ІНТЕРНЬЮЗ УКРАЇНА

ЗВІТ ЗА РЕЗУЛЬТАТАМИ ГЛИБИННИХ ІНТЕРВ'Ю

Потреби з цифрової безпеки журналістів та представників громадського сектору

Вибірка: 20 інформантів

Терміни проведення: 26 червня — 10 липня 2024

КИЇВ 2024

ЗМІСТ

ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО ДОСЛІДЖЕННЯ

Повномасштабне вторгнення рф призводить до посилення інформаційної війни та спричиняє істотну зміну ландшафту українського медіапростору. В умовах війни журналісти та активісти стають об'єктом особливого інтересу з боку російських спецслужб, унаслідок чого актуалізується питання цифрової безпеки.

Основна мета дослідження — визначити наявні потреби з цифрової безпеки журналістів та представників громадських організацій. Для досягнення цієї мети були поставлені такі завдання:

- визначити основні зміни, що відбулися в українському медіапросторі протягом повномасштабного вторгнення;
- охарактеризувати зміни цифрової безпеки, що відбулися в медійних організаціях за останні 2–3 роки;
- виявити правила цифрової безпеки, якими керуються журналісти та активісти;
- визначити чинники спротиву запровадженню елементів цифрової безпеки в організаціях;
- виявити елементи політик цифрової безпеки, що прийняті на рівні медійних організацій;
- з'ясувати потреби журналістів та активістів у навчанні та послугах цифрової безпеки.

Методологія дослідження: 20 глибинних інтерв'ю з журналістами, представниками громадських організацій, експертами з цифрової безпеки.

Формат проведення: телефонні інтерв'ю та онлайн-зустрічі за допомогою платформи Zoom.

Схема вибірки

Терміни проведення: 26 червня — 10 липня 2024 року.

РЕЗЮМЕ

З початку повномасштабного вторгнення відбувалася **посилення загроз** в інформаційному просторі. З одного боку, інформанти відзначають істотне збільшення кількості кібератак на медійні ресурси, поширення фейкової інформації в соціальних мережах та інформаційно-психологічних спецоперацій (далі — ІПСО) в цілому. З іншого боку, експерти з кібербезпеки та представники громадських організацій частіше говорять не так про появу якісно нових загроз, як про зростання зацікавленості та інтенсивності дій зловмисників щодо зламу ресурсів та проведення ІПСО.

Очевидним чинником посилення загроз є **збройна та інформаційна агресія з боку російської федерації**, спецслужби якої інформанти найчастіше згадують серед бенефіціарів кібератак. Серед інших зловмисників називають також окремих представників української влади (частіше як фігурантів антикорупційних журналістських розслідувань), українські спецслужби (як знаряддя в руках недобросовісних українських посадовців), шахраїв (зокрема транснаціональних груп).

Окрім безпосередньо активізації війни, опитані відзначають **розвиток технологій**, зокрема штучного інтелекту (далі — ШІ), які призводять до кількісного та якісного збільшення фейкової інформації, а також посилення кібератак.

Іншим чинником є поширення та **проникнення соціальних мереж** серед населення України, внаслідок чого відбувається відносне **зниження середнього рівня інформаційної грамотності**, зростання ризику зламування акаунтів рідних та знайомих журналістів, а відповідно — зростання загроз для особистої цифрової безпеки.

Серед особливих небезпек журналісти згадують **посилення тиску** на них і як наслідок — **поширення самоцензури** через побоювання про можливі наслідки публікації певних матеріалів. Названі процеси призводять до ерозії поля журналістики в цілому через загальне **зниження рівня довіри** до відповідного інституту, що в перспективі загрожуватиме функціонуванню демократичних інституцій в Україні.

Посилення загроз спричиняє **посилення вимог до цифрової безпеки**, до чого медійні та громадські організації виявилися неготовими. Протягом останніх 2–3 років інформанти стикалися з DDoS-, фішинговими та вірусними атаками, внаслідок яких відбувався злам доступу до адмінпанелей сайтів, сторінок в соціальних мережах; серверів, на яких зберігаються дані, зокрема сенситивні.

Попри заходи, спрямовані на посилення цифрової безпеки, інформанти відзначають **актуальність загроз витоку персональних даних**, створення фейкових каналів у соціальних мережах та месенджерах, що мімікрують під справжні; конструювання якісних дипфейків за допомогою ШІ, прослуховування та зовнішнє спостереження, зокрема GPS-трекінг, масовані кібератаки. Лише деякі опитані вважають, що їхня організація має **високий рівень захисту**.

Як зазначають експерти з цифрової безпеки, стан цифрового захисту організацій прямо залежить від інтенсивності практик особистої кібергігієни. Дослідження показало, що інформанти здебільшого говорять, що **ознайомлені з базовими правилами**, серед яких найчастіше згадують ті, що пов'язані з паролями до сайтів та сторінок (генерація та регулярне оновлення складних паролів через менеджери, двофакторна аутентифікація), та обережні під час отримання повідомлень через електронні засоби комунікації. Лише деякі респонденти до названого переліку додають використання антивірусів, VPN, створення резервних копій інформації, ознайомлення з технічною документацією під час встановлення програм (яке залишається здебільшого вибірковим), використання та регулярне оновлення ліцензійних програм, запобігання завантаженню документів на особисті пристрої, перенесення роботи винятково до інтернет-простору.

Попри загальну обізнаність щодо існування правил цифрової безпеки, інформанти відзначають, що вони та їхні колеги часто їх **не дотримуються повною мірою**. Серед причин найчастіше називають те, що впровадження змін призводить до **порушення звичного способу життя та роботи**, що спочатку спричиняє відразу, відчуття браку сил та часу; **брак мотивованості**, посилений небажанням визначити себе як потенційну жертву зловмисників, які начебто не цікавляться діяльністю локальних організацій; **брак фінансування** на програми та пристрої, які забезпечують більш надійний цифровий захист, а також окремі випадки виникнення **технічних проблем** зі згенерованими складними паролями через вимкнення електроенергії та/або збої в операційних системах гаджетів. Слабким місцем в організації особистої цифрової безпеки залишається те, що **журналісти несвідомо розмежовують** сервіси, які необхідні для професійної діяльності, та ті, які вони використовують у вільний час (здебільшого розважальні). Відповідно вони не поширюють правила цифрової безпеки на такі програми та застосунки.

Частина організацій опитаних співробітників мають **окрему політику щодо цифрової безпеки**, в інших — формалізованої політики немає, проте вживають **окремих заходів для впровадження цифрової безпеки**. Існують різноманітні форми ознайомлення працівників з правилами цифрової безпеки, зокрема безпосереднє спілкування служби безпеки з окремими департаментами (підрозділами) організації та/або системними адміністраторами, ознайомлення під час онбордингу, проведення регулярних тренінгів та інструктажів з інформаційної безпеки (як внутрішніх, так і зовнішніх), розсилка інструкцій через організаційні канали комунікації (як одноразова, так і регулярна). Зазвичай правила інформаційної безпеки обмежені **базовими інструкціями** щодо поведінки з ресурсами та сервісами, з якими працює організація. Лише в деяких організаціях існують посилені правили безпеки, зокрема **протоколи реагування** на випадки зламу акаунту, серверу тощо; **обмеження доступу** до ресурсів організації та роботи з персональних пристроїв; наявність **дублювальних хмар** та закритих серверів. Частина організацій має відповідну **службу безпеки**, якій делегована діяльність щодо запобігання зламу цифрової безпеки та реагування на відповідні випадки. Лише деякі організації намагаються поєднати заходи з технічних та соціальних (організаційних, особистих) аспектів цифрової безпеки.

Окремою вразливою ланкою кібербезпеки є сервіси, якими користуються журналісти **для внутрішньої комунікації**. Частина організацій не має політики, яка визначила б вичерпний перелік таких сервісів, тому їхні співробітники можуть користуватися декількома одночасно. У великих компаніях працівники можуть використовувати корпоративну пошту, Google Drive, Trello, Notion, а також різноманітні месенджери, що створює додаткові проблеми та загрози. Серед месенджерів інформанти частіше називають Telegram (водночас наголошуючи на розумінні ризиків, пов'язаних з походженням цього ресурсу) та WhatsApp, рідше — месенджери Facebook, Signal, Slack. Лише в деяких організаціях **поділяють комунікацію на робочу**, що передбачає залучення документів (здебільшого через корпоративну пошту) **та неробочу** (переважно через месенджери). Небажання переходити до більш захищених сервісів спілкування пов'язане зі зручністю (необхідність пересилати великі обсяги інформації, зокрема фото- та відео-, обмежує коло сервісів; комунікація з працівниками, які можуть перебувати, зокрема, на окупованій території, призводить до намагання полегшити способи комунікації) та коштами, необхідними на користування ними.

За словами інформантів, у їхніх організаціях працівники зазвичай **ознайомлені з алгоритмами захисту від фішингу**. Частина опитаних зазначила, що дізнається про такі правила під час тренінгів, які проводять або сама організація, або організація-партнер, що спеціалізується на цифровій безпеці. Менша частина респондентів **недостатньо ознайомлена** з такими алгоритмами, тому розв'язує проблеми з фішингом під час консультацій з відділом безпеки або з представниками організацій-партнерів, що зазвичай призводить до зайвих витрат часу.

За організацію заходів безпеки в організаціях частіше відповідають **окремі технічні відділи та департаменти**. Їхня компетенція здебільшого поширюється на організацію технічних параметрів та застосування рішень, спрямованих проти спланованих масових атак. У невеликих медіа та громадських організаціях за заходи безпеки відповідають **окремі працівники**: відповідний технічний спеціаліст, HR, менеджер офісу, голова департаменту або керівник організації. Для **посилення цифрової безпеки** в організаціях поширена практика проведення **тренінгів** (частіше — власними зусиллями, рідше — із запрошеними організаціями, які спеціалізуються на цифровій безпеці). У деяких організаціях замість спільних тренінгів організовують **індивідуальні сесії** із залученням організацій-партнерів. Думки про рівень складності таких тренінгів розділилися: з одного боку, багато інформантів відповіли, що не вважають такі тренінги складними, з іншого, частина повідомила, що їхні колеги під час таких заходів особисто не були зацікавлені. Проте, попри поширеність особистої невмотивованості, усі опитані вказали про актуальність знань та застосування навичок, отриманих під час таких тренінгів. За їхніми словами, з рутинізацією робочих процесів відбувається втрата пильності, тому важливо **регулярно нагадувати про основні правила цифрової безпеки**.

На думку частини інформантів, наявних заходів достатньо для досягнення цифрової безпеки в цілому. Інші інформанти згадували про **доречність таких кроків**, що впроваджені лише в деяких організаціях:

- складання внутрішнього протоколу безпеки;
- формування відділу безпеки, завданням якого був би моніторинг дотримання, наявності та впровадження автоматичних рішень з безпеки, насамперед для запобігання загрозам масових кібератак;

- збільшення відповідальності окремих працівників за власні дії;
- виділення коштів на покращення рівня безпеки сайту;
- запровадження періодичних тренінгів, на яких додатково були б розглянуті практичні кейси та потенційні наслідки недотримання окремих правил кібергігієни;
- поділ робочого та особистого цифрових просторів.

Частина інформантів вказали на особисту зацікавленість щодо регулярного проходження тренінгів з метою моніторингу загроз, які виникають в інформаційному просторі. Відповідно **основна потреба опитаних** — підтримувати наявний рівень обізнаності про інформаційні загрози, бажано з використанням матеріалів з конкретними кейсами. Лише деякі інформанти мають **конкретні запити**:

- інформація про різновиди VPN;
- способи захисту, зокрема хмарного, сайтів медіа;
- способи збереження сенситивного контенту;
- створення захищених каналів під час передачі інформації;
- убезпечення від незаконного стеження, способи ідентифікації прослуховування через девайси;
- особливості протоколів шифрування даних у месенджерах;
- використання ШІ для продукування фейків та способи розпізнавання дипфейків,
- особливості ІПСО;
- способи ідентифікації суб'єктів скарг на матеріали в соціальних мережах, що призводить до блокування сторінок організації (окрема людина, група людей, конкуренти тощо).

За словами респондентів, для тих користувачів, які лише починають ознайомлюватися з основами цифрової безпеки, доцільно використовувати **формат тренінгів**, під час яких вони матимуть змогу отримати відповіді на поширені запитання, для більш просунутих оптимальними будуть **індивідуальні консультації**. Участь у тренінгу **в офлайн-форматі** називають ефективнішою через можливість поставити більше запитань, сфокусувати увагу, що є запорукою результативного навчання, а також мінімізувати наслідки вимкнень електроенергії. Під час проведення тренінгів у будь-якому форматі доцільно звернути увагу на конкретні кейси, в ідеалі — від самих організацій; зосередитися на одній програмі, якою послуговуються в організації; використовувати домашні завдання, що разом дає змогу краще розібратися з нюансами, а також проводити тренінги на різну тематику для різних представників організації.

Послуг з цифрової безпеки потребує лише частина інформантів. Найчастіше вони згадують **аудит захищеності** серверів, адмінпанелей сайтів, корпоративної пошти тощо. Деякі опитані наголошували на потребі залучити **додаткове програмне забезпечення**, зокрема хмарні сховища, що потребує більших коштів. Один з інформантів згадав потребу в **гарячій лінії**, куди можна звернутися у випадку зламу ресурсів організації. Натомість потенційними **бар'єрами для проведення аудиту** можуть стати високий рівень недовіри до організації, яка його проводить, а також неготовність до відповідних фінансових витрат.

Зацікавленість у **створенні онлайн-платформи**, що об'єднувала б ініціативи з цифрової безпеки, проявили лише деякі інформанти. Насамперед вони не розуміють доцільності свого долучення, оскільки за потреби журналісти воліють звертатися по відповідні послуги особисто до фахівців. Експерти з кібербезпеки та представники громадських організацій виявили більшу зацікавленість. Щоб посилити їхній інтерес, варто роз'яснити, за яким напрямом така платформа працюватиме, на яких умовах туди можна долучитися, які джерела фінансування платформи, терміни співпраці та ступінь її захищеності. На думку інформантів, платформа могла б виконувати **такі функції**:

- цілодобова підтримка, розміщення контактів фахівців з різних напрямків;
- місце для формування навчальної програми та чеклістів для організацій, які хотіли б самостійно розв'язувати проблеми зі станом цифрової безпеки;
- оперативний обмін досвідом щодо новітніх загроз, зон ризику, способів забезпечення цифрового захисту організації;
- публікація дайджестів про тенденції е сфері інформаційної безпеки (актуальні загрози, кейси про наслідки зламів, способи визначення рівня небезпеки ресурсів, методи розпізнавання дипфейків, зміни політик соціальних мереж; софт, який допоможе убезпечити організацію тощо).

1. СПРИЙНЯТТЯ ЦИФРОВИХ ЗАГРОЗ

Зміни в медіапросторі за останні декілька років інформанти найчастіше пов'язують з **посиленням російсько-української війни** в цілому та інформаційного складника війни зокрема. Російські спецслужби, за словами опитаних, використовують інформаційну сферу для **поширення фейків** з метою розколу українського суспільства. Так, у медіапросторі можна спостерігати створення **дублікатів медіа** (часто — каналів у месенджерах), **поширення паніки** через фейкові історії, посилення **кібератак** з метою викрадення як персональних даних, так і даних організації. Окрім безпосередньо російського чинника, експерти називають появу транснаціональних груп, які здійснюють атаки водночас у різних регіонах світу.

Інформанти визначають останні роки як час, протягом якого відбулося **істотне пришвидшення життя**. Так, дехто пов'язує це з розвитком та поширенням використання месенджерів (передусім Telegram) як серед звичайних користувачів, так і серед журналістів. Прискорення потоків інформації стає причиною трансформації стандартів журналістики та встановлення часу публікації як найважливішого критерію. Це посилює **ризик публікації неперевіреної інформації**, оскільки, щоб прискорити публікацію, час заощаджують шляхом перевірки джерел. Відповідно інформанти, що працюють у сфері журналістики, фіксують зростання кількості повідомлень, що не пройшли фактчекінг, навіть у тих медіа, які зазвичай його проводять.

Водночас спостерігають посилення проникнення технологій у суспільство, що призводить до **погіршення середнього рівня медіаграмотності** нових користувачів. Унаслідок цього ризики як поширення фейків, так і зламу в медіапросторі суттєво посилилися. Часто самі журналісти не встигають стежити за інноваціями, тому їхні практики цифрової гігієни не завжди відповідають сучасним викликам, що створює вразливі ланки в системі організаційної безпеки.

«У цьому швидкому новинному порядку денному дуже часто стається, що ми ретранслюємо меседжі великій аудиторії, хоча мали б за всіма нашими правилами отримати 2—3 підтвердження. Утім, це зазвичай неможливо зробити, тому що в нас немає людей на місцях, певних джерел у дуже різних містах».

Гаяне, журналістка

«Потенційно більш небезпечний. Розвиваються технології. Тут навіть не війна, а час винен. Ну а вже з війною з'являються технології стеження за людьми, що потребують більшого розвитку».

Володимир, представник громадської організації

Серед **зловмисників, які цікавляться інформацією** від журналістів, найчастіше називають рф, у тому числі російські спецслужби. Окрім цього, журналісти також серед потенційних зловмисників згадують українську владу (зокрема Офіс Президента, корумповану частину української влади, українські спецслужби); окремих громадян, щодо яких проводилися журналістські розслідування; а також шахраїв, яких може цікавити отримана журналістами інформація.

«Основними зловмисниками є нечесні корумповані люди всередині української влади. А з іншого боку є зовнішні вороги, які теж бачать загрозу в діяльності журналістів, якщо журналісти, наприклад, розкривають військові секрети або агентів росії всередині країни».

Андрій, журналіст

«Це можуть бути просто шахраї, які намагаються якось на тебе вплинути; представники влади, адже ми знаємо, що в нас були випадки стеження за журналістами. Вони більше стосувалися не кіберсфери, але все ж таки. Також, я думаю, що з боку російської федерації така загроза може бути».

Владислав, журналіст

До **основних загроз** інформанти відносять злам зловмисниками акаунтів з метою отримання сенситивної інформації та/або поширення фейків, створення баз даних щодо журналістів, які пишуть на різноманітні тематики тощо. Такі загрози поширюються не лише на самих журналістів, але й на їхніх інформаторів / джерела в офіційних органах влади, що сприяє руйнуванню довіри до журналістів у цілому. До цього деякі опитані додають ризик зламу технічних пристроїв (смартфон, ноутбук), які можуть потрапити до рук окупантів, особливо якщо журналіст чи представник громадської організації працює на прифронтових територіях. Окрім самих інформантів, під загрозою перебувають члени сім'ї журналістів, адже інформація про них може стати підґрунтям для тиску на журналіста з метою публікації певної інформації.

Під час воєнного стану відбувається посилення боротьби з корупцією, ненавмисні наслідки чого негативно позначаються на роботі медіа. Оскільки відповідні злочини можуть бути кваліфіковані як державна зрада, істотно **посилюється тиск на журналістів та громадські організації**, що займаються, зокрема, боротьбою з корупцією. Зокрема поширеною є практика погроз журналістам через анонімні телеграм-канали. Наявність тиску та підвищення рівня небезпеки з боку зловмисників призводять до **посилення самоцензури** серед журналістів: розуміючи, що публікація певної інформації може спричинити особисті проблеми, деякі журналісти відмовляються проводити / доводити до кінця відповідні розслідування.

Окремо інформанти зазначали небезпеку з боку **розвитку технологій ШІ**. Так, можливості створення як тестового, так і аудіо- та відеоконтенту, дипфейків призводить не лише до зниження загальної якості матеріалів, що розміщуються в медіа, а й до конкуренції між журналістами та ШІ. Оскільки останній за один і той самий проміжок часу може створити набагато більше контенту, який матиме попит серед користувачів з невисоким рівнем медіаграмотності, журналісти в довгостроковій перспективі програють таку конкуренцію.

У цілому названі проблеми свідчать про **поступове розмиття медіапростору та дисфункцію інституту журналістики**, що несе небезпеку для репутації України та/або української армії, руйнує єдність українського суспільства, обмежує кількість належно перевіреної інформації, а відтак і можливість приймати адекватні рішення та функціонування демократії в цілому на тлі недовіри до інституту журналістики.

«Небезпеки зламу, шантаж, використання в неправдивих своїх цілях, змушування друкувати тощо. Тобто злам, хакерство — це одне, а соціальна інженерія, примушування журналістів робити якусь іншу роботу — одна з найбільших загроз».

Андрій, представник громадської організації

«Для активістів і журналістів, по-перше, це достатня необізнаність щодо функцій багатьох девайсів, неусвідомлення того, що можна в роботі, що — ні. Усе цифрується — і документи, і тому подібне. Знання, як правильно захистити інформацію, яка зберігається як на хмарі, так і на власних персональних комп'ютерах і телефонах».

Наталія, журналістка

«Пряме перешкоджання журналістської діяльності. Що більше буде випадків, де викриватимуть інформацію, викрадати персональні дані з будь-якою метою (...), то частіше журналісти, які займаються якоюсь своєю справою, думатимуть десять разів, чи потрібно їм публікувати матеріали, наскільки вони взагалі є захищеними у своєму середовищі й що в принципі проти них можуть вчинити звичайний кіберзлочин. Він наче й не несе дуже великої шкоди, але по факту проти них багато чого можна буде використати».

Дмитро, журналіст

«Є загроза, що вони отримують неправдиві відомості, вірять у них, роздмухують якісь спеціальні протидержавницькі настрої, що загрожує суспільству в цілому. Це руйнує єдність, тому що зараз дуже нестійка психіка в багатьох людей (...) І дуже складно переконати потім, що це, наприклад, був фейк або спотворена інформація».

Юлія, журналістка

«З'явилися інструменти, штучний інтелект, який дає змогу не тільки дискредитувати, але й переписувати тексти, змінювати та створювати дипфейки. Дуже багато інструментів не просто дискредитують, а й замінюють роботу журналіста. Тобто там, де журналіст буде довго писати й перевіряти статтю, ми за допомогою штучного інтелекту згенеруємо відео, голос, текст — і за годину-дві є будь-яка дипфейкова новина, на яку журналіст міг би витратити довгий час. Тобто створення великої кількості неправдивої, іпсошної інформації й заміна журналістів. Небезпека в тому, що журналіст може одну-дві-три новини грамотних написати за день, а штучний інтелект — двадцять і задавити кількістю».

Андрій, представник громадської організації

До **сенситивної інформації**, якою цікавляться зловмисники, опитані передусім відносять особисті дані журналістів, за допомогою яких можна відстежувати їхні дії. Окрема категорія такої інформації — дані про рідних та дітей, які можна використати для кіберцькування та шантажу з метою здійснення тиску та впливу на їхню діяльність.

Часто зловмисників, передусім росіян, цікавить **доступ до робочої системи та ресурсів медіа**. З початку повномасштабного вторгнення журналісти неодноразово фіксували спроби зламу ресурсів з метою захоплення медіа, а також пропозиції передачі прав на домени, сайти, що свідчить про намагання поширювати певні наративи серед аудиторії, яка вже довіряє цьому медіа.

Окрім можливості транслювати наративи, зловмисників може цікавити **інформація про персональні дані**, фото, відеоматеріали щодо героїв медійних сюжетів: військових, зокрема дані щодо пересування військ, їхніх родичів, полонених, жителів прифронтових, деокупованих та окупованих територій та їхніх рідних; інформаторів, налагодження стосунків з якими могло тривати багато років; закордонних колег, а також фігурантів кримінальних злочинів, щодо яких журналісти проводять розслідування. Деякі медіа збирають та зберігають інформацію про злочини росіян та про рух їхніх коштів, що в майбутньому може стати частиною доказової бази обвинувального вироку. Відповідно російські хакери докладають багато зусиль для зламу, отримання доступу та знищення таких даних. Окрема проблема — потенційна небезпека ідентифікації героїв сюжетів, які перебували в окупації та мають рідних, що залишись в окупації. Тому журналісти зазвичай покладають на себе велику відповідальність за безпеку людей і водночас підвищують власну вразливість перед наслідками зламування акаунтів та витоку інформації.

«... ми втратили величезну частину архіву якраз часів 2022 року. І відновити це вручну в повному обсязі, як було тоді заархівовано, практично неможливо. Вони знищували те, що може свідчити про їхні гроші. Для них це питання життя і смерті, якщо буде суд, я маю на увазі якийсь міжнародний. (...)

Якщо ми говоримо про внутрішніх зловмисників, які зацікавлені в дискредитації конкретних авторів, то я знаю про багатьох колег, які заявляють про свободу слова, своє право на професію, про те, що не може бути жодної цензури, яка прикривається певною воєнною цензурою, а насправді є просто політичною цензурою. Вони потерпають від нападів, від дискредитації, від поширення брехливої інформації чи персональної, і це відбувається неодноразово».

Марина, журналістка

Сприйняття інформантами **актуальності загроз цифрової безпеки** для їхньої організації залежить, по-перше, від ідентифікації зловмисників, які несуть цю загрозу, по друге — від усвідомлення масштабу та потенційних наслідків власної професійної діяльності. На думку опитаних, їхній цифровій безпеці найчастіше погрожують особи, пов'язані з росіянами, тому в умовах війни вони усвідомлюють загрозу від небезпечного ворога. Про особливу небезпеку зазначають організації та медіа, які знають, що вони наділені номінацією «терористичної організації» та/або отримують фінансування з джерел, пов'язаних з американськими організаціями, зокрема неурядовими. Водночас рівень загрози оцінюють згідно з масштабом діяльності, яку веде організація. Так, якщо медіа діють на локальному (обласному) рівні, зазвичай представники цього медіа вважають, що не становлять інтересу для російських спецслужб. Красномовним винятком є медіа, чия діяльність охоплює територію, близьку до зони бойових дій. Внаслідок намагання «зачистити» там інформаційний простір, особливо під час перших місяців повномасштабного вторгнення, агресор намагався зламати ті медіа, які базувалися й освітлювали події на окупованих територіях, прикордонних регіонах та в зонах бойових дій.

Інша загроза, яку називають деякі медіа, які ідентифікують себе як опозиційні, — українська політична влада. Деякі інформанти зазначали, що мали справу зі встановленням прослуховування, імовірно, з боку українських спецслужб. Причому це було зроблено протягом останніх двох років, тобто після повномасштабного вторгнення, а не раніше.

«Звісно, цікаві. Ще до вторгнення я був ідентифікований російськими спецслужбами як ворог і мені намагалися зламати багато разів інстаграм, фейсбук, gmail. Відповідно вони хотіли отримати сто відсотків доступу до моїх персональних даних, якихось моїх листувань і, можливо, знищити мої соцмережі, тому що були атаки ботів, які намагалися деактивувати, наприклад, інстаграм».

Андрій, журналіст

«Атакують найактивніших. Або чим більше коло людей чи зачіпаєш, тим більше атак на тебе організовують. Оскільки ми не є гігантським ЗМІ, так би мовити, і завдаємо удари по корупції точково — на місцевих чиновників, то і відповідь отримуємо регіонального рівня».

Володимир, представник громадської організації

«Ми — медіа місцевого формату. Описуємо, звісно, і створюємо ті сами відеоновини на сайті всеукраїнського формату, де розповідаємо про злочини посадовців або тих, хто, умовно кажучи, визнані винними у зраді. Звісно, це для них теж погано, але не думаю, що ми можемо нести для них велику загрозу і вони захочуть з нами поквитатися».

Дмитро, журналіст

«Були ситуації, пов'язані з тиском на наших журналістів. Була "прослушка" у Віталія Портнікова вдома виявлена; незрозуміло, хто її поставив, але найімовірніше, що це наша влада зробила. Була історія, коли наймані пропагандисти влади дискредитували наших журналістів, наш телеканал. Тобто це реальна ситуація, яка сталася тільки за останні два роки, а до того схожого не було».

Андрій, журналіст

У цілому інформанти здебільшого оцінюють **імовірність втрати / витоку інформації**, з якою працюють, як середню. Під час глибинних інтерв'ю неодноразово лунала думка про те, що зловмисники завжди мають можливість зламати будь-які бази даних, тому імовірність зламу залежить, з одного боку, від того, чи перебуває медіа в полі зору спецслужб, з іншого — від ступеня захищеності. Один респондент підсилював цю тезу, посилаючись на наявні російські інформаційні ресурси, створені за допомогою ШІ, для пошуку інформації про різних осіб, присутніх в інформаційному просторі, зокрема в соціальних мережах. Тому він пропонував актуалізувати не так питання захисту даних, як розуміння того, як викрадена інформація може бути використана проти самих медіа.

Представники загальнонаціональних медіа частіше повідомляли про те, що вживали додаткових заходів з цифрової безпеки, завдяки чому змогли підвищити рівень безпеки до середнього. Утім, водночас цей рівень не може стати високим через зацікавленість зловмисників як з боку рф, так і з боку представників української політичної влади. Натомість локальні медіа частіше апелювали до незацікавленості російських (у випадку опозиційних медіа — українських) спецслужб до їхньої діяльності.

«Для нашої організації загрози є високими, тому що наші акціонери не частина влади, а скоріше — критики. Ми займаємо чітку проукраїнську позицію, тому і зовнішні вороги нас можуть не любити, намагаються дискредитувати. Це сумарно робить з нас компанію під подвійним ударом: тут і внутрішньополітична історія, і зовнішня».

Андрій, журналіст

«У цьому плані протизаконним ми нічим не займаємось, тому турбуватися сильно нема чого. Протизаконної діяльності немає. Наша інформація не є такою критичною. Якщо в нас були б якісь глобальні масиви тощо, тоді була б загроза».

Володимир, представник громадської організації

Частина інформантів з медійних та громадських організацій мали **досвід проблем з цифровою безпекою**. Найчастіше опитані називають DDoS-, фішингові атаки, блокування сторінок у соціальних мережах через численні скарги ботів, злам доступу до сторінок в соціальних мережах, адмінпанелей сайту та телевізійних комунікацій, вірусні атаки, спам ботів у коментарях до постів у соцмережах та месенджерах. Одна інформантка повідомила про злам сторінки інформаційного агентства, що призвело до знищення цифрових архівів, зібраних журналістами. Здебільшого організації у відповідь на такі злами проводять відповідні тренінги для персоналу, посилюють вимоги до паролів, обмежують доступ до адмінпанелей сайту, відновлюють акаунти та створюють нові. Багато інформантів зазначають, що їхні колеги часто не хочуть особливо заглиблюватися в проблеми цифрової безпеки, тому покладають відповідальність на представників технічних відділів компаній.

«Дуже важливо, коли в медіа (...) є людина, яка профільно технічно може оперативно усунути проблему в плані злому, або, якщо потрібно, терміново обмежити доступ до акаунту. Така людина все-таки технічно швидше це зробить, ніж просто журналіст або редактор».

Дмитро, журналіст

«Один з прикладів: у нас у Новоселицькому районі за допомогою фішингу зламали доступ до сторінки у фейсбуці. (...) Когось одного зламали, навіть ніхто не знає як, і залишили там непристойний контент. П'ять тисяч людей, районний ЗМІ, а вони поширюють там непристойне».

Юлія, журналістка

Опитані вважають, що майже всі **загрози для інформаційних ресурсів залишаються актуальними**: витік персональних даних, що може спричинити, зокрема, дискредитацію медіа через публікацію особистої інформації; створення фейкових каналів у соціальних мережах та месенджерах, що мімікрують під справжні; конструювання якісних дипфейків, GPS-трекінг, прослуховування та зовнішнє спостереження, масовані DDoS-атаки та робота з дискредитованими соціальними мережами й медіа.

«Ситуації просто проговорені, і насправді вони проговорені на помилках. Тобто, коли ми стикаємося з такими кейсами, то поширюємо цю інформацію для інших редакцій, щоб вони цих помилок просто не повторювали».

Гаяне, журналістка

«Гігієну доступу не всі розуміють. Прості тренінги з журналістами ми проводимо з інфогігієни. Зайшли сюди, клікнули сюди, подивилися те, налаштували те — така проста інфогігієна, що вони не розуміють, що можна тут покласти двофакторну, наприклад. Хтось розуміє, а хтось — ні. Говоримо про доступ до персонального акаунту, до робочих акаунтів. Тобто це стосується такої інфогігієни».

Андрій, представник громадської організації

«Нам здається, що ми убезпечили доступ до пошти, випрацювали в організації внутрішні правила користування і спілкування месенджерами. Але недостатньо знань щодо ютубу і сайтів. Через брак ресурсів ми також не можемо зробити доступ безпековий, оцінку ризиків щодо існування сайтів».

Наталія, журналістка

«Які були, такі й залишились, — ризик атаки, фішингу. Єдине, що я зараз розумію, — те, що розширилось коло й ризик збільшився. Тобто раніше був умовний зловмисник на 100 людей, а зараз він уже на 10 людей».

Володимир, представник громадської організації

Усі інформанти відзначають **актуалізацію викликів в умовах повномасштабної війни**. Майже всі повідомляють про неготовність до них, що спричиняє необхідність реагувати. У відповідь на підвищення ризиків та на досвід безпосереднього зіткнення з загрозами організації опанували нові інструменти, пов'язані з інформаційною гігієною:

- ввели нові перевірки, тестування, тренінги щодо реагування на отриману інформацію через електронну пошту та месенджери;

- посилили вимоги до зміни паролів, запровадили регулярність (у деяких організаціях — що два тижні);
- перейшли на корпоративне листування через відповідну електронну пошту, що убезпечує дані у випадку зламу особистої пошти;
- припинили частину доступів до адмінпанелей сайтів (передусім для осіб, які опинились на окупованій території), почали постійно оновлювати сайти.

Цікаво, що деякі організації говорять про посилення заходів безпеки, посилаючись на протилежні заходи. Так, представник однієї з організацій повідомив про обмеження можливості дистанційно заходити в адмінпанелі сайтів та їхню прив'язку до офісної техніки; представниця іншої організації — про запровадження дистанційного доступу до серверів, що згодом дало змогу працювати в умовах вимкнень світла. Лише деякі інформанти оцінюють готовність своєї організації як високу або через те, що почали запроваджувати зміни до 2022 року, або через практику регулярно звертатися до спеціалістів з цифрової безпеки з проханням проводити відповідні аудити.

«Ніхто не готовий до змін у цифровій безпеці, тому що будь-які зміни в компанії викликають спротив колективу і це завжди час. Тобто мало змінити й сказати: "Тепер працюємо по-новому". Треба ще людей навчити, супроводжувати ці зміни, розв'язувати проблеми, які виникають, тому що можуть траплятися якісь злами тощо. Не тому, що хтось зловмисний, а тому, що це нова система».

Андрій, журналіст

«Ми зробили жорсткішою систему зміни паролів. Вони змінюються раз у певний період, а не коли ти створюєш пароль, і він в тебе три роки один і той самий. Заборонили тримати всі паролі вкупі, тому що коли відбувся злам, велика частина персональної інформації потрапила назовні тому, що вона зберігалася в тої людини від наших програмістів, які цю інформацію тримали чомусь на своєму компі. Ми заборонили так робити. Пароль кожного — це пароль кожного, а не зібрані в одному файлі всі паролі від усіх компів, які тільки є в компанії. Тому ми зробили жорсткішими ці правила».

Марина, журналістка

«У нас був кейс у Луганській області, коли редакцію забрали в підвал і єдиним доказом того, що в них немає доступу до сайтів, було те, що ми продовжували ці сайти оновлювати. І вони кажуть: ну дивіться, ми з вами тут сидимо, а сайт оновлюється, у нас типу немає ніяких прав, у нас все забрали. І це фактично тоді врятувало їх, і вони змогли потім виїхати з окупації. Тобто з цими доступами ми дуже оперативно тоді спрацювали — і це було дієво».

Гаяне, журналістка

«Ні. Я можу скільки завгодно говорити, що я про це думав побутове, але... Бо я не уявляю, як можна до цього підготуватися максимально добре... Людина — це така істота, у якої постійно якісь емоції. Десь щось забув, десь на щось не звернув уваги — це абсолютно людський фактор. Мені було складно передбачити абсолютно всі ймовірні варіанти, сценарії, ризики... Ми не знаємо, де щось впливає, де щось виникне».

Олег, представник громадської організації

2. ПРАКТИКИ ОСОБИСТОЇ ЦИФРОВОЇ БЕЗПЕКИ

Через залученість усіх користувачів до різних осередків єдиної комунікаційної мережі стан цифрової безпеки організації прямо **залежить від особистих практик інформаційної гігієни** її працівників.

У цілому інформанти зазначають, що **ознайомлені з базовими правилами цифрової безпеки**. Найчастіше серед таких правил вони називають ті, що пов'язані з паролями для програм, сервісів та застосунків (електронна пошта, соціальні мережі, месенджери, адміністративні панелі сайтів тощо; генерація паролів, зокрема за допомогою програм-менеджерів, двофакторна авторизація), а також обережність під час отримання повідомлень електронною поштою або в месенджерах. Лише деякі опитані до визначеного переліку додають такі заходи: використання антивірусів, VPN; створення резервних копій інформації; ознайомлення з технічною документацією під час встановлення програм (здебільшого вибіркове), використання ліцензійних програм, запобігання завантаження документів на пристрої, не пов'язані з сервером організації, та перенесення роботи винятково до інтернет-простору.

«Щодо програм, то щоб почистити комп'ютер щось є, але якраз цього бракує. У мене всі адміністратори віддалено працюють, і їм особисто привезти комп'ютер — це проблема. (...) І ще головне: усі розказують, що нам допомагають різні організації тощо, а от тим не можна користуватись... А чим тоді можна? Те, чим можна, коштує грошей. Допоможіть тоді. Або безплатно такі програми встановіть, або оплатіть ці безпечні програми, щоб їх встановити... Усе залишаємо на потім — зроблю потім, встановлю потім, — а минає рік, а нічого так і не зроблене. Треба якийсь контрольний тиждень мати. Щоб, наприклад, комп'ютер добре почистити, треба хоча б два тижні. Якщо самостійно. А якщо це роблять фахівці, то пів дня, день витратити і гроші».

Володимир, представник громадської організації

«Особисто, час від часу. Коли в когось проблема, одразу починаєш звертати увагу й дивитися, що в тебе в цій сфері робиться».

Наталія, журналістка

«Усе-таки іноді не має сил, бажання. У мене стоїть антивірус, паролі подвійні надійні. Я використовую ліцензійні програми. Стараюсь не постити особисту інформацію в соцмережах, але все одно іноді буває».

Юлія, журналістка

«Так, воно інколи бісить, особливо коли це нагадування змін у паролі. А коли Google раз на два тижні викидає з акаунту, і знову пароль вводити, це трошки напружує, але ти розумієш, навіщо це і що це твоя безпека. Роблю так не завжди, але останнім часом частіше».

Дар'я, журналістка

Попри усвідомлення обмеженості власних знань щодо заходів цифрової безпеки, лише частина інформантів відзначає, що повністю дотримується їх. Серед **причин недотримання відповідних правил** опитані частіше називають такі:

- порушення звичного способу життя та роботи, що на початку змін призводить до відрази, відчуття браку сил та часу (особливо під час появи нового сервісу чи соціальної мережі) та посилюється необхідністю постійно моніторити зміну ліцензійних угод, які відбуваються під час оновлення програм та застосунків, а також проблемами переходу до менш зручних програм (передусім незвичних месенджерів);
- брак мотивованості, посилений відсутністю ідентифікації себе як потенційної жертви зловмисників через локальну обмеженість діяльності організації;
- брак фінансування на програми, які забезпечують більш надійний цифровий захист;
- виникнення технічних проблем зі згенерованими складними паролями через вимкнення електроенергії та збої в операційних системах гаджетів.

Натомість експерти та представники громадських організацій частіше говорять про найбільшу складність саме першого етапу переходу до застосування нових правил та подальше посилення відчуття безпеки, адже дотримання базових правил не потребує набагато більше часу та зусиль.

«Бо фізично не встигаю. Неможливо. Багато обов'язків. Якщо чесно, не дотримуюсь часто. Коли оновлення тих правил, які присилають Google чи інша програмка, треба перечитати, що вони змінюють в політиці конфіденційності, але часу немає. Інколи особисте змішується з робочим і тому не дотримуюсь правил».

Андрій, представник громадської організації

«Зараз, в умовах вимкнень світла, в мене коли заглючив телефон, це була прямо трагедія, тому що на ньому була зав'язана двоетапна ідентифікація, а він перестав працювати. І ти зі зламаним апаратом практично втратив зв'язок з усім — з поштами, месенджерами — і просто став поза зоною. Тому хочеться все-таки мати в голові цю інформацію, а не десь в пристрої на 16 знаків — великих і маленьких, від спеціальних і так далі історій. Тому з цим складно».

Марина, журналістка

«Ми всі знаємо, що телеграмом не варто користуватися, але це зручно, ним твої контрагенти, друзі користуються, і на роботі теж. У результаті телеграм використовує багато людей, хоча це й недобре. Багато в нас таких історій. Те саме й про інші речі, складні паролі наприклад. Іноді ти думаєш, що створиш складний пароль складний, забудеш його, тож краще створити новий. Або створюєш складний, записуєш десь на папірці, а потім все одно виявляється, що це не той рівень захисту. Ти той папірець, щоб не загубити, все одно кладеш собі в кишеню, наприклад, або в гаманець, і він там поруч з карткою лежить, і це вже неправильно з погляду цифрової безпеки».

Андрій, журналіст

«Доволі складно упровадити, бо це порушує якийсь звичний спосіб життя на початках, але з досвіду свого і з досвіду всієї організації це навпаки дуже зручно, коли ти використовуєш менеджер паролів, де тобі не треба їх ні запам'ятовувати, ні записувати. Коли ти маєш двофакторні автентифікації, ти одразу бачиш, коли хтось намагається зламати твої профілі. Маючи окремі фінансові номери й електронні пошти для банкінгів, різноманітних акаунтів, ти просто почуваєшся набагато безпечніше... Це потребує часу, коли ти тільки починаєш з цим працювати. Але потім усе одно йде просто вже по накатаній, стає дуже зручно. Мені здається, що на перспективу це про оптимізацію, а на момент впровадження, звісно, складно, особливо коли в тебе велика редакція й тобі треба кожного проконтролювати. І люди не завжди хочуть робити додаткову роботу, що також нормально. Але з огляду на фідбек і те, що ми маємо зараз, люди навпаки задоволені».

Віталій, представник громадської організації

Опитані журналісти відверто зазначають, що найбільше їх дратує необхідність створювати різні паролі для різних сервісів і регулярно змінювати їх. Попри це, у цілому серед них найбільш поширена думка про те, що правила цифрової безпеки не є надмірними з огляду на ризики втрати соціального капіталу, який є ключовим для медіаполя.

Деякі інформанти звертають увагу на те, що сервіси, якими вони користуються в повсякденні (соціальні мережі, поштові послуги тощо) часто потребують, на їхній погляд, зайвої інформації, що підсилює ризики. До того ж частина застосунків, якими опитані користуються в повсякденні, не видаються їм такими, що мають підпадати під суворі правила цифрової безпеки. Відповідно одним зі **слабких місць в організації особистої інформаційної безпеки** видається те, що журналісти несвідомо розмежовують сервіси, які необхідні для професійної діяльності, і ті, які вони використовують у вільний час (здебільшого розважальні).

«Базові правила невитратні взагалі, тобто ти просто приймаєш для себе якісь правила і за ними комунікуєш. А коли реальна проблема вже стається, то тут теж дуже індивідуально ... Я ж кажу, інколи атаки тривали один день, а інколи... після місяця ми не могли поновити. Тобто залежить від кейсу... Тут я не зможу узагальнити. Здається, більшість базових правил — раціональні й допомагають підвищити власну безпеку. І сказати, що щось є зайве, то, напевно, ні... З огляду на наш досвід, усе одне й те саме. Робочі пристрої й особисті. Люди користуються ноутбуком і телефоном як для роботи, так і для особистих цілей. Дуже рідко коли буває, що в людини є окремо робочий ноутбук, а окремо — особистий планшет. Зазвичай це змішано, і тут однакові правила для обох пристроїв мають бути».

Гаяне, журналістка

«Дуже багато сервісів, які насправді не несуть складної інформації, тобто вони не стосуються якоїсь персональної інформації. Застосунок для вивчення англійської мови, наприклад. І він вимагає створювати якісь суперскладні паролі. Я вважаю, що то занадто. Розробники окремих застосунків просто беруть якісь стандартні правила і з ними працюють. Ще занадто, коли дуже часто вимагають персональну ідентифікацію, яку нема сенсу про себе давати. Навіщо? З чим я востаннє стикався — просили паспорт на пошті чи десь. Я не дуже розумію, навіщо поштовому оператору знати, хто я персонально є. Це вже якесь особисте життя. Я замовляю щось з інтернет-магазина... А пошта хоче мене ідентифікувати. Вона бачить відправника, отримувача, і відповідно вже у неї така є Big Data, і вона її може продавати. Те саме з соцмережами, які збирають про нас інформацію. Ми їм віддаємо цю інформацію самостійно, але іноді її забагато. Наскільки я знаю, TikTok збирає купу інформації з людей, яку він міг би не просити».

Андрій, журналіст

Наявний рівень заходів безпеки інформанти у цілому сприймають як достатній. Лише деякі зазначають, що можливо посилити захист або технічно (встановити додаткові антивірусні програми, використовувати ліцензійні програми для оброблення аудіо- та відео-), або шляхом поширення правил інформаційної гігієни серед широкого загалу. Оскільки часто злам відбувається через соціальні мережі шляхом надсилання повідомлень від контактів, які, як правило, не пов'язані з інформаційною діяльністю та не застосовують відповідні правила, щоб посилювати безпеку, важливо створювати відповідне захищене інформаційне середовище.

«Таких застосунків багато, і кожен собі може встановлювати, які йому подобаються. Тобто вони не зайві. Програма дає змогу відключити антивірус, який у вас є, або якийсь інший програмний продукт. Тобто це потрібно. Якщо не хочете — не встановлюйте. Якщо боїтесь за безпеку — встановіть антивірусник чи ще щось».

Андрій, представник громадської організації

«Як на мене, мало популяризації цього всього. Тобто є лише групи людей, які пропонують навчання, і зацікавлені фірми, які ці навчання приймають. А якщо ми говоримо про навчання суспільства загалом, то якраз бракує інформації про те, що добре, а що погано; про те, наскільки емоційно забарвлені новини можуть бути фейками й так далі. Мені здається, що така інформація зосереджується якраз в спільноті, яка це не практикує. Так, інформацією про розвінчання фейків володіє досить обмежене коло людей, а широке коло громадян, яке потребує цих знань, залишається необізнаними. Тобто якщо інформацію поширюють, наприклад, у фейсбуці, а людина цим не цікавиться, то фейсбук це просто їй не покаже. Це має бути якась ширша кампанія державного рівня, коли людям на зупинках на плакатах будуть пояснювати покроково, що робити, коли вам дзвонить незнайомий номер і говорить вам щось про вашу кредитну картку».

Марина, журналістка

3. СТАН ЦИФРОВОЇ БЕЗПЕКИ В ОРГАНІЗАЦІЯХ

Частина інформантів повідомила, що в їхній організації **немає окремої політики щодо цифрової безпеки**. Формалізована відповідна політика частіше зустрічається в медіа всеукраїнського рівня, натомість лише в одній локальній організації повідомили про її наявність. В інших організаціях спеціальної політики немає, однак вживають окремих заходів щодо впровадження елементів цифрової безпеки. Дослідження засвідчило наявність різних **форм ознайомлення працівників з правилами цифрової безпеки**:

- безпосереднє спілкування служби безпеки з окремими департаментами (підрозділами) організації та/або системними адміністраторами;
- ознайомлення співробітників з основними правилами під час онбордингу;
- регулярні тренінги та інструктажі з інформаційної безпеки (як внутрішніх, так і зі спеціальними громадськими організаціями);
- розсилка інструкцій через організаційні канали комунікації (як одноразова, так і регулярна).

Зазвичай правила інформаційної безпеки обмежують базовими інструкціями щодо поведінки з ресурсами та сервісами, з якими працює організація. Менша частина інформантів повідомила про наявність в їхній організації посилених правил безпеки, які містять протоколи реагування на випадки зламу акаунту, серверу тощо, обмеження доступу до ресурсів організації, правила щодо оголошення зборів від інших громадських організацій та благодійних фондів, обмеження роботи з персональних комп'ютерів, наявність дублювальних хмар інформації та закритих серверів.

Частина організацій має **відповідну службу безпеки**, якій делегована діяльність щодо запобігання зламу цифрової безпеки та реагування на відповідні випадки. Лише деякі організації намагаються поєднати заходи з технічних та соціальних (організаційних, особистих) аспектів цифрової безпеки.

«ІТ-служба цим опікується. У нас є певні захисні механізми, договори, хмари, які дублюють інформацію; є закриті сервери, куди ми завантажуємо застарілу інформацію. Тобто в нас ціла система захисту... Якщо ти працюєш з ноутбука, то маєш принести його на роботу, і вони встановлюють цей доступ».

Юлія, журналістка

«У нас є люди, які займаються безпекою, тобто вони говорять як про безпеку фізичну, так і про безпеку цифрову... Це офіцери з безпеки фактично. Вони є і в наших закордонних офісах, і тут. Вони про це дбають, розсилки роблять, є обов'язкові тренінги, які треба проходити, про що дбають менеджери команд».

Владислав, журналіст

Окремою вразливою ланкою цифрової безпеки є особисті пристрої працівників. Дослідження свідчить, що лише деякі організації вживають окремих заходів щодо цифрового захисту приватних пристроїв, з яких можна мати доступ до робочих матеріалів. Серед таких заходів інформанти називають допомогу зі встановленням VPN-сервісів, ідентифікацію особистого пристрою через IP, створення захищених серверів інформації з обмеженим правом доступу, інсталяцію захищеного софту та антивірусів на кожний девайс працівника.

«Не до всіх є доступ. До критичних — ні, але до деяких є. В принципі просто навіть коли пишеш звичайну статтю, ти ж все одно її пишеш спочатку в Google Docs чи деінде. Не можна мати доступ до робочих чатів з персональних пристроїв. Було б ідеально, звісно, щоб у людини був робочий пристрій окремо, а персональний — окремо, але, на жаль, ми не можемо забезпечити всім нашим працівникам купівлю комп'ютерів, щоб вони вдома ними користувалися суто з робочою метою. Оскільки вже люди використовують власні комп'ютери для роботи, засуджувати їх за те, що вони ще й персональні дані там мають, ми не можемо. Тому деякі працівники працюють з персональних комп'ютерів і виконують робочі завдання. Особливо це SMM стосується. Є телеграм-канал з новинами, які ми робимо. Не відмовилися поки від цього, хоча думаємо періодично».

Андрій, журналіст

«Ніяк компанія не захищає, просто вона мені дає рекомендації, і я дотримуюсь їх. Наприклад, рекомендацій для ноутбука робочого я дотримуюсь і під час використання власного домашнього телефона. Хоча власний — це дуже відносно, бо я його використовую і для роботи. Двофазна авторизація для всіх облікових записів. Це ж і робочі, і неробочі записи».

Юлія, журналістка

У багатьох організаціях **немає визначених сервісів для комунікації**. У великих компаніях працівники можуть користуватися як корпоративною поштою (найчастіше згадували саме цей засіб зв'язку), Google Drive, так і різноманітними месенджерами, що створює додаткові проблеми та загрози. Серед месенджерів інформанти частіше називають Telegram (водночас наголошуючи на розумінні ризиків, пов'язаних з походженням цього ресурсу) та WhatsApp, рідше — месенджери Facebook, Signal, Slack. Лише в деяких організаціях поділяють комунікацію на робочу, що передбачає залучення документів (здебільшого через корпоративну пошту), та неробочу (через месенджери).

Окремі опитані повідомили про використання захищених систем електронного документообігу. Небажання переходити до більш захищених сервісів спілкування пов'язане зі зручністю (необхідність пересилати великі обсяги інформації, зокрема фото- та відео-, обмежує коло сервісів; комунікація з працівниками, які можуть перебувати, зокрема, на окупованій території, призводить до намагання полегшити способи комунікації) та коштами, необхідними на користування ними.

«Якось історично склалося, що, наприклад, телебачення користується вотсапом, а сайт — телеграмом, а для інших потреб використовують пошту. Тобто немає єдиного рішення, що компанія працює тільки ось у цій системі. І через це, звісно, загрози. І це незручно для людей, які взаємодіють з різними підрозділами компанії».

Андрій, журналіст

«Воно відбувається в багатьох месенджерах. Але це пов'язано зокрема з тим, що будь-які з цих месенджерів можуть впасти, тому є дублювання. Ми користуємося фейсбучним месенджером, вотсапом і телеграмом для спілкування. Телеграм мені не подобається як місце спілкування, але він найкращий з погляду передачі великих масивів відеоінформації, адже не стискає її так, як фейсбук, тому ми його використовуємо для виробничих питань. Ми намагалися перейти на якісь платні сервіси спілкування в компанії, типу Trello або Slack, але покористувавшись ними в пробній безплатній версії, зрозуміли, що для нашої великої компанії це задорого, й відмовились. Тобто реально це велика сума, щоб перевести 300 осіб для спілкування в Trello і платити щомісяця там сотні доларів за користування».

Марина, журналістка

«Є довіра до WhatsApp. Telegram я теж користуюсь. Це швидше таке компромісне... Я змирився з цим, тому що розумію, що багатьом людям, зокрема на окупованій території, максимально простіше в багатьох випадках саме використовувати телеграм-зв'язок, особливо в умовах нестабільного інтернету, в умовах окупації тощо. Я ніяк не можу на це вплинути. Поки люди використовують цей засіб комунікації, я буду його використовувати. А Viber меншою мірою, але теж з тієї самої причині. Тобто я взагалі використовую будь-які месенджери, засоби комунікації, але більше довіряю WhatsApp. І, власне, переважна комунікація робоча відбувається через WhatsApp, частково через Signal і частково через месенджер Facebook».

Олег, представник громадської організації

За словами опитаних, в їхніх організаціях працівники зазвичай **знають про алгоритми захисту від фішингу**. Частина інформантів зазначила, що дізнається про такі правила під час тренінгів, які проводять або сама організація, або організація-партнер, що спеціалізується на цифровій безпеці. Менша частина респондентів не ознайомлена з такими алгоритмами, тому розв'язує проблеми з фішингом під час консультацій з відділом безпеки або з представниками організацій-партнерів, що зазвичай призводить до зайвих витрат часу. Знання щодо засобів запобігання фішингу здебільшого зводять до того, щоб не надавати особистої інформації (адреса електронної пошти, номер телефону) на сайти, які підозрюєте в ненадійності, а також уникати листів, які приходять від невідомих контактів.

Про користування віддаленим робочим столом інформанти повідомляли рідко, зазвичай така практика спостерігається в окремих відділах великих організацій. Опитані, які чули про таку можливість, але не скористалися нею, розповіли про побоювання щодо вразливості відповідного сервісу, ширшу практику його використання в комерційних підприємствах, а також про оцінку уваги зловмисників до їхньої організації як низьку через локальний рівень її діяльності.

Про складання матриці загроз повідомили лише деякі інформанти. В окремих випадках мова про виконання відповідної вправи під час тренінгу, а не про використання на рівні організаційного заходу.

«Ми просто попереджали, щоб не переходили за посиланнями. Більшість журналістів, які з нами працюють в команді агенції, розуміють, що це фішинг, і нікуди не переходять. Ті редакції, з якими ми співпрацюємо як партнери, якщо сумніваються, завжди можуть кинути нам скриншотик в редакційний чатик і спитати, що це таке».

Гаяне, журналістка

«Як не переходити, що є загрозою, що перевіряється — такі загальновідомі речі знають. Якщо на пошту приходять листи з незрозумілими темами, яких ми їх не очікуємо, то їх ніхто не відкриває. Для цього є спеціально навчена людина, яка їх перевіряє на наявність загроз. Тобто ніхто не відкриватиме листи не на тему або коли незрозуміло, від кого цей лист надійшов».

Наталія, журналістка

«Єдине, що там ці боти, тобто за ними стоять реальні люди, просто підписані іншими ніками. А з іншого боку, якщо заблокують, почнеться атака ботів така професійна, я не хотів би з цим зіткнутися. Тобто загальне уявлення, як цьому протистояти, в мене є, але як воно на практиці й у критичній ситуації буде — я не знаю. Єдине, що я зрозумів, що контрзаходи протягом 24 годин мають бути впроваджені. А якщо в цей момент ти не був взагалі на сайті? (...) Я знав про цей віддалений стіл, комп'ютер ще, мабуть, років п'ятнадцять назад, я розумів, що це дуже зручно, але я бачив в цьому і зворотну сторону медалі, що це дуже вразливо. Мені це не дуже потрібно. Я вважаю, що це рівень обласного телебачення, якщо серед ЗМІ, або крутого, дуже потужного ЗМІ».

Володимир, представник громадської організації

За організацію заходів безпеки в медійних організаціях частіше відповідають **окремі технічні відділи та департаменти**. Здебільшого їхня компетенція поширюється на організацію технічних параметрів та застосування технічних рішень, спрямованих проти спланованих масових атак. У невеликих медіа та громадських організаціях за заходи безпеки відповідальні окремі працівники: відповідний технічний спеціаліст, HR, менеджер офісу, голова департаменту або керівник організації.

Для **підвищення рівня цифрової безпеки** в організаціях поширена практика проведення тренінгів (частіше — власними зусиллями, рідше — із запрошеними організаціями, які спеціалізуються на цифровій безпеці). Зазвичай інформанти повідомляли, що відповідні тренінги відбувалися раз, рідше — що їх проводять з певною регулярністю (частіше в діапазоні від пів року до року). У деяких організаціях замість спільних тренінгів організовують індивідуальні сесії за допомогою організацій партнерів.

Думки про рівень складності таких тренінгів розділилися. З одного боку, багато інформантів відповіли, що не вважають такі тренінги складними. З іншого боку, частина опитаних повідомила, що їхнім колегам було складно відвідувати такі заходи через незацікавленість та особисту невмотивованість. Проте усі інформанти зазначили актуальність знань та підтвердили застосування отриманих під час таких тренінгів навичок. Одним з порівняно поширених способів стимулювати використання здобутих навичок є блокування доступу до сервісів з боку служби цифрової безпеки організації.

«У мене люди реєструються і слухають уважно. Ми минулого разу щось почули, щось забули, щось пропустили. Не зайве це повторювати, тому що хай і провели рік назад тренінг, але не всі будуть дотримуватися. Треба все одно нагадувати, тому що люди забувають, втрачають пильність ... У київському офісі постійно спонукають пильнувати, а, наприклад, в офісах регіональних я нагадувала б, бо часом люди не особливо заморочуються тим, щоб ті паролі міняти нескінченно чи робити резервне копіювання».

Юлія, журналістка

За словами інформантів, здебільшого їхні колеги **дотримуються правил двофакторної ідентифікації та генерації складних паролів** (проте вони не завжди регулярно змінюють такі паролі). Ті, хто не повністю дотримуються правил цифрової безпеки, зазвичай посилаються на брак, по-перше, часу, необхідного для налагодження роботи та комунікацій у більш захищений спосіб, по-друге, усвідомлення необхідності постійно підтримувати безпеку. Серед інших причин також називали розмір організації, який ускладнює уніфікацію правил цифрової безпеки, проведення регулярного навчання, моніторинг стану безпеки в умовах плину кадрів; інтенсифікує поділ організації на центральний та регіональні відділи (працівники в Києві ставляться до заходів з кібербезпеки серйозніше, зокрема, через більш свідому політику керівництва центрального відділу).

Опитані зазначають, що з рутинізацією робочих процесів відбувається втрата пильності, тому важливо регулярно нагадувати про основні правила цифрової безпеки.

«Ну зламають, ну що зробиш. Подумаєш! Як люди думають? Та в мене там нічого немає цінного. От правда, більшість моїх колег так і думають: "А що в мене там цінного? Нічого там такого особливо немає". Типу я ж паролі банківської картки не тримаю у себе в телефоні, я його просто напам'ять знаю. Все! Значить, уже безпечно».

Юлія, журналістка

На думку частини опитаних, **наявних заходів достатньо для досягнення цифрової безпеки** в цілому. Інші інформанти згадували про доречність наступних кроків, які, як свідчить дослідження, упроваджені лише в деяких організаціях:

- складання внутрішнього протоколу безпеки, що передбачає як загальні правила кібергігієни, так і способи реагування на окремі події;
- поява відділу безпеки, завданням якого був би моніторинг дотримання, наявності та впровадження автоматичних рішень з безпеки, насамперед для запобігання загрозам масових кібератак;
- збільшення відповідальності окремих працівників за власні дії;
- виділення коштів на покращення рівня безпеки сайту;
- запровадження періодичних тренінгів, на яких додатково були б розглянуті практичні кейси та потенційні наслідки недотримання окремих правил кібергігієни;
- під час проведення тренінгів акцентувати не лише на технічну, а й на психологічну сторону захисту, оскільки можливі невдачі в умовах неможливості досягнення 100% рівня захисту;
- поділ робочого та особистого цифрових просторів, зокрема робота на корпоративних (організаційних) девайсах, недопущення суміщення особистих та корпоративних застосунків на одному пристрої.

«На цих тренінгах переважно приділяють увагу технічній стороні. А треба більше — психологічній. Про неї або не згадують взагалі, бо тренінг проводить людина-технар, яка знає все про віруси, акаунти, захисти... Коли ти озброєний технічною інформацією, то тобі легше дати собі раду, але війна показала, що є випадки, коли ти ніяк не можеш вплинути, тобто, ти максимально захищений. Або твою аудиторію, людей, з якими ти комунікуєш, це не рятує ніяк, ти зробив усе як слід, але воно ніяк тебе не врятувало чи цих людей. Тобі це може бути психологічно складно прийняти».

Олег, представник громадської організації

4. ПОТРЕБИ В НАВЧАННІ ТА ПОСЛУГАХ З ЦИФРОВОЇ БЕЗПЕКИ

Хоча частина інформантів вважає, що наявної інформації достатньо й потрібно звернути більше уваги на її впровадження, інші вказали на необхідність регулярно проходити тренінги, щоб моніторити загрози, які виникають в інформаційному просторі. Відповідно **основною потребою інформантів** є підтримка наявного рівня обізнаності про інформаційні загрози, бажано з використанням матеріалів з конкретними кейсами. Лише деякі опитані мають **конкретні запити**:

- інформація про різновиди VPN;
- особливості ІПСО;
- способи розуміння того, хто стоїть за скаргами на матеріали в соціальних мережах, які спричиняють блокування сторінок організації (окрема людина, група людей, конкуренти тощо);
- способи захисту, зокрема хмарного, сайтів медіа;
- способи збереження сенситивного контенту;
- створення захищених каналів під час передавання інформації (особливо в умовах роботи на фронті);
- убезпечення від незаконного стеження, способи ідентифікації прослуховування через девайси (смартфони, ноутбуки, трекери тощо);
- особливості протоколів шифрування даних у месенджерах;
- використання ШІ для продукування фейків та способи розпізнавання дипфейків.

За словами інформантів, для тих користувачів, які лише починають ознайомлюватися з основами цифрової безпеки, доцільно використовувати формат тренінгів, під час яких вони матимуть змогу отримати відповіді на поширені запитання. За словами декількох опитаних, **онлайн-тренінги** неефективні. **Участь у тренінгу офлайн** є більш пріоритетною, бо цей формат надає можливість поставити більше запитань, дозволяє сфокусувати увагу, що є запорукою результативного навчання, а також мінімізувати наслідки вимкнень електроенергії, що може перешкодити проведенню вебінарів. Інформанти вказують, що зазвичай інші поширені формати (онлайн-курс, відеоролик, поштова розсилка тощо) дають змогу уникнути відповідного фокусування. Під час проведення тренінгів у будь-якому форматі доцільно зосередити увагу на одній програмі, використовувати домашні завдання, що разом дає змогу краще розібратися з нюансами, а також організовувати різні тренінги для різних представників організації.

«Звичайно, найкраще в офлайн-форматі, щоб одразу з прикладами, з налаштуваннями. Можна й онлайн, але в нас просто було таке навчання онлайн, і нам не сподобалось. Ми стараємось відвідувати більше офлайн-заходів, тому що онлайн все одно не так сприймається інформація».

Олеся, журналістка

«Ці тренінги можуть бути різного рівня. Наприклад, для топменеджменту — один тренінг, для технічного персоналу — більш поглиблений, а для персоналу, який творчий, — менш поглиблений. І так можна працювати з компанією. Тобто під час тренінгу для технічних працівників заглиблюватися в протоколи, частоти, забезпечення роботи під час відсутності світла, — те, чим безпосередньо опікуються технічні підрозділи. А з творчими працівниками більше говорити про захист персональної інформації та джерел інформації; безпечне спілкування з джерелами інформації — ворожими; такими, що хочуть їх дискредитувати; або просто розіграшами пранків, — щоб вони могли правильно з цим працювати».

Андрій, журналіст

Ті користувачі, які вже мають певний рівень обізнаності, частіше потребують **проведення індивідуальних консультацій**, оскільки в тренінгах зазвичай беруть участь люди з різним рівнем підготовки та запитами. Під час індивідуальних консультацій бажаним є розгляд кейсів від організації, яка звертається по допомогу, щоб на практиці застосувати знання для підвищення її рівня цифрової безпеки.

Деякі інформанти також звертають більше уваги на зручність дистанційного формату, особливо для організацій, які мають філіали в різних областях України.

«Тренінги — так. Якщо це невеликий тренінг, можна навіть онлайн робити. Тоді буде змога залучити всіх наших регіональних працівників, тобто людей, які працюють у регіонах. Можна наживо, звичайно, але мені здається, що онлайн краще. Тільки не просто розказати, що потрібно робити, а конкретно показати, як зробити підміну автентифікації, двофакторну автентифікацію. Не сказати: «Складіть складний пароль», а показати, як це зробити, й уточнити, що там має бути знак, цифра, велика літера, мала літера, латина чи ні тощо. Тобто говорити дуже конкретні речі».

Юлія, журналістка

Для всіх інформантів важливою є можливість застосовувати отримані навички на конкретних кейсах, бажано під час роботи з сервісами організації, що звернулась по тренінг / консультацію. Оптимальна тривалість тренінгів та консультацій — від 1 до 2 годин, якщо потрібно більше, варто поділити на два заняття.

Частина опитаних, які не виявили зацікавленості, кажуть про недоцільність проведення тренінгів та семінарів на загальні теми та орієнтацію на звернення до спеціалізованих організацій у випадку сформованості конкретного запиту.

«Якщо в мене буде запит, я знаю, де мені знайти цю допомогу. Але коли витрачаються шалені гроші й треба заманити людей, щоб ви прийшли до нас і повчилися, я вважаю це дурною тратою грошей. Тобто має бути піар, спрямований на те, що, будь ласка, опікуйтесь своєю безпекою, вам це загрожує, а якщо потрібна допомога — звертайтеся. А не ми вам проведемо семінар... У війну ці довоєнні методи, тренінги й семінари, дуже дратують, тому що в тебе дуже мало часу, сил, багато емоцій, а коли тебе ще й відволікають тим, що не дуже актуально наразі, тому що ми вже з цим впоралися, це незрозуміло взагалі».

Марина, журналістка

Думки щодо прослуховування подкастів розділилися. Серед тих інформантів, які зацікавилися такою формою матеріалу, поширена думка про бажаність запрошення як українських, так і іноземних експертів. До формату також не висувають особливих побажань: це можуть бути лекції, інтерв'ю, короткі серії з розкриттям найбільших небезпек та гумористичним наповненням тривалістю 3–5 хвилин.

«Коли мені потрібно закрити свої прогалини, тобто відновити щось у пам'яті, то я, якщо натикаюся на невеличкі блоги на цю тему, їх із задоволенням дивлюся, використовую».

Олег, представник громадської організації

«Кожен має свої спеціалізовані канали й просто слухає інших, де можна якусь інформацію дізнатись, насамперед навчальну, якісь практичні кейси, гайди, які можемо використати у своїй роботі. Тобто практичні кейси. Не загальні, а практичні речі».

Андрій, представник громадської організації

«Я з досвіду колег знаю, що більшість у позаробочий час точно не будуть це слухати. А в робочий час у них є інші задачі, які вони виконують. Можливо, вони прочитали б текст на якомусь медіа про медіа з порадами, але, мені здається, не всі стежать за оновленнями Медіамейкера чи Детектора. Ну і загалом ця тема, як і медіаграмотність, вважається такою нудною, не першочерговою».

Гаяне, журналістка

Послуг з цифрової безпеки потребує лише частина інформантів. Найчастіше вони згадують послуги з **аудиту захищеності** серверів, адмінпанелей сайтів, корпоративної пошти тощо. Натомість **потенційними бар'єрами** для проведення аудиту може стати високий рівень недовіри до організації, яка його проводить, а також неготовність до відповідних фінансових витрат. Відповідно потреба в зовнішньому аудиті варіюється залежно від наявної політики цифрової безпеки організації.

Окрім того, інформанти згадували потреби в залученні додаткового програмного забезпечення, зокрема хмарних сховищ, що потребує більших коштів.
Також один з опитаних згадав про актуальність можливої гарячої лінії, куди можна звернутися у разі виникнення надзвичайної ситуації, пов'язаної зі зламом ресурсів організації.

«Можливо, мати черговий дзвінок, консультацію... Може, щоб була гаряча лінія, де можна проконсультуватися щодо того, як діяти, що робити в тому чи іншому випадку».

Володимир, представник громадської організації

Опитані зустріли нейтрально інформацію про ініціативу їхнього долучення до **майбутньої онлайн-платформи**, що об'єднувала б ініціативи з цифрової безпеки. Насамперед інформанти-журналісти не зовсім розуміють доцільності своєї участі, оскільки за потреби воліють звертатися особисто до фахівців за відповідними послугами. Також один з журналістів повідомив про нібито наявність подібної ініціативи, у якій він, однак, поки не бачить істотних переваг конкретно для представників його професії.

«У якому форматі долучатися? Якщо я редакторка медіа про медіа і буду писати про ці небезпеки, тобто як висвітлювати діяльність, то можливо. А сама я не сильно займаюсь цифровою безпекою. Напевно, як активний учасник я була б не дуже корисна. Які формати могли б бути? Ті, що ми проговорили, якісь індивідуальні консультації, можливо воркшоп. Я завжди за корисне, практичне і прикладне, тому мені ці формати заходять. Але інформаційний аспект — це висвітлення нових загроз, до чого ще готуватися і з чим ще треба бути обережним».

Дар'я, журналістка

«Є прекрасна робота Національного банку України в напрямку боротьби з фінансовою безграмотністю — кампанія «Шахрай Гудбай», туди цифрова безпека теж входить, і вони вчать людей, що не можна передавати номер картки (...) Тобто запозичити цю ідею і, можливо, обрати найбільш больові точки, месенджери, наприклад, або паролі, і попрацювати з цими історіями (...) Якщо про журналістів ми говоримо, то журналістів треба вчити особисто».

Андрій, журналіст

На думку опитаних, така платформа могла б виконувати декілька функцій:

- цілодобова підтримка у випадках, коли виникає потреба запобігти цифровим загрозам;
- розміщення контактів відповідних спеціалістів, пошук фахівця з певної тематики, що зазвичай потребує істотних часових витрат;
- місце для формування навчальної програми для організацій, які хотіли б розв'язувати проблему з захистом власних ресурсів самостійно, розміщення чеклістів для перевірки стану цифрової безпеки організації;
- оперативний обмін досвідом щодо новітніх загроз, зон ризику, обмін практиками щодо способів убезпечити свою організацію;
- публікація дайджестів про тенденції у сфері інформаційної безпеки (загрози, кейси про наслідки зламів, способи визначення ресурсів, до яких небезпечно звертатися, методи розпізнання дипфейків, інформація про зміни політики соціальних мереж; софт, який допоможе убезпечити організацію тощо).

«Добре було б мати можливість онлайн-консультувань, якщо в тебе виникає якась потреба і ти знаєш, що є таке місце, де є певний фахівець з кібербезпеки, до нього можна звернутися, він тобі дасть оперативну відповідь, що робити, що не робити».

Марина, журналістка

«Обмін кейсами, обмін інформацією про те, які є зараз типи шахрайства, де зони ризику і відповідно як від цього можна убезпечитися, проінформувати співробітників, звернути увагу на цю історію. Це суто має бути якась практична історія. Обмін досвідом, обмін практиками, рекомендації, як запобігти таким речам, або якийсь терміновий alert, що це дуже небезпечно, зверніть увагу, не можна це ігнорувати».

Ігор, експерт з цифрової безпеки

Експерти з кібербезпеки виявили більшу зацікавленість до платформи. Здебільшого і вони, і журналісти висловлювали нерозуміння того, з яким напрямом така платформа працюватиме, за яких умов можна до неї долучитися, які джерела її фінансування, терміни співпраці, ступінь захищеності тощо. Кожен з цих параметрів накладає певні обмеження на готовність експертів та журналістів до співпраці.

«Може бути, але треба розуміти, як саме ми можемо долучитися і що від нас вимагають, які ресурси на це треба витрачати. Тут така дуже практична історія — що, скільки, навіщо і так далі. Якщо це повноцінний проєкт, тоді нам треба для цього людина і відповідно — фінансування. Якщо це така партнерська історія в дусі нашого чатика, то це трошки інше. Тому треба чітко розуміти, про що мова».

Ігор, експерт з цифрової безпеки

«Цікавить фінансова сторона зокрема, тобто ми маємо розуміти свій бенефіт, а не бути членами чергового об'єднання, щоб хтось класно про це прозвітував державі або донору. Це доступ до якихось безоплатних послуг міг би бути цікавий, зокрема мені, але не компанії, тому що у нас свій протокол і ми нікого стороннього не пускаємо всередину свого адміністрування. Також залежить від того, хто ініціатор цього об'єднання, його партнер; хто фінансуватиме, який термін співпраці».

Софія, журналістка

«Не цікаво, тому що вона не розв'язує наші питання. У нас є різні питання, проблеми, і ми шукаємо відповіді на спеціалізованих і тому подібних каналах. А єдина платформа не відповість на наші запитання, тому що спеціалістам із соціальної інженерії не цікаве програмування, а спеціалістам з маркетингу чи ІПСО цікаве щось інше, і вони можуть знайти це в гайдах, прикладах не в офіційних джерелах, де покажуть неофіційну інформацію. Тобто те, що нам потрібно розміщене на спеціалізованих закритих платформах, до яких доступ або платний, або внутрішній. Це специфічна журналістика, це програмування, це багато інших речей, які на єдиній платформі зібрати не можна. Це все по крупинках. Тому в нас немає потреби в єдиній платформі, але є потреби в різноманітних сервісах, які розробляють, тестуванні їх».

Ігор, експерт з цифрової безпеки

На замовлення ГО «Інтерньюз-Україна» дослідження провела соціологічна група «Рейтинг». Звіт підготували за результатами глибинних інтерв'ю з журналістами, представниками громадських організацій та експертами з цифрової безпеки.