Секретність і прозорість:
забезпечення належного балансу у сфері оборони

Вступ

Невід'ємними рисами демократії є прозорість та доступ до публічної інформації. Якщо громадяни знають, яким чином держава приймає рішення, розподіляє податки і витрачає кошти, тоді вони мають важелі впливу на уряд. На жаль, аргумент «національної безпеки» часто використовують для зловживань – щоби приховати інформацію від громадськості чи створити умови для непрозорої та незаконної діяльності. Усе це несе серйозні ризики для демократії та національної і міжнародної безпеки.

У червні 2018 року Україна прийняла новий Закон про національну безпеку, що створив основу для подальшого оновлення та розробки законодавства у цій сфері. Йдеться про реформу Службу безпеки України, а також реформу парламентського контролю над сектором безпеки та оборони. Щоб ці закони запрацювали, необхідно добре розуміти, що таке державна таємниця, яка процедура віднесення інформації до таємної, та які ризики з одного боку надмірного, а з іншого – недостатнього засекречування інформації.

Багато хто вважає, що сьогодні, коли Україна бореться за демократію і захищає свій суверенітет від збройної агресії з боку РФ, підвищення прозорості у секторі безпеки та оборони аж ніяк не на часі. Водночас, ми спостерігаємо небувале зростання оборонного бюджету й переосмислення ролі органів безпеки та громадського контролю. Саме тому зараз як ніколи важливо, щоби законодавці та експерти визначили оптимальний баланс між засекречуванням інформації, режимами секретності та громадським контролем.

Безперечно, відкритість має свої недоліки. Суворе обмеження доступу до інформації і надмірне засекречення сприяє корупції і призводить до порушень прав людини, тоді як недостатня охорона інформації, особливо під час війни, створює загрозу національній безпеці. Повне та передчасне розкриття інформації може суттєво нашкодити виконанню завдань держави, зокрема, плануванню та вибору оптимальних стратегій.

Немає держави, перед якою не стояло би завдання пошуку балансу між потребами національної безпеки та свободи інформації. Неспроможність зберегти таємницю, пов'язану з національною безпекою, може мати катастрофічні наслідки. І навпаки, надмірна засекреченість може створювати загрозу національній безпеці. Коли ж держава знаходить оптимальний баланс між прозорістю та потребами національної безпеки, це одразу підвищує довіру громадськості до державних інституцій, і як наслідок – допомагає виявляти та усувати причини корупції та конфліктів.

Тому дуже важливо, щоби держава ухвалила якісне законодавство про свободу інформації (англ. – Freedom of Information Act). За його допомогою види й порядок розкриття інформації базуватимуться на об'єктивній оцінці шкоди, яку може спричинити таке розкриття.

Національна безпека і державна таємниця – це міжгалузеві поняття, що потребують ретельного аналізу і вдосконалення. Особливо зараз, коли Україна починає працювати над реформуванням сектору безпеки і оборони, перебудовою безпекових інституцій і підвищенням ефективності демократичного контролю.

У цій роботі ми пропонуємо загальний нарис проблематики. Для наочного прикладу ми використовуємо сферу оборонних закупівель. Ми покажемо, які ризики виникають через засекречування інформації та пов'язані із цим зловживання, і як цього можна уникнути, підвищивши прозорість та зменшивши бюрократію у сфері доступу до державної таємниці.

Мета

Мета цієї роботи – відповісти на запитання:

- Чому прозорість у секторі безпеки і оборони важлива?
- Якою є система засекречування інформації в Україні?
- Які основні ризики надмірного засекречування?
- Які є провідні міжнародні практики у цій сфері?
- Як можна виправити недоліки системи?

Переваги прозорості

Поступово світ починає розуміти і сприймати переваги відкритого врядування. За останні кілька років понад 90 держав ухвалили закони про свободу інформації. Перед ними стояла непроста задача: як запровадити нові принципи прозорості та підзвітності не ризикуючи при цьому інтересами національної безпеки. Це надзвичайно позитивні зрушення, які допомагають збільшити прозорість та підзвітність у секторі безпеки та оборони. Достатня прозорість та ефективний громадський контроль дають важливі переваги, а саме:

- **Вдосконалення процедури формування державної політики**. Відкритий підхід до формування державної політики – це запорука створення підходів, що враховують соціальні й політичні реалії та потреби сьогодення. Якщо у державі не працює демократичний нагляд і контроль; якщо держава не дослухається до громадянського суспільства чи окремих його представників, на яких поширюється вплив її дій чи рішень; якщо держава не здатна підтримувати діалог з експертами, які можуть надати доказову базу, аналітику чи ідеї, – то така держава ризикує порушити свої зобов'язання за суспільним договором.

- **Побудова громадської довіри.** Відкритість – головна складова соціально-політичного здоров'я демократичної держави. Держава витрачає кошти платників податків і приймає рішення, що впливають на життя багатьох осіб. Коли громадяни мають доступ до інформації, державні органи несуть відповідальність за свої дії, а якість та продуктивність суспільного діалогу зростає. Якщо ж доступ до інформації надмірно

обмежений, держава не зобов'язана пояснювати свої дії та рішення. Через це вона ризикує втратити суспільну довіру та зрештою – легітимність.

- **Запобігання корупції.** У державі, де не працює система стримувань і противаг, виникають суттєві ризики того, що окремі посадовці зловживатимуть службовим становищем заради особистої вигоди. Якщо ж громадяни отримують доступ до необхідної інформації, це неодмінно підвищує відповідальність уряду. Водночас, це розширює можливості обох сторін викривати і повідомляти про незаконні чи неправомірні дії. Існує пряма залежність між зниженням рівня корупції та кількістю років, відколи країна запровадила законодавство про свободу інформації: що довше діють такі закони, тим нижчим є рівень корупції.

Повне засекречення є часто непотрібним, до того ж його важко забезпечити. Коли рішення про віднесення інформації до таємної приймаються непублічно і свавільно, дуже складно організувати, ефективний нагляд та контроль. Засекречення не завжди призводить до корупції, але між ними існує тісний взаємозв'язок. Чим прозорішою є держава, тим нижчий рівень корупції. І навпаки, слабкі системи контролю створюють можливості для зловживання владою задля особистої вигоди.

В усьому світі доступ до інформації про оборонні бюджети держав, як правило – обмежений, оскільки ця інформація безпосередньо стосується питань національної безпеки. Це часто пояснюється тим, що така інформація не повинна потрапити до рук потенційного ворога. У деяких випадках це цілком виправдано.

Кращі міжнародні практики у цій сфері викладені у *«Принципах Цване»* (2013 рік). Відповідно до цих Принципів, засекречування інформації допускається, якщо її розкриття створює *реальний* та *визначений* ризик нанесення *значної шкоди законним* інтересам національної безпеки[1]. До такої інформації можуть належати, зокрема, плани конкретних військових операцій чи подробиці науково-дослідних проектів з розробки ключового озброєння і військової техніки. В Україні категорії секретної інформації оборонного бюджету є незбалансованими і містять багато «сірих зон», що створює умови для корупції, неправомірного заволодіння майном та навіть узурпації влади.

Механізми засекречування інформації слід прямо передбачити законодавством, яке має бути доступним для громадськості і яке повинне встановлювати чіткі й зрозумілі правила про те, що може, а що не може бути віднесено до інформації з обмеженим доступом.

- **Формування бюджету.** Оборона є часто найбільшою сферою державних видатків. Коли інформація про розподіл ресурсів між оборонними установами є обмеженою, існує висока ймовірність їхнього неефективного використання та корупції. Часом ці видатки стають нецільовими чи йдуть на потреби приватних осіб та компаній, а не на забезпечення інтересів держави. Це призводить до марнування бюджетних коштів.

[1] "Глобальні принципи щодо національної безпеки та права на інформацію" (Принципи Цване), "Основи відкритого суспільства" (Global Principles on National Security and the Right to Information (Tshwane Principles), Open Society Foundations: https://osf.to/2LRe77j (Accessed June 2018).

Наприклад, солдати можуть не отримувати платню, не закуповується життєво необхідне озброєння і військова техніка, прибутки від військових контрактів розкрадаються, а окремі особи зловживають своїм посадовим становищем для отримання нелегальних доходів. Слабкий контроль за використанням бюджетних коштів може мати ще глибший вплив на стабільність демократії у випадках коли великі обсяги державних коштів викачуються на підтримку структур, що знаходяться під політичним покровительством чи на фінансування виборчих кампаній.

- **Закупівлі.** Прикриття інтересами національної безпеки може спричинити тиск на владу з боку окремих осіб, які прагнуть до укладання угод саме з ними в обмін на вигідні «відкати». Як наслідок, не лише державні кошти марнуються на хабарі, але часто придбане озброєння і військова техніка не відповідають тактико-технічним характеристикам або взагалі є непотрібними. Ймовірні втрати можуть бути величезними. У довгостроковій перспективі, відсутність прозорості у процесах закупівлі може стримувати доброчесних постачальників, які не віритимуть, що рішення будуть ґрунтуватися на чесній конкуренції. Це створює ризик застою в оборонній промисловості. Якщо приватні оборонні компанії не можуть адекватно оцінити рівень попиту на свою продукцію, вони дедалі менше будуть готові інвестувати в нові виробничі лінії та об'єкти. Компанії також не можуть належним чином оцінити можливості щодо своєї потенційної участі у тендерах.

Засекреченість оборонних бюджетів і закупівель також може потенційно привести до економічних втрат. Це призводить до непотрібних закупівель та зменшення рівня підзвітності, оскільки ціни встановлюються таємно і збільшується ризик, що платники податків переплачують за придбані вироби.

- **Політика і планування.** Зовнішній аналіз політичних питань, із залученням громадськості та за її підтримки, є ключовим елементом для прийняття ефективних рішень. Надмірна секретність означає, що менша група людей може фахово та обізнано впливати на процес прийняття політичних рішень. Також це означає, що рішення щодо державної політики і планування будуть прийняті без широкого зовнішнього залучення. Зараз, коли Україна переходить до системи планування закупівель на середньострокову та довгострокову перспективу, особливо важливо забезпечити прозорість, яка дозволить здійснювати фахову та обізнану підтримку процесу прийняття рішень щодо державної політики і планування.

Продовжувати засекречувати оборонні витрати та закупівлі основних видів озброєння і військової техніки стає дедалі складніше. Наприклад, Стокгольмський міжнародний інститут досліджень миру (SIPRI) має 45-річний досвід збору інформації про військові бюджети та міжнародну передачу озброєнь. Відкриті джерела (офіційні або неофіційні) надають SIPRI величезний обсяг інформації про закупівлю основних видів озброєння і військової техніки. Якщо такі організації як SIPRI, що працюють лише з відкритими джерелами, можуть з високим ступенем повноти і точності розраховувати військові витрати і відслідковувати глобальні переміщення озброєння, то національні розвідувальні установи точно можуть

досягати в цій сфері значно кращих результатів щодо отримання інформації про потенційних противників.

Ситуація в Україні

У цьому розділі розглядається питання визначення ступенів секретності в рамках чинного законодавства України та існування можливості надмірного засекречення. Режим секретності охоплює всі сектори національної безпеки і оборони та вимагає ретельного аналізу і вивчення. Проте, у цій аналітичній роботі особлива увага приділяється до двох сфер з високими ризиками: бюджетування та закупівлі. Існуючі законодавчі ініціативи, які спрямовані на підвищення прозорості оборонного бюджету України, описані наприкінці цього розділу.

Засекречення - визначення того, що можна приховувати

Закони України, як правило, передбачають презумпцію відкритості інформації. Це означає, що вся публічна інформація має бути відкритою, за виключенням окремих випадків. Засекречування інформації, пов'язаної з обороною, регулюється наступними основними нормативними актами: Закони України «Про інформацію»[2], «Про доступ до публічної інформації»[3], «Про державну таємницю»[4], «Про державне оборонне замовлення»[5], «Про основи національної безпеки України»[6] та іншими підзаконними актами. Велика кількість законодавчих актів, які охоплюють питання доступу до публічної інформації, містять винятки щодо питань, пов'язаних з національною безпекою. Оскільки ці винятки окреслені досить загальними формулюваннями, іноді складно приймати чіткі рішення про те, що слід чи не слід засекречувати.

Зазначеним законодавством передбачено три рівні захисту інформації: «Конфіденційно», «Для службового користування» та «Таємно». Категорія «Таємно» у свою чергу поділяється на «Таємно», «Цілком таємно» та «Особливої важливості». На практиці, більшість питань пов'язаних з обороною та безпекою часто невиправдано визначаються як таємні. Більше того, станом на сьогодні відсутні чіткі оприлюднені критерії визначення того, що становить загрозу національній безпеці, і що можна безпечно оприлюднювати.

Прийняття рішень

Для початку, слід розрізняти засекречування інформації, що *стосується* державної таємниці, та засекречування матеріалів, що *містять* державну таємницю. Перше здійснюється державними експертами з питань таємниць. Друге - службовцем-виконавцем, який працює над документом. Таким чином, віднесення інформації до державної таємниці зводиться до процесу ідентифікації загальної сфери належності інформації, яка є або державною таємницею, або такою, що вважається таємною в межах певного міністерства (відомства).

---

[2] Закон України № 2657-XII «Про інформацію» від 2 жовтня 1992 року.

[3] Закон України № 2939-VI «Про доступ до публічної інформації» від 13 січня 2011 року.

[4] Закон України № 3855-XII «Про державну таємницю» від 21 січня 1994 року.

[5] Закон України № 464-XIV «Про державне оборонне замовлення» від 3 березня 1999 року.

[6] Закон України № 964-IV «Про основи національної безпеки України» від 19 червня 2003 року.

Повноваження щодо формування правил засекречення та розсекречення інформації належать державним експертам з питань таємниць[7]. Перелік усіх експертів з питань державних таємниць наведено в Указі Президента України. Він включає, але не обмежується, Президентом, міністрами та їх заступниками, а також керівником Ради національної безпеки і оборони (РНБО).

Державні експерти з питань таємниць можуть визначати ступінь секретності інформації або за власною ініціативою, або у відповідь на звернення керівників відповідних державних органів, органів місцевого самоврядування, підприємств, установ, організацій, а також громадян. Відповідні категорії, що стосуються складових державної таємниці, консолідуються Службою безпеки України та формують "Звід відомостей, що становлять державну таємницю"[8].

Таким чином, у частково децентралізованій формі (механізм засекречування визначається експертами, а узагальнюється та реєструється СБУ), конкретні документи, що містять певні дані, засекречуються відповідно до порядку, визначеного уповноваженою посадовою особою.

Документ, який посадова особа подає для засекречування, має містити принаймні таку інформацію: саму інформацію, підстави її засекречування, причини віднесення інформації до державної таємниці, обґрунтовані аргументи стосовно загрози національній безпеці, що виникають у разі її розкриття, ступінь секретності та суму фінансування заходів щодо віднесення інформації до державної таємниці, її засекречування та охорони.

Після того, як уповноважена посадова особа засекретила інформацію та визначила необхідний ступінь секретності, доступ до документу обмежується і він підлягає належному зберіганню. У теорії, відповідальність за це лежить на СБУ. Вже зазначалося, що на практиці це не завжди так, оскільки у деяких випадках приватні інтереси іноді переважають над законом[9]. Ця проблема потребує подальшої уваги та вирішення.

СБУ має значний вплив на процес засекречування інформації, проте сама система до певної міри децентралізована. Відповідно до чинного законодавства, СБУ оцінює рішення державних експертів з питань таємниць про віднесення інформації до категорії секретної. Якщо, на думку СБУ, вимоги виконано, то рішення реєструється в журналі рішень державних експертів з питань таємниць. СБУ відповідає за забезпечення належного зберігання та охорони інформації.

Хоча процес засекречування не є повністю централізованим, процес прийняття рішень залишається в руках невеликої кількості осіб, за якими не здійснюється достатній контроль.

---

[7] Розсекречення інформації та надання висновків у разі порушення вимог або витоку секретної інформації є окремою темою, яка буде розглянута, досліджена і представлена *Незалежним антикорупційним комітетом* з питань оборони (NAKO) в останньому кварталі 2018 року.

[8] Див.: http://bit.ly/NAKO-3

[9] Інформація, отримана під час спілкування між NAKO та українським експертом з питань безпеки, серпень 2018 року.

Хоча правила засекречування інформації[10] розробляються державними експертами з питань таємниць, поза межами СБУ не існує механізму контролю та нагляду за рішеннями. Якщо між вищезгаданим експертом та посадовими особами СБУ існують корупційні зв'язки або особисті інтереси, то рішення про засекречування інформації може бути прийняте на користь цих інтересів без будь-якого подальшого контролю.

Перевірка наявності "суспільного інтересу"

Відповідно до Закону України "Про доступ до публічної інформації", обмеження доступу до інформації здійснюється за умови дотримання сукупності трьох вимог (так званий "трискладовий тест"):

- виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку;
- коли розголошення інформації може завдати суттєвої шкоди цим інтересам;
- коли шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Загалом, ці вимоги відповідають прийнятним, найкращим світовим практикам.
Однак Transparency International рекомендує публікувати обґрунтування, чому інформацію засекречують, оскільки це полегшує зовнішню оцінку необхідності та правомірності засекречення. В Україні такі обґрунтування не є загальнодоступними. В результаті, неможливо перевірити, чи вірно проведено "трискладовий тест".

Оборонний бюджет

Хоча загальні показники оборонного бюджету і оприлюднюють, інформація про витрати та статті бюджету недостатньо прозора. Відповідно до Індексу антикорупційної політики в оборонному секторі (Government Defence Anti-Corruption Index) за 2015 рік, відсоток витрат на таємні закупівлі та програми в оборонному бюджеті України достеменно невідомий. Крім того, в оборонному бюджеті не наведено детальної інформації про витрати на військові дослідження та розробки, бойову підготовку, будівництво, витрати на утримання особового складу, закупівлі, розпорядження майном та експлуатаційні витрати. Єдина доступна інформація – це загальний обсяг оборонного бюджету і суми, виділені на різні бюджетні програми. Сьогодні можливо знайти у відкритому доступі бюджетні запити Міністерства оборони України на певні державні цільові програми, де міститься детальніша інформація про конкретну програму, але рядки бюджету залишаються об'єднаними (наприклад, платежі та послуги). *Як наслідок, депутати, які голосують за оборонний бюджет, мають поверхневе уявлення про деталі фінансування кожної програми.* Така закритість підриває належний демократичний контроль за виконанням бюджету, не дає залучати зацікавлені сторони до процесу вироблення політики та створює значні корупційні ризики.

Закупівлі

У 2015 році оборонний бюджет Сполучених Штатів склав 596,02 млрд. дол. США. Витрати на засекречені програми склали 58,7 млрд. дол. США, що становить близько 10%. В Україні за

[10] Наприклад, див. механізм та відповідну таблицю, розроблені Державною службою України з надзвичайних ситуацій: http://bit.ly/NAKO-4

цей самий рік оборонний бюджет становив 45,8 млрд. грн. (1,7 млрд. дол. США), а засекречені видатки (державне оборонне замовлення (ДОЗ), тобто всі засекречені витрати на закупівлю) становили 8 млрд. грн. (0,3 млрд. дол. США), що становить 17,6%.

Основною причиною такої засекреченості є велика кількість закупівель, що проводиться в рамках ДОЗ. Вони здійснюються переважно без застосування конкурентних процедур, і їх деталі повністю засекречують. Усі закупівлі зброї, військової техніки та боєприпасів здійснюються в рамках ДОЗ. ДОЗ – це перелік усіх товарів, робіт та послуг, необхідних для забезпечення потреб оборони. Майже всі закупівлі, що здійснюються в рамках ДОЗ, відбуваються без конкурентного, прозорого процесу.

Згідно чинного законодавства[11], частину закупівель в рамках ДОЗ здійснюють відповідно до Закону України "Про державні закупівлі" з використанням системи електронних закупівель ProZorro. Іншу частину закупівель, що містять дані, які становлять державну таємницю, здійснюють без використання конкурентних процедур. На практиці, без конкурентних процедур в рамках ДОЗ здійснюють близько 95% закупівель: споживач обирає постачальника і безпосередньо укладає з ним угоду. Замість конкурентної процедури, ціна формується відповідно до постанови Кабінету Міністрів України (КМУ) від 8 серпня 2016 р. № 517. Остаточні узгоджені деталі вартості товарів, придбаних в рамках такого механізму, приховані від громадськості. Відома лише загальна сума.

Дані, необхідні для формування ДОЗ, консолідуються Міністерством економічного розвитку і торгівлі (МЕРТ) на основі заявок, поданих державними замовниками з оборонно замовлення. Постанова Кабінету Міністрів України від 27 квітня 2011 р. № 464 визначає державними замовниками 15 органів виконавчої влади. Отримавши інформацію від державних замовників про те, що вони планують закупити, МЕРТ підраховує кількісні показники і подає їх на затвердження до КМУ. Затверджений реєстр виконавців ДОЗ координується МЕРТ. Щоб потрапити до цього переліку, виробник має подати заявку і надати ряд документів, включаючи документ, що засвідчує наявність державної таємниці у його продукції або послугах. Перелік постачальників за ДОЗ є таємним (стаття 7, пункт 3, Закон про ДОЗ).[12]

<u>Законодавчі ініціативи, спрямовані на підвищення прозорості оборонного бюджету</u>
Два законопроекти, спрямовані, зокрема, на підвищення прозорості оборонного бюджету України, були внесені на розгляд Верховної Ради України 28 лютого 2018 року:[13]

- проект Закону про внесення змін до Бюджетного кодексу України № 8076 від 28 лютого 2018 року;
- проект Закону про внесення змін до Закону України "Про Регламент Верховної Ради України" № 8075 від 28 лютого 2018 року.

[11] Стаття 7 Закону України № 464-XIV «Про державне оборонне замовлення» від 3 березня 1999 року.
[12] Пункт 3 Статті 7 Закону України № 464-XIV «Про державне оборонне замовлення» від 3 березня 1999 року.
[13] Внесені групою з семи депутатів Верховної Ради, які працюють над проектом щодо внесення змін до Бюджетного кодексу України (у частині, що стосується державного оборонного бюджету)http://bit.ly/NAKO-2.

Зокрема згадані законопроекти передбачають:

- введення нового юридичного терміну, а саме “Державний оборонний бюджет” (ДОБ). ДОБ має залишатись частиною Державного бюджету України (у формі додатку);
- ДОБ має передбачати кошти, виділені Міністерству оборони України та Міністерству внутрішніх справ України;
- щодо структури, ДОБ має бути розділений на дві частини: описовий і детальний.

У свою чергу, витрати в деталізованій частині ДОБ розділені на три категорії:

- витрати на споживання;
- витрати на розвиток;
- витрати на військові дії.

Крім того, законопроекти містять детальні описи усіх трьох видів витрат бюджетного замовлення та перелік конкретних категорій інформації, яку вони містять. Законопроекти скасовують положення, які стояли на заваді деталізації та обґрунтуванню засекречування видатків державного бюджету України.

Слід відзначити, що обидва законопроекти *рекомендують запровадити порядок надання всім народним депутатам доступу до інформації про засекречені видатки* (за умови підписання зобов'язання про нерозголошення).

Окремі приклади кращих практик і принципів

Зрозуміло, що Україна веде боротьбу з російськими військовими на сході держави. Тому для захисту інформації щодо національної безпеки потрібен вищий рівень секретності. Проте, це не повинно виправдовувати відмову від кращих міжнародних практик щодо законодавчого регулювання захисту державної таємниці. Зокрема, кращі практики передбачають основні норми і рекомендації щодо збалансування потреби в обґрунтованому засекречуванні з одночасним забезпеченням права громадськості на доступ до інформації.

Ці основні рекомендації визначають наступне:

- Повноваження щодо приховування або засекречування інформації мають бути чітко визначені та походити від законного джерела влади і виконуватись відповідно до процедур, встановлених оприлюдненими правовими нормами;
- Інформація може бути захищена шляхом засекречування та/або її нерозголошення, якщо існує реальний та суттєвий ризик того, що її оприлюднення може спричинити серйозну шкоду;
- Якщо інформацію приховують, то повинні існувати процедури (доступні для всіх), які дозволяють незалежним органам здійснювати ефективний контроль. Також має бути гарантія, що інформацію не будуть приховувати від громадськості протягом невизначеного терміну;
- Засекречування та рішення про приховування інформації повинні бути обґрунтовані письмово, а інформація має бути належним чином архівована задля сучасних та історичних цілей.

Законодавство повинне передбачити перевірку наявності суспільного інтересу задля визначення необхідності приховування чи розкриття інформації або навіть містити заборону засекречення окремих категорій інформації:

- у кожного ступеня секретності має бути максимальний термін дії;
- будь-яке обмеження права на інформацію має відповідати міжнародно-правовим стандартам, і ці принципи також мають бути враховані національним законодавством.

Принципи Цване детальніше описують ці стандарти. Це набір принципів, викладених групою академічних інституцій та неурядових організацій. Вони базуються на широко визнаній переконаності, що надаючи громадськості контроль за діяльністю держави, доступ до інформації стає ключовим компонентом справжньої національної безпеки та демократичної участі. У принципах Цване викладені вказівки щодо того, яку інформацію можна приховувати з міркувань безпеки. Йдеться про інформацію, що пов'язана з:

- поточними оборонними планами, операціями та військовим потенціалом протягом періоду часу, коли інформація є оперативно корисною;
- виробництвом, військовим потенціалом або використанням систем озброєння та інших військових систем, включаючи системи зв'язку;

- конкретними заходами, ефективність яких залежить від секретності, що спрямовані на захист території держави, критичної інфраструктури або критичних національних інституцій від загроз, або застосування сили, або від диверсій;
- операціями, джерелами і методами роботи розвідувальних служб, якщо вони стосуються питань національної безпеки;
- питаннями національної безпеки, які пов'язані з побажаннями конфіденційності, що висловлені іноземною державою або міжурядовим органом, а також з іншими дипломатичними відносинами, якщо вони зачіпають питання національної безпеки.

Підзвітність та обґрунтованість є ключовими факторами, коли інформація є надто чутливою для публічного розголошення і де потрібен парламентський контроль, наприклад, з боку певного парламентського комітету. Цей нагляд має забезпечити функціонування механізмів стримувань і противаг, необхідних в рамках демократії. Цей механізм повинен запобігати надмірному засекречуванню інформації у сфері оборони і безпеки. До забезпечення функціонування цих принципів має бути залучене громадянське суспільство. Гарантією ефективного громадського моніторингу і нагляду буде недопущення надмірного засекречування державою інформації (яка не стосується національної безпеки) та наявність доступу громадян до інформації.

Кращі практики щодо Доступу до Інформації зазначено у документах “Кращі практики прозорості бюджету” Організації економічного співробітництва і розвитку (1999 рік) та “Стандартизований інструмент звітності про військові витрати ООН” (1980 рік). Наразі вони залишаються єдиними офіційними, глобальними системами звітності.

Імплементація: уроки, отримані кращих міжнародних практик та досвід Великої Британії.

Загалом, механізми захисту державної таємниці функціонують в рамках правової бази, до якої, зокрема, входять закони про національну безпеку, про запобігання злочинності та про державну таємницю. Зазвичай кожен, хто працює в органах державної влади або співпрацює з урядом, зобов’язаний застосовувати політику засекречення та захисту конфіденційності інформації і даних, до яких він має доступ.

Системи захисту державної таємниці

Класифікація таємної інформації відображає чутливість інформації. Кращі міжнародні практики визначають кожну категорію засекречення з точки зору вірогідних наслідків, що можуть виникнути внаслідок втрати або несанкціонованого розголошення таємної інформації. Така класифікація визначає, як слід поводитись з інформацією кожної категорії. Наприклад, у Великій Британії існує три рівня секретності: “Службовий”, “Таємно” і “Цілком таємно”:

Деякі інші країни мають більше категорій. Німеччина, наприклад, має чотири ступеня секретності:

- **Цілком таємно**: несанкціоноване розголошення інформації може поставити під загрозу існування або життєво важливі інтереси Федеративної Республіки Німеччини або однієї з її Земель (федеральних земель).
- **Таємно**: несанкціоноване розголошення інформації може поставити під загрозу безпеку Федеративної Республіки Німеччини або однієї з її Земель, або завдати серйозної шкоди її інтересам.
- **Обмежено - Конфіденційно**: несанкціоноване розголошення інформації може бути шкідливим для інтересів Федеративної Республіки Німеччини або однієї з її Земель.
- **Обмежено – Тільки для службового використання**: несанкціоноване розголошення інформації може бути невигідним для інтересів Федеративної Республіки Німеччина або однієї з її Земель.

Ризики та їх контроль

Більшість державних відомостей взагалі не слід засекречувати, зокрема, інформацію, яка стосується діяльності оборонних інституцій. Наприклад, Міністерство оборони Норвегії опублікувало документ обсягом понад 100 сторінок, в якому детально описуються їхні довгострокові плани щодо запланованих закупівель на період до 2025 року. Також, у Нідерландах оприлюднено детальну інформацію про системи оплати праці, яка наведена на їх веб-сайті.[14]

Очевидно, що не вся інформація є однаково чутливою. Наприклад, Великобританія дає визначення рівня загрози для ступеня секретності “Службовий”, як “загалом подібний до того, що притаманний великій британській приватній компанії з цінною інформацією та

[14] Оборонний бюджет Нідерландів (2018) http://bit.ly/NAKO-1

послугами". Це означає, що необхідні засоби контролю мають бути спрямовані на захист інформації від несанкціонованого доступу осіб з обмеженими можливостями та ресурсами, таких як журналісти, які проводять розслідування, хакери або більшість злочинних груп.

Серйозніші загрози вимагають більш ретельного контролю. Очевидно, що уряди намагатимуться мінімізувати ризики витоку інформації з найвищим ступенем секретності. На жаль, правила за якими відбувається засекречення інформації у Великій Британії не є загальнодоступними, хоча вони могли б послужити корисним орієнтиром.

Головною метою будь-якої системи захисту таємної інформації є контроль ризиків. Тому кожна категорія засекречення передбачає певний базовий набір персоналу і засобів забезпечення фізичної та інформаційної безпеки відповідно до рівня ризику. Цілком імовірно, що міжвідомчий Головний відповідальний за інформаційні ризики (Далі – ГВІР) відповідатиме за узгодження заходів з контролю, які потім повинні застосовуватись в усіх державних органах. Крім того, їх слід регулярно переглядати. В Україні фундаментальні поняття та функції ГВІР реалізовані в інституті державного експерта з питань таємниць.

Прийняття рішень та забезпечення їх імплементації
Центральне місце ефективної системи безпеки - це не просто створення ефективного механізму. Необхідно надати персоналу повноваження, щоб виконавці на відповідних рівнях приймали правильні рішення щодо обробки інформації.

У кінцевому підсумку, співробітники, навіть на відносно низьких рівнях, мають знати, як оцінювати ризики у разі витоку інформації та бути в змозі збалансувати ситуацію так, щоб інформація була доступна потрібним людям в потрібний час.

На практиці, це означає чітке делегування відповідальності за втілення міжвідомчої (в рамках уряду) політики захисту таємної інформації. У першу чергу, будь-який урядовий орган (відомство) може призначати високопосадову особу відомчим ГВІР, яка буде відповідати за забезпечення ефективного застосовування політики захисту таємної інформації у своєму відомстві. Однак відомчий ГВІР навряд чи прийматиме рішення щодо визначення рівня засекречення в кожному окремому випадку. Радше слід очікувати, що працівники відомства будуть належно проінструктовані та навчені задля забезпечення того, щоб вони могли впроваджувати політику захисту інформації на практиці, в залежності від типу інформації, з якою вони мають справу.

Таким чином, будь-який чиновник (навіть низького рангу), починаючи роботу над новим документом, доповіддю або звітом, має прийняти обґрунтоване рішення щодо визначення ступеню секретності цього документу. У рамках конкретного ступеню секретності необхідно буде чітко викласти процедури, що можуть передбачати використання певної ІТ-системи, способи зберігання або обмеження доступу окремих осіб чи категорій персоналу.

Не зважаючи на те, що чиновнику необхідно буде у певній мірі визначити ступінь секретності, йому/їй, як правило, не буде надано всієї повноти прийняття рішення щодо подальших рівнів контролю ризиків. Ці методи контролю, що випливають зі ступеня

секретності документу, повинні бути чітко встановлені міжвідомчим ГВІР (як описано вище). У свою чергу, відомчий ГВІР має гарантувати, що відповідні підрозділи належно підготовлені та забезпечені.

Для прийняття рішень щодо присвоєння ступенів секретності, персонал має бути підготовлений через навчання, тренінги та управлінські ланцюжки. Управлінські ланцюжки мають працювати так, щоб забезпечити належний контроль та механізм його дотримання. Відомчий ГВІР може також прийняти рішення про запровадження додаткових організаційних механізмів для виявлення слабких місць або недоліків. Це може означати, що підпорядковані підрозділи його відомства визначать особу, відповідальну за взаємодію між ГВІР та підрозділами, щоб забезпечити належне виконання інструкцій у кожному з підрозділів.

Як правило, будь-яка урядова структура за визначенням має прагнути до застосування найнижчого необхідного ступеню секретності. Нездатність розповсюдити та використати інформацію може перешкодити ефективному вирішенню державних справ і привести до серйозних наслідків (наприклад, неефективне оборонне підприємство не зможе задовольнити потреби армії). Водночас, принципи відкритості, прозорості, доступу до відкритих даних і можливість повторного використання інформації можуть вимагати від осіб-виконавців оприлюднення державної інформації та наборів даних на випередження. Щоб досягти правильного балансу, необхідне мотивоване рішення. Прийняття таких рішень може бути покладено на виконавців, однак у підрозділі може бути призначений як співробітник, відповідальний за інформаційну безпеку, так і експерт з відкритих даних, які забезпечать повсякденну діяльність підрозділу. Важливо відзначити, що ця функція може становити лише невелику частину робочого навантаження такої особи, залежно від ризику або розміру відповідного підрозділу.

Рекомендації зі вдосконалення порядку засекречування інформації в Україні

Перед кожною державою стоїть важливе завдання: забезпечити баланс між засекреченням інформації, розголошення якої може створити загрозу для держави та її громадян, та доступом громадськості до інформації. Прозорість – це питання не лише прав людини, але й національної безпеки. Якщо інформація засекречена понад міру – це сприяє корупції, заважає ефективному плануванню та розробці стратегій, і зрештою, знижує довіру суспільства до держави. У цій роботі ми проаналізували провідні міжнародні принципи й практики і окреслили курс, якого варто дотримуватися Україні, якщо вона бажає вдосконалити чинну систему засекречування інформації.

- Органи, де працюють державні експерти з питань таємниць, повинні отримати можливість публікувати критерії, які визначають ступінь секретності інформації. Ці критерії повинні відображати законні підстави віднесення інформації до державної таємниці (на 5, 10 або 30 років). Критерії мають бути обов'язковими до використання при обґрунтуванні рішень про засекречення інформації.

- МЕРТ у співробітництві з органами у сфері безпеки та оборони повинні розкрити більшу частину ДОЗу. Для цього Верховна Рада України має створити правові основи шляхом внесення змін до Закону України "Про державну таємницю". Безперечно, окремі частини ДОЗу слід залишити закритими з міркувань національної безпеки, проте рішення щодо відповідних категорій інформації має відповідати вимогам трискладового тесту і бути публічно обґрунтованим. При цьому члени Комітету з питань запобігання і протидії корупції, Комітету з питань національної безпеки і оборони та аудиторські органи повинні мати доступ до всієї інформації.

- ДОЗ – це зона підвищеного ризику надмірного засекречування, а отже, ДОЗ має стати пріоритетною сферою реформування. МЕРТ і СБУ мають оприлюднити критерії, якими вони керуються при вирішенні порядку здійснення закупівлі: за відкритою процедурою чи в рамках ДОЗ. Крім того, МЕРТ і СБУ повинні поставити за мету скоротити частку закупівель, що відбуваються в рамках ДОЗ. МЕРТ має відкрити доступ до реєстру виконавців ДОЗ.

- Необхідно забезпечити більшу деталізацію оборонного бюджету і суттєво зменшити частку таємних закупівель. Проект і фінальна версія оборонного бюджету повинні носити комплексний характер і викладатися у вільний доступ – для громадянського суспільства та донорів.

- Після оприлюднення критеріїв віднесення інформації до державної таємниці органи, де працюють державні експерти з питань таємниць, мають переглянути та привести у відповідність до вимог законодавства свої внутрішні процедури, щоби забезпечити можливості делегування повноважень працівникам нижчого рівня, та провести навчання для персоналу з питань ступенів секретності інформації.

Висновки

Порядок обмеження доступу до інформації помітно різниться залежно від країни. Грань між засекречуванням інформації в інтересах національної безпеки та її приховуванням задля особистого збагачення дуже хитка, особливо у країнах з перехідною економікою. Реформа державної таємниці – благородна справа, що має на меті підвищити економічну ефективність, удосконалити порядок використання бюджетних коштів та забезпечити загальне благо. Це делікатний процес, що потребує узгодженої взаємодії різноманітних державних органів і структур.

У цій роботі на прикладі оборонних закупівель представлені деякі основні проблеми обмеження доступу до інформації. Щоби виявити системні проблеми, що сприяють корупції (відсутність ефективного демократичного нагляду та контролю, надмірне засекречування інформації, неефективність, а часом і повна відсутність засобів правового захисту, застарілі підходи до управління), потрібно провести подальші дослідження.