КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (12), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.12.6168
УДК 004.056

Дзюба Тарас Михайлович
кандидат технічних наук, доцент
доцент кафедри Управління інформаційною та кібернетичною безпекою
Державний університет телекомунікацій, Київ, Україна
ORCID ID: 0000-0001-6607-2507
iwartar@gmail.com

Опанасенко Максим Ігорович
аспірант
кафедра Управління інформаційною та кібернетичною безпекою
Державний університет телекомунікацій, Київ, Україна
ORCID ID: 0000-0002-5010-9376
matrosovmaxim62@gmail.com

РОЗРОБЛЕННЯ ПАСПОРТУ ЗАГРОЗИ ДЛЯ СИСТЕМИ РАННЬОГО ВИЯВЛЕННЯ ЗАГРОЗ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

Анотація. У статі розглянуто проблеми виявлення загроз національній безпеці держави, зокрема в інформаційній сфері, а також шляхи їх вирішення. Проаналізовано досвід провідних країн щодо підходів до створення та функціонування національних систем виявлення ризиків та загроз, а саме Сполучених Штатів Америки, Великої Британії, Королівства Нідерландів та Нової Зеландії. Визначено значний вплив особливостей інформаційної сфери при формуванні ризиків і загроз усіх безпекових сфер. Особливу увагу приділено питанням спрямування та націлювання процесу моніторингу на пошук певних маркерних подій, які дадуть можливість створювати чітку уяву про початок формування ризиків та визначати загрози на ранніх стадій. Обгрунтовано доцільність розроблення Паспорта загроз національній безпеці держави для його узгодженого використання в системі виявлення та оцінки загроз в усіх безпекових сферах, зокрема для системи раннього виявлення загроз в інформаційній сфері. Проведено аналіз теоретичних засад розробки паспортів загроз. Запропоновано уніфіковану структуру Паспорта, який враховує переважну більшість аспектів процесу формування ризиків з перетіканням у загрози національній безпеці держави. Наведена зміст основних та інформаційних аспектів розробленого Паспорту. З огляду на багатофункціональність Паспорта загроз відмічено, що ступінь його деталізації має важливе значення для можливості його використання для розроблення системи раннього виявлення загроз в інформаційній сфері держави. Визначено, що розробка Паспорту виконується на невизначений термін з подальшим корегуванням та внесенням нових даних у зв'язку з динамікою безпекового середовища. Встановлено, що для раннього виявлення загроз необхідно розглядати процеси формування і виявлення ризиків з акцентом на їх початкові латентні стадії. Даний підхід поєднує опис (оцінки) і відповідної загрози і її представлення в інформаційному просторі.

Ключові слова: загрози; ризики; сфери національної безпеки; інформаційна сфера; паспорт загроз; система виявлення й оцінки загроз, система раннього виявлення загроз.

ВСТУП

Аналіз збройних конфліктів у світі за останні 10-15 років дозволяє зробити висновок, що сьогодні основним типом війни є гібридна війна, як поєднання застосування військової сили з різними невоєнними механізмами в єдиній системі для примушення жертви прийняти волю агресора. Не менш важливим є висновок, що у XXI сторіччі будь-яка війна є загрозою вже не тільки для регіональної, але й для міжнародної безпеки, тобто в умовах глобалізації економіки та єдиного інформаційного простору

локальні та регіональні збройні конфлікти вже стосуються практично кожної держави світу.

Збройна агресія, розв'язана Російською Федерацією проти України в 2014 році, не є виключенням. Агресивні наміри РФ було реалізовано через застосування різноманітних поєднань інструментів і методів, до числа яких спеціалісти відносять: конвенціональні та нерегулярні бойові операції; підтримку і супроводження політичних протестів; економічний тиск; кібер операції; інтенсивну дезінформаційну кампанію [1]. Інформаційна кампанія Росії проти України та світу стала стратегічним центром тяжіння, як безпосередньо в цій війні, так і в сучасних геополітичних процесах.

У зв'язку з переходом від силових методів боротьби до несилових, м'якої сили та мережевих війн, характер впливів значно змінився. Сьогодні головною зброєю являється вплив інформаційний з метою підриву державного суверенітету. Це докорінно змінило фокус дискусій щодо сутності гібридних воєн й стало поштовхом для розроблення нових стратегій зміцнення оборонних спроможностей протидії гібридним загрозам провідними державами світу. Цей серйозний виклик для сектора безпеки кожного суб'єкта міжнародних відносин зумовлює пошук дієвих рішень, спрямованих на розроблення методик і систем виявлення й оцінки загроз в інформаційній сфері держави.

Розробленням таких систем займаються науковці усіх сфер безпеки держави, адже інформаційна складова присутня практично у всіх складових національної безпеки. Та віднедавна кут зору на цю проблему почав зміщуватися в бік розроблення систем раннього виявлення загроз, так як в момент повної ініціалізації загрози, усі зусилля з її протидії чи нейтралізації вже не мають необхідного ефекту або потребують значних часових та матеріальних ресурсів для ліквідації наслідків.

Постановка проблеми. На сьогоднішній день, в Україні, інтегрована система оцінки інформаційних загроз та реагування на них досі не створена. В проекті відповідної державної Концепції (2019 рік, розробник – Міністерство інформаційної політики України) йдеться про те, що коригування стратегії держави в інформаційній сфері має включати формування підходів та спроможностей раннього виявлення інформаційних повідомлень та їх поширення, які можуть становити загрозу для національних інтересів України. Така система має ґрунтуватися на засадах раннього попередження осіб, що приймають управлінські рішення, про загрози та ризики інформаційного характеру, що з'являються в інформаційному просторі, з метою їх об'єктивної та всебічної оцінки, підготовлення та здійснення відповідного реагування [2].

На даний час наукові публікації з даної тематики свідчать про розбіжності у поглядах щодо вибору інструментарію для реалізації цього завдання. Науковцями проведено всебічний системний аналіз природи інформаційних впливів, джерел їх виникнення, методів та етапів створення інформаційних продуктів деструктивного характеру та способів їх передачі до цільової аудиторії. Поряд з цим існує погляд, що найбільш дієвим інструментом на рівні національному є розроблення паспорту загроз національній безпеці держави у різних безпекових сферах, з описом їх характерних ознак та належності до певного класу для чіткої ідентифікації усього можливого спектру загроз. Так як паспорт загроз – це документ, який передбачає оцінку подій, що створюють небезпеку, його розроблення дасть можливість спрямувати існуючі можливості щодо ведення цільового моніторингу інформаційного простору у необхідне русло в межах функціонування системи раннього виявлення загроз в інформаційній сфері держави.

Аналіз останніх досліджень і публікацій. Сьогодні в наукових колах все частіше обговорюється питання, щодо недостатньої ефективності виявлення загроз в інформаційній сфері в момент їх повної ідентифікації. Боротьба за настрої та прихильність окремих груп суспільства починається задовго до реалізації агресивних дії супротивної сторони і в момент виявлення загрози деструктивні процеси вже є незворотніми. В цьому аспекті значно більший інтерес представляє можливість відтворювати плани та задуми противника за складовими ланцюга змодельованих інформаційно-маніпулятивних актів, володіючи даними лише його початкових ланок. Цінність таких можливостей полягає у тому, що відтворення запущеного процесу інформаційного впливу має відбутися задовго до того, як увесь процес буде повністю завершений і визначений як певна загроза. Такі дії з аналізу інформаційного простору мають риси прогнозування, які через багатоваріантність можливого розвитку подій дуже складно піддаються моделюванню й формалізації.

Інформації про створення систем раннього виявлення загроз, базових підходів і механізмів до їх реалізації у відкритих джерелах практично немає. Переважно, в наукових дослідженнях з даної тематики висвітлюються питання виявлення інформаційних ризиків чи загроз в кожному окремому середовищі розповсюдження та передачі інформації, їх детальна класифікація й т.і. Так авторами запропоновано рішення щодо виявлення інформаційних операцій в соціальних мережах, в сервісах мережі Інтернет або в засобах масової комунікації, посягання на конфеденційну інформацію окремих підприємств, установ та організацій [3]. За допомогою програмних продуктів, розроблених на основі вищезазначених досліджень, проводиться моніторинг інформаційного середовища за запитом фахівців, які здійснюють відбір релевантної інформації, її аналіз й оброблення. Тобто результати моніторингу залежить від вдало сформульованих інформаційних запитів з досліджуваної проблематики та інтуїтивно-професійних якостей фахівців.

Однак допоки такі процеси моніторингу носять дещо фрагментативний або ситуативний характер і не мають системного цільового підходу. Для виявлення ризиків та загроз на початкових стадіях процес моніторингу має бути спрямований на пошук маркерних подій, про які необхідно мати чітку уяву. На думку Ситника Г.П. [4] такі орієнтири для пошуку може надати саме паспорт загроз оснований на глибокому аналізі багатьох аспектів процесу (алгоритму) формування викликів, ризиків та загроз інформаційної сфери з необхідним ступенем їх деталізації.

За своєю сутністю, саме поняття “раннього виявлення загроз” наштовхує на думку, що для розроблення паспорту необхідно розглянути процеси формування і виявлення ризиків з акцентом на їх початкові латентні стадії з подальшим прогнозуванням загроз національній безпеці держави.

Тому **метою статті є** на основі алгоритму формування ризиків з перетіканням у загрози національній безпеці держави та рекомендацій зі створення паспорту загроз національній безпеці держави, визначити необхідний обсяг параметрів паспорту загроз національній безпеці держави у інформаційній сфері у межах реалізації завдання розроблення системи раннього виявлення загроз.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Більшість провідних країн світу приділяє значну увагу вирішенню питань пов’язаних із оцінкою характеру, масштабів, структур та джерел сучасних викликів, ризиків, загроз та небезпек національній безпеці. Події, які відбувались в світі, на кшталт

глобальної фінансової кризи в 2008 році, революційні події в арабських країнах, збройна агресія з боку Російської Федерації на окупованих територіях Донецької та Луганської області, анексія Криму, вихід Великої Британії зі складу Європейського Союзу та поширення COVID-19, які дестабілізують міжнародну і регіональну обстановку, продемонстрували низьку готовність провідних аналітичних центрів та розвідувальних структур до передбачення та реагування на загрози, що негативно вплинули на стан захищеності держав.

Досвід розбудови та функціонування національних систем оцінки ризиків та загроз кращих світових практик свідчить про необхідність створення власного системного підходу до розроблення системи оцінки загроз. В Новій Зеландії основою методологією оцінки ризиків є те, що всі ризики на національному рівні можна порівнювати, використовуючи стандартний набір принципів і правил, однакові параметри і критерії, основними з яких є ймовірність ризику та важкість наслідків [5]. У Великій Британії система оцінки загроз і ризиків функціонує комплексно і послідовно в єдиному алгоритмі у рамках циклу стратегічного планування у сфері національної безпеки. При проведенні оцінки ризиків і загроз в ієрархічній структурі управління системи застосовується принцип "зверху донизу", відповідно до якого загальнонаціональна оцінка ризиків і загроз є основою для розробки відповідних оцінок на регіональному та місцевому рівнях. Публічно доступною версією Національної оцінки ризиків є Національний реєстр ризиків надзвичайних ситуацій у сфері цивільного захисту (National Risk Register of Civil Emergencies) [6]. Привертає увагу досвід Королівства Нідерландів щодо розроблення національного профілю ризиків (National Risk Profile) При створенні якого враховується також загальний контекст ситуації і довгострокові мегатренди, досліджуються причини виникнення загрози, тригери, фактори впливу, каскадні ефекти, розробляються сценарні прогнози тощо. Крім того, оцінюються наявні спроможності для реагування на ситуацію на етапах запобігання, підготовки, встановлення контролю за ситуацією, реагування і ліквідації наслідків; визначаються уразливості; оцінюється вплив невизначеності. З урахуванням отриманих результатів розробляються висновки і рекомендації щодо посилення спроможностей і розбудови національної стійкості [Нідерланди] [7], [8].

Акумулювавши міжнародний досвід вітчизняні вчені пропонують уніфікувати підхід до розроблення систем виявлення й оцінки загроз, зокрема й раннього виявлення, шляхом створення паспорту (матриці) загроз національній безпеці України.

Паспорт (матриця) загрози національній безпеці – це документ, який передбачає оцінку подій, явищ, процесів, інших чинників, що створюють небезпеку реалізації життєво важливим національним інтересам, характеристику їх можливого розвитку (масштаб, тенденції розвитку, можливі наслідки для національної безпеки тощо), а також визначення основних організаційно-правових та інших механізмів діяльності суб'єктів забезпечення національної безпеки по реагуванню на загрози (моніторинг, превентивні дії, локалізація, тощо)[9].

Очевидно, що розробити такі паспорти представляється можливим лише на невизначений термін, коли дана загроза є актуальною. В подальшому вони потребуватимуть постійного корегування та розроблення нових з врахуванням динаміки змін безпекового середовища. Тому важливим завданням постає визначення таких описових аспектів процесу формування загроз, які дадуть можливість охарактеризувати їх будь-який вид та клас. Для цього форма й структура паспорта загроз має бути уніфікованою для усіх сфер національної безпеки.

Зважаючи на міжнародний досвід [10] та результати наукових досліджень вітчизняних вчених пропонується визначити структуру паспорта загрози і включити такі основні компоненти:

I. Загальні аспекти:

1. Найменування загрози;
2. Шифр загрози (відповідно до сфери національної безпеки);
3. Національні інтереси, яких стосується загроза;
4. Сфери національної безпеки, яких стосується загроза;
5. Масштаб загрози (регіон України, Україна в цілому, Європа, світ);
6. Достатність інформації про загрозу (можливість точно та детально визначити і оцінити загрозу);
7. Рівень загрози: низький, середній, високий;
8. Ймовірність реалізації загрози (ймовірність понесення втрат від реалізації загрози): низька, середня, висока, катастрофічна;
9. Орієнтовний час до реалізації загрози та понесення втрат: роки, місяці, дні, години;
10. Об'єкти, на які спрямована реалізація загрози (керівництво, населення, галузі економіки, об'єкти критичної інфраструктури тощо);
11. Джерело загрози (агресивна політика іноземної країни, наміри застосування збройних сил проти України, активізація терористичної діяльності, зростання злочинності, природні катаклізми, хвороби тощо);
12. Можливі наслідки реалізації загрози (можливі втрати):

- життя людей;
- здоров'я людей;
- довіра до влади;
- рівень дестабілізації суспільних відносин;
- фінансові та ресурсні;
- рівень міжнародної підтримки України та засудження дій агресора (ООН, ОБСЄ, НАТО, США, Великобританія, ЄС, Франція, Німеччина, Польща, країни Балтії, Угорщина, Румунія, Канада, Китай, Японія, Туреччина, Великобританія, Азербайджан, Грузія, Молдова);
- часові (збільшення часу на реалізацію оборонних заходів, на реалізацію державних програм, на стабілізацію ситуації з COVID, на покращення життя населення тощо).

II. Інформаційні аспекти (додатково до основного опису)

13. Зміст основних наративів (ліній переконання), які супроводжують реалізацію загрози;
14. Цільові аудиторії, на які спрямовані заходи інформаційного супроводження реалізації загрози з визначенням їх доступності;
15. Інформаційні джерела, які супроводжують реалізацію загрози;
16. Канали реалізації заходів інформаційного супроводження реалізації загрози;
17. Кількість інформаційних матеріалів, спрямованих на реалізацію загрози, частота їх повторення, кількість поширень;
18. Впливовість та популярність авторів інформаційних матеріалів/заяв/повідомлень, спрямованих на реалізацію загрози;
19. Реагування цільових аудиторій на інформаційні матеріали, які супроводжують реалізацію загрози: підтримують/засуджують, поширюють, коментують;

20. Тенденція зміни інтенсивності інформаційних заходів, які супроводжують реалізацію загрози: збільшення/зменшення;

21. Перелік методів, за якими здійснюється оцінка рівня загрози;

22. Список експертів, що брали участь в оцінці стану і тенденцій розвитку загрози.

Наведений авторський підхід до визначення паспорту загроз національній безпеці України поєднує опис (оцінки) і відповідної загрози і її представлення в інформаційному просторі. Завдяки такому підходу стає можливим раннє виявлення загрози шляхом моніторингу інформаційного простору та порівняння його станів в динаміці стосовно різних сфер національної безпеки України.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Запропонований паспорт загроз національній безпеці держави враховує переважну більшість характерних аспектів загроз, незалежно від безпекової сфери, для реалізації уніфікованого підходу до розроблення системи виявлення та оцінки загроз, зокрема системи їх раннього виявлення в інформаційній сфері держави. В подальшому деталізація окремих аспектів паспорту дасть можливість створити науково-методичне підґрунтя для ідентифікації за розробленим паспортом латентних початкових станів формування ризиків для системи раннього виявлення загроз в інформаційній сфері.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Giles Keir. (2016). *NATO Defense College Cataloguing in Publication-Data: Handbook of Russian Information Warfare.* DeBooks Italia srl. https://www.researchgate.net/publication/313423985_Handbook_of_Russian_Information_Warfare.
2. *Концепція інтегрованої системи оцінки інформаційних загроз та реагування на них*. (2018). https://www.documentcloud.org/documents/20600270-kontseptsiia-isomizor
3. Dodonov A., Lande D., Tsyganok V., Andriichuk O., Kadenko S. & Graivoronskaya A. (2017). *Information Operations Recognition: from Nonlinear Analysis to Decision-making.* IPRI of NAS of Ukraine.
4. Ситник Г. П., Абрамов В. І., Мандрагеля В. А., Шевченко М. М. & Шипілова Л. М. (2012). *Обґрунтування концептуальних та організаційно-правових засад розробки паспортів загроз національній безпеці України.* НАДУ.
5. *AS/NZS ISO 31000:2009 Risk management — Principles and guidelines*. (2009). https://infostore.saiglobal.com/preview/293451727151.pdf?sku=119718_SAIG_AS_AS_274522
6. *The National Security Strategy and Strategic Defence and Security Review.* (2015). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf
7. *National Security Strategy of Netherlands*. (2019). https://english.nctv.nl/topics/nationalsecuritystrategy/documents/publications/2019/09/19/national-security-strategy
8. Резнікова О. О., Войтовський К. Є. & Лепіхов А. В. (2020). *Національні системи оцінки ризиків і загроз: кращі світові практики, нові можливості для України*. НІСД.
9. Абрамов В. І., Андреєв С. О., Дацюк А. В., Завгородня С. П., Кириленко В. І., Клименко Н. Г., Кравченко В. В., Мандрагеля В. А., Марутян Р. Р., Орел М. Г., Сальнікова О. Ф., Ситник Г. П., Смолянюк В. Ф., Устименко О. В. & Шевченко М. М. (2016). *Глобальна та національна безпека*. НАДУ.
10. Office of the Director of National Intelligence. (2021). *Annual threat assessment of the US intelligence community.* https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (12), 2021
ISSN 2663 - 4023

Dzuba Taras
PhD, assistant professor
Assistant professor of Department of Management of Information and cyber security
State University of Telecommunications, Kiev, Ukraine
ORCID ID: 0000-0001-6607-2507
iwartar@gmail.com

Opanasenko Maksym
PhD student of Department of Management of Information and cyber security
State University of Telecommunications, Kiev, Ukraine
ORCID ID: 0000-0002-5010-9376
matrosovmaxim62@gmail.com

ROSE PASSPORT OF A THREAT FOR THE EARLY DETECTION SYSTEM OF THREAT TO THE NATIONAL SECURITY OF UKRAINE

Abstract. The article considers the problems of identifying threats to national security, in particular in the information sphere, as well as ways to solve them. The experience of leading countries in approaches to the establishment and operation of national risk and threat detection systems, namely the United States, the United Kingdom, the Kingdom of the Netherlands and New Zealand, is analyzed. The significant influence of the peculiarities of the information sphere in the formation of risks and threats of all security spheres is determined. Particular attention is paid to the direction and focus of the monitoring process on the search for certain marker events that will provide a clear idea of the beginning of the formation of risks and identify threats in the early stages. The expediency of development of the Passport of threats to national security of the state for its coordinated use in the system of detection and assessment of threats in all security spheres, in particular for the system of early detection of threats in the information sphere is substantiated. The analysis of theoretical bases of development of passports of threats is carried out. A unified structure of the Passport is proposed, which takes into account the vast majority of aspects of the process of risk formation with the threat to national security. The content of the main and informational aspects of the developed Passport is given. Given the multifunctionality of the Threat Passport, it is noted that the degree of its detail is important for the possibility of its use for the development of a system of early detection of threats in the information sphere of the state. It is determined that the development of the Passport is carried out indefinitely with further adjustment and introduction of new data in connection with the dynamics of the security environment. It is established that for early detection of threats it is necessary to consider the processes of formation and detection of risks with an emphasis on their initial latent stages. This approach combines the description (assessment) and the corresponding threat and its presentation in the information space.

Keywords: threats; risks; spheres of national security; information sphere; threat passport; early detection system.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Giles Keir. (2016). *NATO Defense College Cataloguing in Publication-Data: Handbook of Russian Information Warfare.* DeBooks Italia srl. https://www.researchgate.net/publication/313423985_Handbook_of_Russian_Information_Warfare.
2. *The concept of an integrated system for assessing and responding to information threats*. (2018). https://www.documentcloud.org/documents/20600270-kontseptsiia-isomizor
3. Dodonov A., Lande D., Tsyganok V., Andriichuk O., Kadenko S. & Graivoronskaya A. (2017). *Information Operations Recognition: from Nonlinear Analysis to Decision-making.* IPRI of NAS of Ukraine.
4. Sytnyk H. P., Abramov V. I., Mandrahelia V. A., Shevchenko M. M. & Shypilova L. M. (2012). *Substantiation of conceptual and organizational and legal bases of development of passports of threats to national security of Ukraine.* NADU.

5. *AS/NZS ISO 31000:2009 Risk management — Principles and guidelines*. (2009)/ https://infostore.saiglobal.com/preview/293451727151.pdf?sku=119718_SAIG_AS_AS_274522
6. *The National Security Strategy and Strategic Defence and Security Review.* (2015). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf
7. *National Security Strategy of Netherlands*. (2019). https://english.nctv.nl/topics/nationalsecuritystrategy/documents/publications/2019/09/19/national-security-strategy
8. Reznikova O. O., Voitovskyi K. Ye. & Lepikhov A. V. (2020). *National systems of risk and threat assessment: world best practices, new opportunities for Ukraine*. NISS.
9. Abramov V. I., Andreiev S. O., Datsiuk A. V., Zavhorodnia S. P., Kyrylenko V. I., Klymenko N. H., Kravchenko V. V., Mandrahelia V. A., Marutian R. R., Orel M. H., Salnikova O. F., Sytnyk H. P., Smolianiuk V. F., Ustymenko O. V. & Shevchenko M. M. (2016). *Global and national security.* NADU.
10. Office of the Director of National Intelligence. (2021). *Annual threat assessment of the US intelligence community. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf*