольорів. Завдання полягає у відкритті цих дверей та описі того, що знаходиться за ними. Ключовим елементом гри є пошук «червоних» та «жовтих» дверей, які, за повір'ями, можуть відкрити доступ до підсвідомості або інших «вимірів».

Незважаючи на те, що гра «Двері розуму» не передбачає прямих завдань, спрямованих на само пошкодження, як у «Синьому киті», такі розваги можуть шкодити школярам як фізично так і психологічно.

Національна соціальна сервісна служба України акцентує увагу на тому, що так зване підкорення «провіднику» чи «куратору» і соціальний тиск можуть використовуватися для підготовки підлітків до виконання небезпечних або злочинних дій, у тому числі на користь країни-агресора¹.

Ці ігри вкотре демонструють, як легко можна залучити неповнолітніх через інтернет, використовуючи їхню вразливість, пошук значущості та бажання належати до «спільноти». Хоча масштаби поширення ігор залишаються предметом дискусій, їх поява стала важливим сигналом про те, що соціальні мережі можуть бути використані для організації більш масштабних «проектів» за участі неповнолітніх.

За даними проведеного дослідження громадянською мережею «Опора» однією з популярніших соціальних мереж в Україні станом на 2024 рік є телеграм (ним користується 78,1% опитаних), друге і третє місце посідають ютуб (59,5%) та фейсбук (44,6%) відповідно². Варто відзначити, що ще в 2023 році телеграму перевагу надавало 71,3% опитаних осіб, тобто за один рік кількість нових прихильників зросла на 6,8%.

¹ Національна соціальна сервісна служба – Небезпечний тренд серед дітей: гра «Червоні двері, жовті двері».. URL: <https://nssu.gov.ua/news/nebezpechnyi-trend-sered-ditei-hra-chervoni-dveri-zhovti-dveri>

² «Опора»: найпопулярнішими соцмережами в Україні є телеграм, ютуб та фейсбук. URL: <https://ms.detector.media/sotsmerezhi/post/35557/2024-07-16-opora-naypopulyarnishymy-sotsmerezhamy-v-ukraini-ie-telegram-yutub-ta-feysbuk/>

Telegram став однією з найпопулярніших платформ для впливу на неповнолітніх через інтернет, оскільки його технічні та функціональні особливості ідеально підходять для таких цілей. Однією з ключових переваг телеграму є можливість зберігати анонімність, так користувачі можуть створювати облікові записи без надання реальних даних (наприклад, номер телефону можна замаскувати), можливість використання псевдонімів дозволяє «кураторам» залишатися невпізнаними.

Telegram надає можливість створювати закриті чати та канали, доступ до яких мають лише конкретні користувачі, тобто, вербувальники можуть створювати приватні групи, де вони координують дії своїх «підопічних», але одночасно з цим учасники не можуть побачити інших учасників чату. Такі чати часто захищені паролями або посиланнями, які доступні лише за запрошенням.

Telegram використовує технологію кінцевого шифрування для секретних чатів, що робить неможливим перехоплення повідомлень. Правоохоронні органи та провайдери не можуть отримати доступ до контенту, саме ця функція зробила цей месенджер популярним серед організаторів нелегальної діяльності.

Платформа неактивно бореться зі шкідливими групами або каналами, поки вони не отримають великої уваги ЗМІ або офіційних скарг, тому вербувальники часто використовують цю «лазівку» для пошуку потенційних жертв.

Вербування і використання дітей прямо заборонені, як міжнародним правом – норма 136 звичайного міжнародного гуманітарного права, спільна ст. 3 Женевських конвенцій 1949 року, ст. 77 Додаткового протоколу до Женевських конвенцій 1949 року, що стосується захисту жертв міжнародних збройних конфліктів, ст. 38 Конвенції про права дитини, факультативний протокол до Конвенції про права дитини щодо участі дітей у збройних конфліктах, так і національним правом – ст. 30 Закону України «Про охорону дитинства». Незважаючи на те, що всі зазначені норми є обов'язковими для виконання, російська федерація, як сторона міжнародних договорів, цинічно порушує ці положення. Такі дії зі сторони країни-агресора є явним порушенням норм міжнародного права та свідчать про нехтування принципами гуманності та захисту прав дитини.

За офіційними повідомленнями правоохоронних органів в період з лютого 2022 року по березень 2025 щонайменше 50 неповнолітніх були завербовані й брали участь у підпалах і підривах. За цей же період відбулись 42 підпали і підриви в адміністративних будівлях, ТЦК, 88 підпалів і підривів військових, військової техніки та правоохоронців¹.

Ці порушення мають систематичний характер і є частиною гібридної війни, тому важливим є не лише документування таких фактів для подальшого їх використання в міжнародних судах, але й проведення активної роботи щодо запобігання вербуванню та захисту прав дітей.

Неповнолітні є особливо вразливими до вербування через ряд психологічних особливостей, які характерні для їхнього вікового періоду. Перш за все, це постійний пошук ідентичності та значущості. У цьому віці молодь часто намагається знайти відповіді на питання «Хто я?» та «Яке моє місце у світі?». Вербувальники використовують цю потребу, надаючи неповнолітнім ілюзію того, що їхні дії мають величезне значення. Наприклад, вони можуть переконувати молодь, що їхня участі у підпалах або підривах є актом «героїзму» або «боротьби за справедливість».

Другий важливий фактор – емоційна лабільність. Неповнолітні частіше дорослих схильні до емоційних коливань, що робить їх більш вразливими до маніпуляцій. Зловмисники часто використовують техніки емоційного тиску, такі як загрози, шантаж або обіцянки нагороди. Наприклад, вербувальники можуть говорити щось подібне: *«якщо ти не виконаєш, твої близькі можуть постраждати»* або *«якщо сьогодні не спалиш машину, я в СБУ відправляю твою розвідку і наші розмови з тобою, у мене все збережено»*.

Представники російських спецслужб в телеграмі можуть додати дитину, без її згоди, до приватних груп. У таких чатах молоді пропонують завдання або обіцянки винагороди за залучення нових учасників. Останні часто навіть не знають, хто саме їх додав. Вербувальними часто використовують фальшиві аккаунти, створюють фейкові профілі, які виглядають доволі реалістично: з фотографіями

¹ Гарасим А., Кельм Н., Романишин Н. Вимкніть телеграм. Він робить з українських дітей терористів (інфографіка). URL: <https://texty.org.ua/articles/114801/vymknit-telegram-vin-robyt-z-ukrayinskyh-ditej-terorystiv-infohrafika/>

та історіями, аналізують відкриті чати (наприклад, волонтерські, тематичні або ті, що є популярними серед неповнолітніх), вибирають потенційних жертв і надсилають їм повідомлення. Вони очікують реакції та намагаються встановити контакт.

Третім і найголовнішим фактором є те, що у підлітковому віці спостерігається значне зростання потреб, які потребують фінансових витрат. Однак через ряд причин реалізувати їх часто стає складно. Це можуть бути обмеження, пов'язані з фінансовим становищем сім'ї, малопривабливі для підлітків способи заробітку (наприклад, фізична праця після занять), правові обмеження на працевлаштування через вік або деякі інші причини. Такі фактори ускладнюють задоволення матеріальних бажань у цьому віці. Проведені дослідження засвідчили, що матеріальні труднощі є однією з найпоширеніших причин учинення неправомірних дій неповнолітніми¹.

Вербування починається з невинних, на перший погляд, завдань, за більш менші суми, таких як намалювати графіті, розклеювати листівки або розповсюджувати інформацію.

Приклад з конкретної ситуації: *«Почни поки що з малого, моя порада. Якраз і придивимося один до одного. Ну щось дріб'язкове спочатку зроби, а далі вже найбільші куші»².*

Вербувальники найчастіше вдаються до маніпуляцій і обіцянок легких грошей. Вони можуть запевняти молодь, що за виконання небезпечних і протиправних завдань вони отримають значну фінансову винагороду. Такі обіцянки часто формулюються так, щоб переконати неповнолітнього, що це «легкий» спосіб швидко заробити, не вимагаючи великих зусиль чи спеціальних навичок. Неповнолітні легко відгукуються на оголошення на кшталт: «2-3 тисячі доларів, навички не потрібні, тільки ваше бажання, ваш телефон і час».

Найчастіше мова йде про суми від кількох тисяч до сотень тисяч гривень, що стає потужним спонукальним мотивом для підлітків. Однак, насправді, ці обіцянки часто є лише приманкою: деякі жер-

¹ Шанкова Т. І. Аналіз причин правопорушень неповнолітніх як підґрунтя соціально-педагогічної роботи з молоддю щодо профілактики злочинності. *Вісник Житомирського державного університету ім. І. Франка*. 2006. № 30. С. 50-53.

² Свобода Р. «Тобі за це нічого не буде»: як спецслужби РФ свідомо вербують дітей для підпалів авто ЗСУ і будівель ТЦК. *Радіо Свобода*. URL: <https://www.radiosvoboda.org/a/news-fsb-pidlitky-pidpaly-avto-zsu/33151236.html>

тви можуть отримати лише частину зазначеної суми як аванс, а інші взагалі залишаються без грошей. Більш того, у багатьох випадках вербувальники ігнорують свої зобов'язання, оскільки їхня мета полягає не в оплаті послуг, а в максимально можливому втягуванні молоді у протиправні дії. У кращому випадку підліток отримує невеликий платіж, але реальна винагорода за свою участь їм так і не сплачується. Такий підхід демонструє маніпулятивну стратегію спецслужб, які намагаються залучити неповнолітніх, використовуючи їх довірливість та недосвідченість.

При цьому вербувальники свідомо замовчують реальні наслідки таких дій. Неповнолітні, які часто ще не мають достатньо життєвого досвіду та критичного мислення, можуть потрапити під вплив таких маніпуляторів і погодитися на небезпечні дії, спокушаючись швидкими грошиками.

Наприклад, у переписках з 12-річним хлопцем вербувальник заявив: *«Навіть якщо тебе спіймають, максимум будеш легко фізично покараний»*¹. Такі заяви формують помилкове враження безкарності.

Співробітник департаменту контррозвідки СБУ вказує наступне: «Були випадки, коли паліями були діти до 14-ти років. Вони ще не мають повністю сформованого бачення, не розуміють всієї серйозності суспільного резонансу і наслідків, і це просто легкий заробіток швидких грошей»².

У вербуванні неповнолітніх для здійснення підпалів автомобілів ЗСУ чітко простежується спланована російська пропагандистська кампанія, метою якої є дестабілізація ситуації в Україні. Відомо, що «куратори» часто намагаються замаскувати свої дії під протест проти територіальних центрів комплектування та соціальної підтримки (далі – ТЦК) або мобілізації. Молоді пропонують знайти будь-який старий, згорілий автомобіль, за умови, що в ньому щось залишилося цілим. Далі їм дають вказівку прикріпити до авто наклейку ЗСУ й підпалити його. Це чітко демонструє, що такі дії є частиною спланованої пропагандистської кампанії.

¹ Свобода Р. «Тобі за це нічого не буде»: як спецслужби РФ свідомо вербують дітей для підпалів авто ЗСУ і будівель ТЦК. *Радіо Свобода*. URL: <https://www.radiosvoboda.org/a/news-fsb-pidlitky-pidpaly-avto-zsu/33151236.html>

² Свобода Р. «Тобі за це нічого не буде»: як спецслужби РФ свідомо вербують дітей для підпалів авто ЗСУ і будівель ТЦК. *Радіо Свобода*. URL: <https://www.radiosvoboda.org/a/news-fsb-pidlitky-pidpaly-avto-zsu/33151236.html>

Під час спілкування з потенційними виконавцями куратори активно наголошують, що їхня «мета» – боротьба з ТЦК. *«Наша мета – захистити простих людей, щоб їх не забирали до мобілізації», «Ми – організація, яка бореться з ТЦК. Нас фінансують, і виділяють великі суми на ці завдання»*¹. Такий наратив спеціально обраний стороною-агресором.

За всіма випадками підпалів стоять російські спецслужби, зокрема ФСБ. Існує спроба створити ілюзію, що підпалювання є актами протесту з боку українців, які не схвалюють політику влади чи мобілізацію. Однак насправді це елемент інформаційно-психологічних операцій (ІПСО), які активно поширюються та набирають обертів у засобах масової інформації та соціальних мережах.

Виходить, що підпал автомобілів – це не окремі випадки вандалізму, а добре продумана стратегія російських спецслужб, метою якої є підриз довіри до української влади та створення ілюзії внутрішнього протистояння.

Однак, країна-агресор не зупиняється лише на підпалах авто, вони «йдуть» далі і вдаються до залучення українських неповнолітніх до терористичних актів.

Так, за інформацією прокуратури та Служби безпеки України, 14-річну неповнолітню завербували через месенджер телеграм для вчинення вибуху біля райвідділу Національної поліції². Вербувальник знайшов дівчину, коли вона шукала можливості швидкого заробітку в інтернеті. Щоб схилити її до співпраці, той «зламав» її телефон і почав шантажувати, загрожуючи оприлюднити її відверті фото. Під тиском погроз дівчина виготовила саморобний вибуховий пристрій за інструкціями, які надавалися онлайн. Конструкція була створена з доступних матеріалів, включаючи елементи електроніки та засоби ініціювання і була прихована під службовим автомобілем поліції.

За даними фахівців, саморобні вибухові пристрої складаються з компонентів, які легко придбати у вільному доступі. Вербувальники надають детальні інструкції через відео зв'язок, пояснюючи, як змішувати хімічні речовини, під'єднати електронні елементи та ство-

¹ Там само.

² Неповнолітню жительку Тернопільщини підозрюють у спробі вчинити теракт біля райвідділу поліції. *СУСПІЛЬНЕ ТЕРНОПІЛЬ*. URL: <https://suspilne.media/ternopil/975867-nepovnitnutu-zitelky-ternopilsini-pidozruut-u-sprobi-vciniti-vibuh-bilajajviddilu-policii/>

рювати механізм підриву. Для цього не потрібні спеціальні знання з хімії, фізики чи електрики, так як «куратор» контролює процес онлайн, крок за кроком¹.

Як зазначалося раніше, неповнолітнім обіцяють значні суми грошей, але ці обіцянки лише приманка. Окрім несплати грошей, «куратори» знищують своїх «агентів» разом із вибуховими пристроями, щоб уникнути розкриття. 11 березня 2025 року в Івано-Франківську стався завчасно спланований теракт, який двоє місцевих підлітків виконували на замовлення і за вказівками російських спецслужб. Через детонацію вибухових пристроїв один підліток загинув на місці, іншому – ампутували ноги².

Наслідки вербування неповнолітніх є руйнівними як для самих жертв, так і для суспільства в цілому. Перш за все, це фізичні та психологічні травми, які отримують неповнолітні. Участь у підпалах, підривах або інших формах насильства часто призводить до травм, інвалідності або навіть смерті або завербовані можуть страждати від посттравматичного стресового розладу (ПТСР), депресії або інших психічних розладів.

Наступним наслідком може стати соціальна маргіналізація. Неповнолітні, які потрапили під вербування, часто стикаються зі стигмою у суспільстві. Їхні родини також можуть страждати від психологічних травм, фінансових труднощів або соціального відвернення. Це створює замкнене коло, де молодь ще більше відчувається відверненою та схильною до повторного впливу.

Далі – дестабілізація суспільства. Дії, організовані через вербування неповнолітніх, спричиняють масову паніку та політичну нестабільність. Це стосується не лише окремих країн, але й глобальної безпеки.

Для ефективної боротьби з вербуванням неповнолітніх необхідно застосовувати комплексний підхід, який включає правові, освітні та психологічні заходи.

Так, у відповідь на тривалу збройну агресію російської федерації проти України та систематичні порушення прав дітей, Кабінет Міні-

¹ Як спецслужби РФ вербують підлітків для терактів: коментарі поліцейських з Тернопільщини. *СУСПІЛЬНЕ ТЕРНОПІЛЬ*. URL: <https://suspilne.media/ternopil/983723-ak-specsluzbi-rf-verbuutpidlitkiv-dla-teraktiv-komentari-policejskih-z-ternopilsini/>

² Вибухи в Івано-Франківську – що відомо. *TCH.ua*. URL: <https://tsn.ua/ukrayina/terakt-v-ivano-frankivsku-shokuvalni-podrobici-vibuhiv-bilya-zaliznichnogo-vokzalu-2786328.html>

стрів України затвердив Національний план превентивних заходів від 22 березня 2024 року № 256-р¹. Цей документ спрямований на припинення та запобігання грубим порушенням прав дітей у зоні конфлікту, зокрема щодо вербування, використання та участі неповнолітніх у бойових діях і збройних конфліктах. Згідно з положеннями якого основними напрямками діяльності держави є: по-перше, інформаційно-просвітницька робота. Одним із ключових завдань плану є проведення широкомасштабної просвітницької кампанії серед дітей, батьків та законних представників. Ця робота передбачає залучення громадських організацій, міжнародних партнерів та медіа для поширення достовірної інформації про загрози, пов'язані з вербуванням дітей. Розробка та розповсюдження інформаційних матеріалів, які пояснюють наслідки вербування та використання неповнолітніх. Залучення експертів для проведення лекцій, семінарів та тренінгів з метою підвищення обізнаності населення. Використання сучасних медіа-платформ для інформування громадян про методи вербування та способи запобігання таким ситуаціям.

По-друге, моніторинг та інформування про факти вербування, офіс Генерального прокурора України має інформувати про будь-які факти вербування (у тому числі прихованого) дітей для участі у збройних формуваннях. Особливу увагу приділяють документуванню таких випадків для подальшого їх використання в міжнародних судових органах.

По-третє, для запобігання можливим випадкам вербування та використання дітей у збройних конфліктах передбачено проведення роз'яснювальної роботи серед молоді щодо того, як розпізнавати методи вербування через соціальні мережі, месенджери та особисті контакти.

Особлива увага приділяється запобіганню залучення дітей до виконання завдань, пов'язаних із збройним конфліктом, таких як розвідка, підпали авто та диверсії. Для цього має проводитись активна робота зі школярами та студентами щодо розуміння наслідків таких дій, впроваджується система раннього виявлення потенційних ви-

¹ Про затвердження національного плану превентивних заходів щодо припинення та запобігання грубим порушенням прав дітей в умовах збройної агресії Російської Федерації проти України: Розпорядж. Каб. Міністрів України від 22.03.2024 № 256-р. URL: <https://zakon.rada.gov.ua/laws/show/256-2024-p#Text>

падків вербування через аналіз активності в соціальних мережах та месенджерах.

Залучення громадських організацій та міжнародних партнерів є невід’ємною частиною реалізації Національного плану. Співпраця з такими організаціями допоможе як забезпечити широкий охопит про-світницьких заходів, так і залучити міжнародні організації до моніторингу порушень прав дітей та документування таких фактів.

Міністерством освіти і науки України батькам стосовно їх дітей рекомендовано: спостерігати за поведінкою, навчати фінансової грамотності, привчати до цифрової безпеки та розпізнаванню маніпуляцій і найголовніше – мати з неповнолітнім відкрите спілкування та підтримувати довірливі стосунки¹.

Відповідно до ч. 2 ст. 150 Сімейного кодексу України батьки зобов’язані піклуватися про фізичний, духовний і моральний розвиток дитини². Батьки мають не тільки створити безпечне середовище для розвитку своєї дитини, а й піддавати її контролю. Інакше кажучи, раціональний та свідомий батьківський контроль може стати запобіжником девіантної поведінки неповнолітнього. Саме для цього існує низка корисних сервісів для батьків, за допомогою яких можна наглядати за неповнолітнім, при цьому не порушуючи його особистих кордонів, таких як Google Family Link, Qustodio, Bark. Однак, батькам не слід покладатися лише на технічні засоби контролю, адже діти можуть знайти способи обійти обмеження. Натомість важливо познайомити їх із прийомами онлайн-вербовки, навчити розрізняти фейки та пояснити наслідки розголошення секретної інформації, яку не слід знати представникам країни-агресора.

Разом з тим, існують ресурси, які допомагають протидіяти дезінформації та вербуванню. Наприклад: телеграм-канал «Брама» надає інформацію про блокування підозрілих акаунтів та дає поради щодо захисту від шахрайства. Канал «StopRussia | MRIYA» пропонує інструкції та завдання для протидії фейкам та інформаційним загрозам. Чат-боти СБУ «Знайди зрадника» та «Спали ФСБшника» дозволяють повідомляти про спроби вербування або інші протиправні дії.

¹ Як розпізнати ознаки вербування дитини? Рекомендації батькам і освітянам. URL: <https://mon.gov.ua/news/yak-rozpiznaty-oznakyverbuвання-dytny-rekomendatsii-batkam-i-osvitianam>

² Сімейний кодекс України: Закон України від 10.01.2002 № 2947-III. URL: <https://zakon.rada.gov.ua/laws/show/2947-14#Text>

Батьки можуть надати дітям конкретні поради для уникнення вербування: бути обережними в інтернеті та уникати контактів із підозрілими особами, звертати увагу на ознаки обману, такі як пропозиції швидкого заробітку за виконання простих завдань. Якщо дитина отримує підозрілі пропозиції, їй слід негайно повідомити про це дорослих або звернутися до поліції за телефоном «102», або заповнивши форму зворотного зв'язку на сайті кіберполіції.

Протидіяти вербуванню можна також через формування сталої системи цінностей, яка ґрунтується на таких ключових принципах, як патріотизм, відчуття національної приналежності, єдності та поваги до своєї країни. Ці цінності допомагають неповнолітнім розуміти важливість захисту держави та її інтересів, а також створюють моральні бар'єри проти залучення до протиправних дій. Виховання у дітей почуття гордості за свою націю та історію формує стійкий імунітет до маніпуляцій з боку країни-агресора.

Ефективними інструментами для формування таких цінностей є активна волонтерська діяльність, яка надає молоді можливість реалізувати себе у корисних для суспільства справах. Наприклад, організація акцій з виготовлення оберегів для військових не лише сприяє підтримці Збройних Сил України, але й дає молоді відчуття причетності до загальнонаціональної боротьби за незалежність. Такі проекти часто супроводжуються лекціями, тренінгами та бесідами, де молодь отримує інформацію про значення кожного внеску у загальну перемогу. Крім того, збір коштів для потреб ЗСУ – це ще один спосіб залучити молодь до активної участі у захисті держави. Це можуть бути благодійні ярмарки, флешмоби чи онлайн-кампанії, які не лише допомагають залучати фінансові ресурси, але й формують відповідальне ставлення до суспільних проблем.

Підсумовуючи вищевикладений матеріал, можна зазначити, що сучасний цифровий світ, незважаючи на свою інноваційність та можливості, несе значні загрози для неповнолітніх, особливо в умовах збройних конфліктів та гібридної війни. Російські спецслужби активно використовують соціальні мережі, месенджери та інші онлайн-платформи для вербування молоді до участі в протиправних діях, таких як підпали автомобілів, підриви, або навіть терористичні акти. Психологічна вразливість, пошук ідентичності, потреба в швид-

ких грошах та недосвідченість роблять неповнолітніх доступними цілями для маніпуляторів.

Небезпечні ігри, подібні до «Синього кита» та «Дверей розуму», є лише частиною ширшої стратегії впливу на свідомість молоді. Ці феномени демонструють, як легко можна залучити дітей через інтернет, використовуючи їхню довірливість та через ряд психологічних особливостей. Наслідки такого впливу є руйнівними: самогубства, каліцтва, психічні розлади, соціальна маргіналізація та дестабілізація суспільства в цілому.

Для запобігання вербуванню та захисту прав дітей необхідний комплексний підхід, який включає просвітницьку роботу, правове регулювання, постійний моніторинг. Затверджений Національний план превентивних заходів є важливим кроком у цьому напрямку. Однак успіх залежить від спільних зусиль батьків, педагогів, правоохоронних органів та громадськості. Саме довірливі стосунки, відкрите спілкування та формування стійкої системи цінностей допоможуть захистити молодь від небезпечного впливу та забезпечать майбутнє безпечного та стабільного суспільства.

Ключові слова: неповнолітні, гібридна війна, цифрові загрози, вербування, соціальні мережі, месенджери, інформаційна безпека, радикалізація молоді, безпека дітей в інтернеті, протидія вербуванню.