Національний університет "Києво-Могилянська академія"

Києво-Могилянська школа врядування

Кафедра суспільного врядування

2018/2020 навч. рік

_____ Андріана Арехта

(підпис) (ПІБ)

_____ Роман Антюхов

(підпис) (ПІБ)

Аналітична записка

Як забезпечити захист штабної інформації, інформації про особовий склад ЗСУ.

(формулювання проблеми)

Анотація

Замовник: Міністерство оборони України, Генеральний Штаб України

Мета вирішення проблеми: Захист інформації про особовий склад Збройних Сил України, впровадження кібербезпеки.

Рекомендований варіант політики: ***Впровадження новітньої інформаційної системи на основі*** **симетричного алгоритму блочного шифрування Advanced Encryption Standard (AES)**

Відхилені варіанти політики: статус-кво, впровадження системи українськими компаніями

Ця Аналітична записка – результат нашої власної роботи, вона була написана нами самостійно без співпраці з ким-небудь. Ми даємо згоду на те, що цю Аналітичну записку можна безоплатно використовувати в повному обсязі або частково для публікації он-лайн, в електронному вигляді та для адаптації в навчальних цілях.

_____	_____
(підпис)	(ПІБ) .
_____	_____
(підпис)	(ПІБ)

Київ – 2020

1. Визначення проблеми, придатної для аналізу політики

1.1. Формулювання проблеми

Відсутність захисту штабної інформації, інформації про особовий склад ЗСУ.

1.2. Замовник аналізу

Замовником даного аналізу є Міністерство оборони України та Генеральний Штаб України, так як відповідно до Законів України "Про Збройні Сили України", "Про військовий обов'язок і військову службу", Указу Президента України від 10 грудня 2008 року № 1153 "Про Положення про проходження громадянами України військової служби у Збройних Силах України" та з метою подальшого вдосконалення та належної організації обліку особового складу Збройних Сил України затверджена Інструкція з організації обліку особового складу Збройних Сил України [1].

1.3. Симптоми проблеми

1.3.1 Опис симптомів

По-перше, активна інтеграція новітніх мережевих технологій у життя пересічного українця стала невід'ємною складовою різноманітних сфер суспільного життя. Не стали винятком і Збройні Сили України.За роки війни значно розширилося використання таких технологій не тільки в процесі повсякденної життєдіяльності, а й у процесі управління діями підрозділів у зоні АТО. Широке залучення інформаційних технологій дає можливість значно зменшити час на прийняття рішень, передачу наказів та обмін інформацією між підрозділами. В 2014 році з початком агресії РФ, підрозділи використовували особисті цифрові прилади для передачі даних та не захищену мережу, що спричинило до витоку інформації про особовий склад ЗСУ, особливо тих, хто знаходився в зоні АТО, зараз в зоні ООС, що є основним симптомом даної проблеми. Важливим симптомом є той факт, що Верховною Радою було прийнято Закон України "Про внесення змін до Конституції України (щодо стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору)" [2] який передбачає стандартизацію ЗСУ до стандартів НАТО, в тому числі і діджиталізацію та захист інформації про особовий склад та боротьбу з кібератаками.

1.3.2 Причинно-наслідкові зв'язки

Після відновлення незалежності України на початку 1990-х принцип позаблоковості, якого дотримувався офіційний Київ, був своєрідним запобіжником від інтеграції до військового блоку на пострадянських теренах. У 1992 році Росія створила Організацію Договору про колективну безпеку (ОДКБ). Ідея позаблоковості мала б передбачати концепцію «орієнтації на власні сили» та створення потужної армії, проте реалії 22 років після проголошення незалежності поглибили суперечність форми і змісту: за умов позаблоковості фінансування оборони відбувалося фактично за залишковим принципом і врешті стало меншим, а ніж у МВС. Так у Державному бюджеті України на 2013 рік витрати на ЗСУ заплановано обсягом $1,9 млрд (15,3 млрд грн, або 0,98% ВВП). Майже чверть століття позаблоковості призвели до небоєздатності армії, яка деградувала дуже швидкими темпами. Позаблоковість – дороге задоволення, оскільки гарантувати безпеку самотужки завжди складніше, аніж спільно із союзниками. Витрати на фінансування української армії були критично малими навіть на тлі держав, що належать до різних військово-політичних альянсів. Адже основна частка тих украй замалих витрат на оборону, які надходили, припадала на утримання військових, тоді як на їхнє навчання чи закупівлю сучасних видів техніки коштів фактично не виділяли. Внаслідок цього ми мали декоративні збройні сили які не здатні були гарантувати країні безпеку чи територіальну цілісність.

В 2014 - початок анексії Криму та окупаційні дії військ Російської Федерації на Сході України показали неспроможність та непідготовленість ЗСУ до зовнішнього втручання. Не

було зв'язку, техніки, координації між ЗСУ та добровольчими батальйонами та великий витік інформації про особовий склад, пересування військ через світову мережу, соціальні мережі. В інтернеті з'являється сторінка “Трибунал ЛНР та ДНР” з особистими даними військовослужбовців та добровольців.

1.3.3 Доказова база

Основною доказовою базою є сайт “Трибунал. Возмездие настанет” [4] - де знаходяться дані 63810 військовослужбовців, волонтерів, журналістів з фотографія ідентифікації особи, з адресами проживання сім'ї , з даними про склад сім'ї. Основний об'єм інформації був на сайті вже наприкінці 2014 року, в основному через російські спецслужби, сервери, які знаходяться на території РФ, халатність та неуважність військовослужбовців ЗСУ та відсутність систем захищеного зв’язку та засобів передачі даних та ведення обліку особового складу.

1.4. Законодавча й інституційна база у сфері, де спостерігаються вказані симптоми

1.4.1 Законодавча база реалізації чинної політики

Першим інструментом є інформування та навчання особового складу щодо використання засобів зв'язку під час служби, під час знаходження на позиціях в зоні ООС. На сайті Міноборони є інформаційні карти щодо загроз та правил [5], але даної інформації не достатньо, навчальні лекції з кібербезпеки в військових підрозділах - є першим інструментом і механізмом.

Щодо законодавчої бази, то дана проблема базується на Наказі Міністерства оборони України № 650 від 17.09.2014 р. про затвердження Концепції інформатизації Міністерства оборони України [6], Закон України “Про захист персональних даних” [7], Законі України “Про державну таємницю” [8]. Прийняті також документи, які складають нормативну базу в цій сфері: Національна програма інформатизації [9], Закон України "Про захист інформації в автоматизованих системах" [10]. Основною базою є стратегія України до Північноатлантичного альянсу (НАТО), що передбачено в Конституції, а отже Сектор безпеки і оборони України повинен відповідати стандартам НАТО.

1.4.2 Інституційна база реалізації чинної політики

Забезпечення національної безпеки входить до компетенції значної кількості органів влади, проте оскільки дана реалізація політики вважається конфіденційною інформацією, та тією, що потребує захисту, інституційна база реалізації чинної політики складатиметься виключно з інституцій, що є суб'єктами забезпечення національної безпеки в межах своїх повноважень (Президент України, Генеральний штаб, Міністерство оборони, спеціальних структурних підрозділів, офіс НАТО в Україні, Кабінет міністрів УКраїни, РНБО, СБУ)

1.5. Масштаб проблеми

Проблема є всеукраїнського масштабу. Мусимо визнати, що війна триває не лише на полі бою. Атаки ворога у кіберпросторі – це цілком військова загроза, на яку необхідно відповідно реагувати. В Україні, на жаль, за кіберпростір кожен орган відповідає сам. Це колективна безвідповідальність, а отже, програш у війні. Кібератаки нині – не точкові дії, а сплановані акції, протистояти яким може лише якісний захист. Нема жодного сумніву в тому, що для створених у лютому 2017 року військ інформаційних операцій у складі Міноборони РФ, найвразливішою мішенню є Україна. Витік інформацію про особовий склад ЗСУ призводить до погрози життю військовослужбовця та членів їх сімей під час проходження служби так і по закінченню проходження служби. В Україні зафіксовано тисячі телефонних дзвінків діючим військовослужбовцям, ветеранам та членам їх сімей з погрозами зі сторони

РФ. Дані передаються для опрацювання в СБУ. Також цією ситуацією користуються шахраї, які використовують інформацію для вимагання грошей у родичів військових, які знаходяться в полоні чи рахуються безвісти зниклими. Мобільні дані солдата на полі бою призводять до вичислення місця дислокації, що призводить до втрат ЗСУ. Мобільні дані використовуються також для психологічних атак, відбувається розсилка СМС -повідомлень для деморалізації бійців.

Використання персональних чи волонтерських комп'ютерної техніки з незахищеними програмами від взлому , використання російських антивірусних програм, використання в штабі особовим складом соц. мереж, програм, що збирають геолокаційні дані, а також загруження секретної інформації через інтернет на диск GoogleDrive призводить до масштабных проблем в сфері безпеки і оборони країни.

1.6. Новизна проблеми

Проблема для України не нова, вона існує досить давно, але досі не вирішена, що спричиняє нагальність пошуку рішень. Країна 5 рік втрачає інформацію, що призводить до втрат особового складу, секретної інформації про обороноздатність країни що призводить до програшу в інформаційній війні, до кібератак, які можуть “паралізувати” інфопростір. Реформування армії, а також перехід від методики “журнал обліку журналів” до цифрових технологій, відхід від російського контенту та російських засобів зв'язку та пережитків пострадянської армії наблизить ЗСУ до стандартів НАТО, а найважливіше збереже життя українцям.

1.7. Опис механізмів та інструментів чинної політики

Для забезпечення ефективності і результативності формування та реалізації чинної політики необхідно в комплексі використовувати інструменти правового, економічного, фінансового, організаційного, інформаційного, освітнього характеру. Система цих інструментів повинна ґрунтуватись на якісному прогнозуванні, відображати національні пріоритети та узгоджувати загальнодержавні інтереси.

Інструменти та механізми:

1. У сфері фінансово-економічного забезпечення:

- довгострокове бюджетне планування;
- якісне використання коштів трастового фонду НАТО проведення аналізу бюджетних запитів розпорядників бюджетних коштів із залученням центральних органів влади в процесі опрацювання проекту державного бюджету України на поточний рік з метою вмотивованого вирішення питань концентрації фінансових ресурсів на реалізацію пріоритетних цілей та програм в секторі безпеки і оборони УКраїни

2. У сфері інституційного забезпечення:

- запровадження електронного урядування та документообігу;
- державна підтримка програм та проектів, що стосуються національної безпеки і оборони України.
- удосконалення стратегічного планування МО, РНБО, їх узгодження з цілями та напрямами національної політики, здійснення бюджетного планування відповідно до стратегічних пріоритетів;
- збереження курсу України в членство в Євроатлантичному Альянсі

1.8. Нагальність вирішення (що буде, якщо не вирішувати)

Основною доказовою базою є сайт “Трибунал. Возмездие настанет” [4] - де знаходяться дані 63810 військовослужбовців, волонтерів, журналістів з фотографія ідентифікації особи, з адресами проживання сім'ї , з даними про склад сім'ї. Основний об'єм

інформації був на сайті вже наприкінці 2014 року, в основному через російські спецслужби, сервери, які знаходяться на території РФ, халатність та неуважність військовослужбовців ЗСУ та відсутність систем захищеного зв'язку та засобів передачі даних та ведення обліку особового складу.

2. Мета вирішення проблеми

2.1 Формулювання мети вирішення проблеми (за необхідності вказати відповідні завдання політики як конкретизації цілей).

Захист інформації про особовий склад ЗСУ, впровадження кібербезпеки. Реалізація політики з впровадженням сучасного механізму документообігу в секторі безпеки і оборони України, практично діючої інформаційної системи управління та підрозділів з кібербезпеки, для захисту військовослужбовця та його сім'ї.

1. Система документообігу
2. Підрозділи з кібербезпеки
3. Наближення до стандартів НАТО
4. Сильна професійна армія, захищений військовослужбовець.

2.1.1 Показники (індикатори) результативності (кожній цілі (завданню) має відповідати свій індикатор результативності або система індикаторів – якщо один індикатор не розкриває всі суттєві аспекти цілі.

Показники (індикатори) результативності

- зменшення витоку інформації якою володіє ЗСУ
- збільшення використання сертифікованою комп'ютерною технікою та програмами
- використання електронного документообігу
- створення підрозділів з питань кібербезпеки

2.1.2 Критерії досягнення цілей (критерій визначає конкретне значення індикатора результативності, яке вважається достатнім для визнання проблеми розв'язаною; кожному індикатору має відповідає свій критерій).

Цільові індикатори - критерії досягнення цілей

- зменшення витоку інформації якою володіє ЗСУ до 2022р. на 70%
- збільшення використання сертифікованою комп'ютерною технікою та програмами до 2022р. на 70%
- використання електронного документообігу до 2022р. на 70%
- створення підрозділів з питань кібербезпеки до 2022р.

2.1.3 Обмеження (список обмежень має охоплювати будь-які ресурси, необхідні для реалізації альтернатив політики).

Бюджетні обмеження- потребує значного фінансування з державного бюджету
Часові обмеження - проблема потребує негайного вирішення
Інші матеріальні ресурсні обмеження - відсутність обладнання, кваліфікованого персоналу;
Ризики державного втручання- військове законодавство України недосконале, діяльність агентури та проросійських політичних партій та громадських організацій
Ризики державного втручання - *«Універсальні»*.

3. Підстави для державного втручання

3.1 Аналіз неспроможностей ринку (які саме ситуації неспроможності ринку потребують державного втручання - з огляду на економічні, соціальні та політичні чинники)

Роки паперового діловодства створили своєрідну систему як у цивільних, так і силових структурах нашої держави. Одним із багатьох недоліків цієї системи є необхідність оперування фізичними об’єктами, що значно сповільнює більшість пов’язаних між собою процесів (виробництво, обмін інформацією, прийняття рішень, надання послуг тощо). Впровадження електронних систем обміну даними в ЗСУ, відкриває можливість застосування величезної гнучкості в обробці та зберіганні інформації, а також змушує організації чи структури працювати швидше та з більшою ефективністю — приймати рішення командирами та віддавати накази відповідно до швидкої зміни бойової обстановки в режимі реального часу. Адже швидкість прийняття правильного рішення в бойовій обстановці є запорукою успіху виконання поставлених бойових завдань та збереження життя військовослужбовців. Ці технології також дають можливість підвищити ефективність роботи та економити час у повсякденній діяльності.

Військові підрозділи в усьому світі вже активно використовують захищені системи обміну даними і майже зовсім відмовилися від паперового діловодства.

Будь-яка система, яка використовується ЗСУ має включати механізм захисту із використанням криптографічного шифрування для: забезпечення збереженості документів, забезпечення безпечного доступу, забезпечення достовірності документів, протоколювання дій користувачів.

Система обміну даними повинна забезпечити не тільки передачу інформації, але її збереження від викрадення чи модифікації, а також мати можливість її швидкого відновлення.

4. Середовище проблеми для аналізу політики

4.1 Складники середовища

- економічне середовище
- політичне середовище
- соціальне середовище
- фізичне середовище

4.2 Ресурсні затрати для вирішення проблеми:

- економічне середовище
- політичне середовище
- соціальне середовище
- фізичне середовище

4.3 Яких ресурсів може бракувати для розв’язання проблеми

- економічне середовище
- соціальне середовище

4.4 Конкретні продукти як результат розв’язання сформульованої проблеми

- Інформаційна системи НАТО на основі Advanced Encryption Standard (AES), — симетричний алгоритм блочного шифрування (розмір блока 128 біт, ключ 128/192/256 біт)
- Підрозділи з кібербезпеки при МО/ГШУ
- Сертифікована комп'ютерна техніка та програми

4.4.1 Короткострокові, середньострокові й віддалені кінцеві результати

Короткострокові

- впровадження політики, яка відповідатиме стандартам НАТО (наближення України до членів Північноатлантичного альянсу)

Середньострокові

- захист штабної інформації в ЗСУ, створення єдиної інформаційної системи управління:
- сертифікована комп'ютерна техніка та програмне забезпечення з високим ступенем захисту інформації

Віддалені кінцеві результати

- повне переоснащення засобів зв'язку новітніми технічними засобами за стандартами НАТО.
- Створена кібернетична система Збройних Сил.

4.4.2 Бажані/небажані, передбачувані/непередбачувані кінцеві результати

Бажані:

- захист життя та безпеки військовослужбовців та членів їх сімей.
- Ефективне виконання військової служби підрозділами ЗСУ внаслідок швидкої передачі даних, оперативного прийняття рішень.
- підвищена обороноздатність ЗСУ

Небажані:

- корупція, привласнення державних коштів (аналіз політики з Укроборонпромом);
- пострадянський спадок, (вища та середня ланка управління ЗСУ, вихована радянською армією, небажання до змін.)

Передбачувані:

- витрати з державного бюджету на закупівлю та навчання особового складу Збройних Сил України
- час на процес впровадження та навчання в умовах війни.

Непередбачувані:

- блокування інноваційної ініціативи з боку різних міністерств, проросійських сил

4.4.3 Результативність розв'язання сформульованої проблеми

- З двох існуючих систем шифрування, інформаційна система НАТО на основі Advanced Encryption Standard (AES), — симетричний алгоритм блочного шифрування (розмір блока 128 біт, ключ 128/192/256 біт - захист даних ЗСУ, менший витік інформації до РФ
- Електронний документообіг, швидке прийняття рішень
- Перевага перед ворогом РФ, зменшення витоку інформації, збільшена можливість для проведення операцій
- Кількість збережених військових

4.4.5 Ефективність розв'язання сформульованої проблеми

- Обороноздатність ЗСУ - швидка передача даних, оперативне прийняття рішення
- Відповідність стандартам НАТО, можливість участі в миротворчих місіях НАТО
- Зменшення невдоволення неефективністю штабного складу, задоволений військовий, довгостроковість служби
- Професійність ЗСУ - закритість даних військових для цивільних

4.4.6 Економічність розв’язання сформульованої проблеми

- Ціна втрати військового в зоні ООС
- Співфінансування по TRUST FUND NATO
- Ціна часу - процес документообігу, перезавантаження людських ресурсів ГШУ та МО

4.4.7 Політичні сили, у програмах і гаслах яких задекларовано

вирішення сформульованої проблеми

- Партія “Слуга народу”
- Партія “Європейська солідарність”
- Партія “Українська стратегія Гройсмана”
- Партія “Голос”
- Партія “ Партія Шарія”
- Партія “Опозиційна платформа “За життя”

5. Консультації

5.1. Аналіз стейкголдерів: категорії заінтересованих сторін, на яких не здійснюється вплив, але які сприяють вирішенню проблеми

“Всеукраїнські об'єднання ветеранів” [11]. Статус - Громадська організація. Зацікавленість може бути як у вирішенні проблеми так і в її утриманні. Організація покликана бути мостом між владою та ветеранською спільнотою, захищати інтереси її членів. Важелями впливу стейкхолдера є безпосереднє відчуття наслідків проблеми на своєму досвіді та довіра діючих військовослужбовців, посестрів та побратимів та авторитет організації. Комунікувати слід на початковому етапі, пояснивши суть проблеми та ефекти від її рішення. Дуже важливо досягти підтримки та співпраці у вирішення проблеми з боку організації.

Всеукраїнське об'єднання “Союз учасників миротворчих місій”[12] - (All-Ukrainian Union of Peacekeeping Operations Members). Статус - громадська організація. Зацікавленість організації перш за все полягає в захисті даних про членів миротворчих місій, в статуті організації прописано взаємодіяти із органами виконавчої влади та місцевого самоврядування з питань забезпечення соціального і правового захисту членів організації; Важелями впливу також є те, що члени організації, які приймали участь в миротворчих місіях в кооперації з миротворчими місіями інших держав можуть поділитися практичним досвідом ведення інформаційної політики чи засобами захисту інформації та навести приклади найкращих методів кібербезпеки , спираючись на практичний досвід. Комунікація має відбуватись на всіх етапах проекту, співпраця принесе більш ефективні результати.

Організація Північноатлантичного договору (НАТО) - зацікавлено в вирішенні проблеми, важелі впливу - виділення коштів на вирішення проблеми.

Служба безпеки України - захист критичної інфраструктури, є важелі на вирішення проблеми;

Міністерство економічного розвитку і торгівлі - є важіль впливу, розвиток оборонно-промислового комплексу;

Міністерство фінансів України - впливає планування бюджету та виділення коштів;

Державна служба спеціального зв’язку та захисту інформації України - формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, є важіль впливу;

Місія України при НАТО - діяльність у військово-політичній сфері в контексті імплементації планів співробітництва з НАТО;

5.2 Розподіл ідентифікованих стейкголдерів на групи:

5.2.1 цільова група:

- військовослужбовці, ветерани російсько-української війни, політики, Міністерство з питань ветеранів та тимчасово переміщених осіб

5.2.2 група непрямого впливу:

- СБУ, громадяни-сепаратисти

5.2 3 група потенційного впливу:

- працівники Держспецзв'язку

5.2 4 група з вагомим авторитетом:

- Місія України при НАТО

5.2 5 експерти:

- Державна служба спеціального зв'язку та захисту інформації України

5.2. 6 групи, які виявляють інтерес:

- спілки ветеранів

5.3 Стейкголдери, якими слід провести:

5.3.1 безпосередня форма консультацій:

- Державна служба спеціального зв'язку та захисту інформації України
- Служба безпеки України
- Мінфін
- працівники Держспецзв'язку
- РНБО
- Місія України при НАТО

5.3.2 опосередкована форма консультацій:

- Військовослужбовці
- ветерани
- Спілки ветеранів
- Міністерство з питань ветеранів та тимчасово переміщених осіб
- депутати ВРУ, політичні партії

5.4 Градуйований перелік стейкголдерів з якими необхідно провести:

5.4.1 електронні консультації:

- Місія України при НАТО
- Мінфін

- Спілки ветеранів
- військовослужбовці

5.4.2 громадські обговорення:
- Державна служба спеціального зв'язку та захисту інформації України
- СБУ
- Мінфін
- Представництво НАТО в Україні
- РНБО

5.5 Градуйований перелік стейкголдерів за очікуваним позитивним короткостроковим чи середньостроковим впливом:

позитивний короткостроковий вплив:
- Державна служба спеціального зв'язку та захисту інформації України
- РНБО
- СБУ
- Міністерство з питань ветеранів та тимчасово переміщених осіб
- Представництво НАТО в Україні

позитивний середньостроковий вплив:
- Державна служба спеціального зв'язку та захисту інформації України
- РНБО
- СБУ
- Місія України при НАТО
- Представництво НАТО в Україні
- Спілки ветеранів

5.6 Градуйований перелік стейкголдерів за очікуваним негативним короткостроковим чи середньостроковим впливом

короткостроковий негативний результат:
- Мінфін
- РНБО
- Представництво НАТО в Україні
- Державна служба спеціального зв'язку та захисту інформації України
- СБУ

середньостроковий негативний вплив:
- Проросійські партії
- РНБО
- Мінфін
- Представництво НАТО в Україні
- Державна служба спеціального зв'язку та захисту інформації України
- СБУ

5.7 Градуйований перелік організацій громадянського суспільства у статутах, проектах і гаслах яких задекларовано вирішення сформульованої проблеми:

- Партія “Слуга народу”

— *Відновимо реформування Збройних сил за стандартами НАТО*
- Партія “Європейська солідарність”

“Модернізувати армію, провести структурні реформи, встановити новий рівень грошового і соціального забезпечення військовослужбовців у відповідності до вимог НАТО”

- Партія “Українська стратегія Гройсмана”

“Забезпечити боєздатність української армії. Захистити державний суверенітет України. Впровадити заходи кібербезпеки різних інститутів та інфраструктури”

- Партія “Голос”

“Створити умови для якісного забезпечення, підвищення навичок, армійського і професійного зростання, комфорту власного побуту та побуту родин військових”

- Партія “ Партія Шарія”

“Встановлення стійкого миру та припинення війни на сході країни. - Укріплення обороноздатності армії. Армія має бути професійною, з високомотивованими та добре забезпеченими військовими, з сучасними технікою, озброєнням та логістичним забезпеченням”

- Партія “Опозиційна платформа “За життя”

Щодо оборони - програма не містить інформації.

5.8 Градуйований, перелік організацій громадянського суспільства для проведення громадської експертизи

1. Всеукраїнське об'єднання “Союз учасників миротворчих місій”
2. Всеукраїнські об'єднання ветеранів
3. ГО “Жіночий ветеранський рух”

5.9 Градуйований, перелік організацій громадянського суспільства які будуть брати активну участь у її вирішенні/не вирішенні через:

5.9.1 вплив:

- Всеукраїнське об'єднання “Союз учасників миротворчих місій”
- Всеукраїнські об'єднання ветеранів
- ГО “Жіночий ветеранський рух”

5.9.2 тиск:

- Всеукраїнське об'єднання “Союз учасників миротворчих місій”
- Всеукраїнські об'єднання ветеранів
- ГО “Жіночий ветеранський рух

5.9.3 контроль: конфіденційність

5.9.4 оцінку:конфіденційність

6. Формулювання варіантів (альтернатив) політики

6.1 Варіант 1: Збереження чинної політики

паперовий документообіг залишається, присутній витік інформації, прийняття рішень бойових рішень неефективне.

6.1.1 потенційні переваги варіанта політики

збереження бюджетних коштів, економія на закупівлю комп'ютерів, програмного забезпечення, економія на навчанні особового складу

6.1.2 потенційні недоліки варіанта політики

неефективні управлінські рішення, втрати особового складу, відсталість Збройних Сил України.

6.2 Варіант 2: ***Впровадження новітньої інформаційної системи на основі симетричного алгоритму блочного шифрування Advanced Encryption Standard*** (**AES**) [15]

6.2.1 потенційні переваги варіанта політики

Підвищення обороноздатності ЗСУ.

Впровадження політики, яка відповідатиме стандартам НАТО, що наближатиме Україну до членів Північноатлантичного альянсу.

Захист життя та безпеки військовослужбовців та членів їх сімей.

Ефективне виконання військової служби підрозділами ЗСУ внаслідок швидкої передачі даних, оперативного прийняття рішень.

Повне переоснащення засобів зв'язку новітніми технічними засобами за стандартами НАТО. Створена кібернетична система Збройних Сил.

Інвестиції. Після вступу до НАТО в економіку нових країн-членів були спрямовані серйозні інвестиції. Свого часу в Іспанію – 160 мільярдів доларів, в Угорщину – близько 50 мільярдів доларів. Подібна ситуація з Польщею і Чехією.

6.2.2 потенційні недоліки варіанта політики

Збільшення витрат з державного бюджету на закупівлю та навчання особового складу Збройних Сил України.

Відходження Укроборонпрому від залежності РФ, що може спричинити до ескалаційних дій на Сході України.

Затрати часу на процес впровадження та навчання в умовах війни.

6.3 Варіант 3: ***Впровадження системи українськими компаніям***

6.3.1 потенційні переваги варіанта політики

Авторські права належать державі, створення програми з нуля

6.3.2 потенційні недоліки варіанта політики

Збільшення витрат з державного бюджету, відсутність опиту розробки відповідних програмних продуктів для потреб Збройних Сил України

6.4 Критерії зіставлення варіантів політики

При визначенні результативності ми відштовхувались від показників результативності в п.6.2-6.3 та врахували прогноз ступеня досягнення цілей політики для відповідної альтернативи. Результативність – це міра досягнення проголошених цілей політики, тож вона визначається як відношення між цільовими показниками до прогнозованих їх значень внаслідок виробництва продуктів політики. Результати зведені у таблиці нижче. Для оцінок результативності альтернатив була обрана трибальна шкала, так як альтернатив лише три. Рейтинг визначався як сума оцінок альтернатив.

Альтернатива №1

Об'єкт впливу	***Вигоди***	***Витрати***
Держава	продовження існуючої політики	політика не потребує додаткових витрат, крім тих які закладені в бюджеті, інформаційна політика призводить до додаткових побічних витрат : виплати постраждалим військовослужбовцям, втрата техніки ЗСУ
Громадські організації	відсутні	додаткові засоби захисту, дозвіл на зброю, купівля легальної зброї, лікування
Місія України при НАТО	продовження існуючої політики	не виконання плану по впровадженню стандартів НАТО та стратегічного партнерства
Разом	-	+

Альтернатива 2

Об'єкт впливу	***Вигоди***	***Витрати***
Держава	ефективне управління ЗСУ, зменшення втрат на Сході України, (людей, техніки), відокремлення від російського впливу, реформа Сектору Безпеки і Оборони України трастовий фонд НАТО 2 мільйони 90 тисяч євро	політика потребує додаткових витрат, крім тих які закладені в бюджеті, корупційна складова
Громадські організації	Захист персональних даних,безпека життя свого та своїх рідних та близьких	Час та громадський контроль по впровадженню інформаційних систем, виявлення корупційної складової
Місія України при НАТО	виконання плану-заходу реалізація політики “курс на НАТО”, імплементація стандартів	Людський та робочий ресурс, час на впровадження та контроль виконання , політика не потребує додаткових витрат, крім тих які закладені в бюджеті
Разом	+	+/-

Альтернатива 3

Об'єкт впливу	***Вигоди***	***Витрати***
Держава	ефективне управління ЗСУ, зменшення втрат на Сході України, (людей, техніки), відокремлення від російського впливу, реформа Сектору Безпеки і Оборони України, робочі місця	політика потребує більш додаткових витрат, крім тих які закладені в бюджеті, корупційна складова , довгострокове впровадження, людський ресурс, можливий негативний результат політики без допомоги міжнародних організацій.
Громадські організації	Захист персональних даних,безпека життя свого та своїх рідних та близьких	Час та громадський контроль по впровадженню інформаційних систем, виявлення корупційної складової
Місія України при НАТО	унікальність продукту, немає контролю з боку виконання політики	ризик невідповідності стандартам НАТО, довготривалий процес, залучення великої кількості людського ресурсу,
Разом	***+/-***	***+/-***

6.5 Порівняння варіантів політики

Критерій порівняння	Оцінка варіанта (альтернативи) політики		
	Варіант 1	Варіант 2	Варіант 3
Результативність	***3 (висока)***	***1(низька)***	***2 (середня)***
Ефективність	***1***	***3***	***2***
Справедливість	***1***	***3***	***2***
Адміністративна здійсненність	***1***	***2***	***3***
Політична здійсненність	***3***	***2***	***1***
Сумарна оцінка варіанта:	***6***	***10***	***8***

7. Оцінювання політики

7.1 Цілі оцінювання

Забезпечення збереження штабної інформації в Збройних Силах України;

реалізована практично діюча єдина інформаційна система управління;

захищений військовослужбовець та його сім'я.

7.2 Організація оцінювання

Згідно плану реалізації політики, буде здійснено три етапи оцінювання політики:

- Оцінювання на етапі розробки політики, до початку реалізації.

Оцінювання проведено, виявлено проблеми, мету та альтернативний варіант реалізації політики.

- Оцінювання на етапі реалізації політики
- Оцінювання після завершення реалізації політики, оцінювання досягнутих результатів та впливу.

Відповідальними виконавцями при проведенні оцінювання будуть :

- МО
- ГШ
- НГО

Буде проведено:

- Проміжна оцінка:
  - щоквартально відповідно до реалізації політики для виявлення проблем та удосконалення процесу реалізації
  - через рік з початку реалізації
- Узагальнююча
  - після завершення реалізації політики
  - через 2 роки після завершення реалізації політик

На етапі проміжного оцінювання провест

- аналіз даних моніторингу реалізації програми на етапі пілотного проекту
- аналіз даних оперативної управлінської звітності виконавців
- аналіз спостереження за виконанням заходів проекту фокус-групи з бенефіціарами/ військовослужбовцями, що залучені до пілотного проекту реалізації
- вивчення окремих випадків реалізації впровадження електронного документообігу та навчального процесу;
- незалежний експертний аналіз стану підрозділів з кібербезпеки та середовища його розвитку.

На етапі узагальнюючого оцінювання:

- аналіз нормативно-правової бази у відповідній сфері;
- аналіз даних моніторингу реалізації політики в ЗСУ
- аналіз даних попереднього та проміжного оцінювання;
- розробка сценаріїв майбутнього розвитку підрозділів з кібербезпеки та ЗСУ;

- фокус-групи з виконавцями та бенефіціарами/військовослужбовцями
- опитування громадської думки - неможливе через сферу політики
- вивчення окремих випадків, зламування системи, технічних збоїв, процесу навчання;
- незалежний експертний аналіз змін у відповідній сфері

7.3 Проведення оцінювання

- Планування оцінки (розробка інструментів) :
- Розробити дорожню карту оцінювання та збору інформації відповідно до плану проміжного та узагальнюючого оцінювання реалізації політики
- Розробити карту розподілу обсягів ресурсів на конкретні заходи оцінки (кошторис витрат).
- Розробити карту залученості експертів на відповідних етапах реалізації політики
- Розробити попередню схему результатів оцінки
- Забезпечення конфіденційності
- Підготовка
- Розробити технічне завдання проведення оцінювання: методи, сроки
- Аналіз нормативно-правової бази
- Основні питання оцінювання політики
- Збір даних
- Спостереження, анкетування, опитування, аналіз документів.
- Аналіз отриманих даних
- Інтерпретація/аналіз/висновки оцінювання : Отримані дані, факти інтерпретувати в висновки та рекомендації
- Звіт про проведення оцінювання
- Розробити звіт про проведення оцінки впровадження політики для внутрішнього користування (сектор безпеки і оборони України) та для зовнішнього(журналісти, громадськість, зацікавлені стейкхолдери)

7.4 Результати оцінювання

Результати оцінювання - це досягнення поставлених цілей оцінювання.

Результати є конфіденційними

Оцінювання впровадження новітньої інформаційної системи з використанням симетричного алгоритму блочного шифрування Advanced Encryption Standard в Секторі безпеки і оборони України

Критерії	Питання , на які має дати відповідь оцінювання	Індикатори	Метод збору даних	Відповідальні виконавці	Терміни
Відповідність	Яким чином проект сприяє вирішенню проблеми?	Відсоток випадків витоку інформації про особовий склад ЗСУ	Опитування, Спостереження	МО/ГШ	2 р о

Результативність	Наскільки проект досяг визначених показників реалізації?	90% в/ч ЗСУ користуються електронним документообігом з захищеною системою/ Сертифіковане обладнання	Аналіз документації	МО/ГШ	ки
Ефективність	Наскільки проект досяг своїх цілей у визначені строки т в рамках запланованого бюджету?	збільшення використання сертифікованою комп'ютерною технікою та програмами до 2022р. на 90% к-сть кібер підрозділів	Аналіз документації	МО\ГШ	
Вплив	Який вплив здійснило дане впровадження політики в ЗСУ?	% готовності сектору безпеки і оборони України до кібератак % випадків витоку інформації про особовий склад ЗСУ Відсоток відповідності ЗСУ до НАТО	Опитування Аналіз документації	МО/ГШ	
Сталість	Чи буде мати політика позитивний вплив на зміни в ЗСУ після закінчення її реалізації?	Відсоток бажаючих присвятити себе службі в ЗСУ Відсоток покращення прийняття рішення Відсоток відповідності ЗСУ до НАТО	Анкетування Опитування Аналіз документації	МО/ГШ/НГО	4 роки

7.5 Рекомендації щодо подальших дій

Взяти до уваги при розробці методології та плану оцінювання конфіденційність інформації.

Поради замовнику про його подальші дії за різних сценаріїв реалізації політики.

1. Розробити план мотивування військовослужбовців до залученості до реалізації політики
2. Розробити план щодо політичного впливу/ зменшення бюджету/ згортання проекту
3. Розробити план залученості медіа та громадськості

8. Рекомендація замовнику

8.1 Рекомендований варіант політики

Варіант 2

Цей варіант підвищить обороноздатність держави, імплемнтує стандартів НАТО, ефективне управління та осучаснення Збройних Сил України.

8.2 Реалізація політики

Створення робочої групи для впровадження варіанта 2, напрацювання нормативно-правових актів.

8.3 Підтримка рекомендованого варіанту

Рекомендований варіант 2

- єдиний можливий, що відповідає визначеному курсу на Євроатлантичний альянс
- зменшення навантаження на державу, через захист військовослужбовця та його сім'ї
- національний захист та безпека держави

8.3.1 Комунікативні цілі:

- розробити комунікаційну кампанію для в\ч ЗСУ
- розробити інформаційну кампанію для в\ч ЗСУ
- розробити інформаційний бюлетень

На загал комунікація не направлена для збереження статусу конфіденційності

8.3.2 Ключові повідомлення

Сучасна Армія - безпека держави

8.3.3 Методи і способи інформування

Комунікація відбуватиметься шляхом :

- офіційного повідомлення на сайтах МО, ГШ
- внутрішнє листування з в\ч
- круглі столи стейкголдерів

- фокус-групи

Автоматизована система управління «Дніпро»

Засоби масової інформації

Соціальні мережі

8.3.4 Фінансове забезпечення

Потребує фінансування рахунок з коштів державного і місцевих бюджетів у межах асигнувань, що передбачаються на відповідний рік, міжнародної технічної допомоги, благодійної та іншої безповоротної допомоги та інших джерел.

9. Перелік посилань

1. Наказ Президента України Про затвердження Інструкції з організації обліку особового складу Збройних Сил України від 26.05.2014 №333 Електронний ресурс: https://zakon.rada.gov.ua/laws/show/z0611-14#n13
2. Закон України “Про внесення змін до Конституції України (щодо стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору)” від 7 лютого 2019 року Електронний ресурс: https://zakon.rada.gov.ua/laws/show/2680-19
3. https://tyzhden.ua/Society/91232
4. Сайт “Трибунал “ - Електронний ресурс: http://tribunal-today.ru/
5. МОУ “Щоденні кіберзагрози” - Електронний ресурс http://www.mil.gov.ua/ukbs/shhodenni-kiberzagrozi/
6. Наказі Міністерства оборони України № 650 від 17.09.2014 р. про затвердження Концепції інформатизації Міністерства оборони України - Електронний ресурс:http://www.mil.gov.ua/content/other/MOU650_2014.pdf
7. Закон України “Про захист персональних даних” - Електронний ресурс - https://zakon4.rada.gov.ua/laws/show/2297-17
8. Закон України “Про державну таємницю” -- Електронний ресурс - https://zakon.rada.gov.ua/laws/show/3855-12
9. Національна програма інформатизації -Електронний ресурс http://search.ligazakon.ua/l_doc2.nsf/link1/JH72M00A.html
10. Закон України "Про захист інформації в автоматизованих системах" - Електронний ресурс - https://zakon.rada.gov.ua/laws/show/2594-15
11. Всеукраїнське об'єднання ветеранів - Електронний ресурс - http://dsvv.gov.ua/finansova-pidtrymka-hromadskyh-ob-ednan-veteraniv/monitorynh-ta-zvitnist-krnkurs-2018/vseukrains-ke-ob-iednannia-veteraniv.html

12. Всеукраїнське об'єднання “Союз учасників миротворчих місій” - Електронний ресурс: : https://www.facebook.com/pages/category/Community-Organization/Союз-Учасників-Миротворчих-Операцій-382295005192829/
13. Аміна Окуєва - Електронний ресурс: - https://ru.wikipedia.org/wiki/Окуева,_Амина_Викторовна
14. Анастасія Гончарова - Електронний ресурс -https://kp.ua/incidents/508566-podrobnosty-hybely-lysy-yz-pravoho-sektora-razvedchytsu-zastrelyly-pod-maryupolem
15. ***Advanced Encryption Standard*** (**AES**) - Електронний ресурс - https://uk.wikipedia.org/wiki/Advanced_Encryption_Standard