УДК 355.4+005.33
д.т.н. Чевардін В.Є. (ORCID 0000-0002-1070-4568, ВІТІ)
к.т.н. Мазулевський О.Є. (ORCID 0000-0002-6042-2577, ВІТІ)

АНАЛІЗ СТРУКТУР КІБЕРКОМАНДУВАННЬ РОЗВИНУТИХ КРАЇН

З розширенням кількості інформаційних послуг, поширенням Інтернету речей, створенням систем управління та підтримки прийняття рішень з елементами штучного інтелекту кіберпростір все більше поширюється в усі сфери життєдіяльності людини. Це призвело до створення і розвитку систем кіберзахисту об'єктів критичної інфраструктури, як у цивільній так і військовій сферах. У статті проведено аналіз структур військових органів управління систем захисту кіберпростору – "кіберкомандування" таких країн, як Сполучені Штати Америки, Федеративної Республіки Німеччини, Французької Республіки, Об'єднаного Королівства, Російської Федерації. З проведеного порівняльного аналізу потенційних можливостей, фінансування і чисельності кібервійськ розвинених країн видно найбільш потужні країни в сфері кіберзахисту, це Китай і Сполучені Штати. Однак, якщо взяти до уваги створення Європейської колективної системи кібербезпеки, в яку входить 25 країн, то ця система за чисельністю ІТ-фахівців, рівнем і фінансуванням буде найпотужнішою з усіх сьогодні відомих. З цього можна зробити висновок, що створення колективних систем протидії кіберзагрозам є перспективним напрямком розвитку потужних систем кіберзахисту і впливу. Створення сучасних колективних систем кібербезпеки реалізується шляхом розміщення на території різних країн центрів реагування на кіберзагрози і оповіщення про кіберінциденти (з програмним і апаратно-програмним забезпеченням), починаючи з периметра мережі, закінчуючи всією ІТ-інфраструктурою країни. У зв'язку з цим, у провідних країнах були створені кіберкомандування і постійно триває нарощування спроможностей кібер-військ (сил). У статті запропоновано варіант складу функцій забезпечення кіберзахисту інформаційно-телекомунікаційної системи ЗС України, в якому виділені основні функції покладені на сили кіберзахисту Збройних Сил України.

***Ключові слова**: кібербезпека, кіберкомандування, збройні сили.*

***Чевардин В.Є., Мазулевський О.Є. Анализ структур киберкомандований развитых стран.** С расширением количества информационных услуг, распространением Интернета вещей, созданием систем управления и поддержки принятия решений с элементами искусственного интеллекта киберпространство все больше распространяется во все сферы жизнедеятельности человека. Это привело к созданию и развитию систем киберзащиты объектов критической инфраструктуры, как в гражданской так и военной сферах. В статье проведен анализ структур военных органов управления систем защиты киберпростанства – "киберкомандований" таких стран, как Соединенные Штаты Америки, Федеративной Республики Германии, Французской Республики, Объединённого Королевства, Российской Федерации. Из проведенного сравнительного анализа потенциальных возможностей, финансирования и численности кибервойск развитых стран видно наиболее мощные страны в сфере киберзащиты, это Китай и Соединенные Штаты. Однако, если принять во внимание создание Европейской коллективной системы кибербезопасности, в которую входит 25 стран, то эта система по численности ИТ-специалистов, уровнем и финансированием будет самой мощной из всех сегодня известных. Из этого можно сделать вывод, что создание коллективных систем противодействия киберугрозам является перспективным направлением развития мощных систем киберзащиты и воздействия. Создание современных коллективных систем кибербезопасности реализуется путем размещения на территории различных стран центров реагирования на киберугрозы и оповещения про киберинциденты (с программным и аппаратно-программным обеспечением), начиная с периметра сети, заканчивая всей ИТ-инфраструктурой страны. В связи с этим, в ведущих странах были созданы киберкомандования и постоянно продолжается наращивание мощностей кибер-войск (сил). В статье предложен вариант состава функций обеспечения киберзащиты информационно-телекоммуникационной системы ВС Украины, в котором выделены основные функции возложеные на силы киберзащиты Вооруженных Сил Украины.*

***Ключевые слова**: кибербезопасность, киберкомандование, вооруженные силы.*

***V.Chevardin, O.Mazulevsky Analysis of cyber commands of developed countries.** With the expansion of information services, the expansion of the Internet of Things, the creation of management and decision support systems with elements of artificial intelligence, cyberspace is expanding and penetrating more and more areas of human activity. This led to the development of cyber defense systems for critical infrastructure. In the structures research of "cybercommand" of such countries as the United States of America, the Federal Republic of Germany, the French Republic, the United Kingdom, and the Russian Federation were analyzed. The comparative analysis of the potentials, funding, and numbers of cyberwarfare developed countries shows that the most powerful countries in the field of cyber defense are China and the United States. However, given the creation of a 25-nation European Collective Cyber Security System, this system is the most powerful of all known to date in terms of the number of IT professionals and their level and funding. From this it is possible to conclude that the creation of collective systems for counteraction to cyber threats is a promising direction for the development of powerful cyber defense systems and influence. Creation of modern collective cybersecurity systems is realized through the establishment of cyber-threat response centers and cyber-incident alerts (with software and hardware) on the territory of different countries, starting from the perimeter of the network, ending with the entire IT infrastructure of the country. In this regard, cyber commands have been*

established in the leading countries and the capacity of the cyber forces (troops) is continuing to increase. In the article was proposed a variant of the set of the cyber defense functions for the information and telecommunication system of the Armed Forces of Ukraine, which outlined the main functions assigned to the cyber defense forces of the Armed Forces of Ukraine.

***Key words**: cyber security, cybercom, armed forces.*

Постановка завдань. Бурхливий розвиток інформаційних технологій і проникнення інформаційно-телекомунікаційних мереж в усі сфери життєдіяльності суспільства обумовили появу нової (віртуальної) площини життя суспільства, функціонування органів державної влади та розвитку суспільства. Ця площина, з часом, отримала назву кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [1]. З розширенням кількості інформаційних послуг, поширенням використання Інтернету речей, створенням систем управління та підтримки прийняття рішень з елементами штучного інтелекту кіберпростір поширився і все більш проникає в усі сфери життєдіяльності людини.

Інтернет став невід'ємною складовою розвитку та фінансового збагачення більшості організацій, компаній та урядів провідних країн, з одного боку. З іншого боку, проникнення мережі Інтернет до кожного дому, до кожної людини створило підґрунтя, як для здійснення простих фінансових махінацій, так і для створення кіберзагроз системам управління транспортом, літаками, електростанціями та іншим об'єктами критичної інфраструктури.

Аналіз літератури. Аналіз літератури показав, що залежність багатьох сфер діяльності суспільства від безпеки у кіберпросторі, призвела до руху провідних країн в напрямку розбудови систем кіберзахисту об'єктів критичної інфраструктури. Одним із прикладів є те, що Європейською комісією було розроблена програма забезпечення безпеки критичної інфраструктури та прийнято низку важливих нормативних актів щодо розбудови розгалуженої системи кібербезпеки Європи [3-7]. Подальший аналіз джерел інформації показав, що сьогодні і в нашій державі відбувається інтеграція міжнародних і європейських стандартів та формування нової власної нормативно-правової бази в сфері кіберзахисту [1, 3-7], в тому числі і в Збройних Силах України.

Згідно закону України [1] Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до своїх компетенції здійснюють різні заходи, з яких одним з головних є підготовка держави до відбиття воєнної агресії у кіберпросторі і впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану. Ці завдання обумовлені тим, що кіберпростір став окремим полем здійснення інформаційної боротьби та іншого впливу на системи управління об'єктами критичної інфраструктури держави. В зв'язку з цим, рівень розвитку інформаційної інфраструктури держави, її економічний потенціал, географічне положення та політичні інтереси визначають потреби та вимоги до системи кібербезпеки держави, які в різних країнах суттєво можуть відрізнятись. Це в свою чергу викликає потребу в визначенні варіанту побудови структури військ кібербезпеки Збройних Сил України, враховуючі, що кібервійська різних країн відрізняються за структурою, чисельністю та своїми функціями.

Метою даної роботи є проведення огляду підходів різних країн щодо побудови системи кібербезпеки збройних сил провідних країн світу та визначення основних функцій системи кібербезпеки ЗС України.

Викладення основного матеріалу. Далі пропонується розглянути аналіз структур та призначення військ сил кіберзахисту Збройних Сил розвинутих країн світу:

Сполучені Штати Америки. Збройні Сили Сполучених Штатів Америки вважаються найпотужнішими в світі. Вони складаються з чотирьох компонентів: сухопутні війська, військово-повітряні сили, військово-морські сили, берегова охорона, які підпорядковуються міністерству оборони країни. Чисельність Збройних Сил Сполучених Штатів Америки складається з регулярних військ – приблизно 1,5 млн. осіб на 2009 рік та резерву – це 851

тис. осіб на 2009 рік. На 2019 рік ці цифри змінилися не суттєво. Сучасні Збройні Сили Сполучених Штатів складаються з одинадцяти командувань, в тому числі європейського командування U.S. European Command (USEUCOM), тихоокеанського командування U.S. Pacific Command (USPACOM), північного командування U.S. North Command (USNORTHCOM), південного командування U.S. South Command (USSOUTHCOM), інтереси яких розповсюджуються на всю територію світу. Завдання, які постають перед ЗС щодо загального керування, логістичного і всебічного забезпечення, інформаційної підтримки військ, сил, під час підготовки та проведення операцій в різних частинах світу, на різних театрах бойових дій і в різних умовах потребують швидкого реагування та прийняття рішень. Це, в свою чергу, створює високі вимоги до системи обміну та захисту інформацією та кіберзахисту інфраструктури. В зв'язку з цим, в ЗС США було створено окреме командування – кіберкомандування United States Cyber Command (USCYBERCOM), структура якого наведена на рис. 1 [8].

USCYBERCOM планує, координує, об'єднує, синхронізує і проводить дії для:

- керування функціонуванням і захистом спеціалізованих інформаційних мереж Міністерства оборони США;

- підготовки до, і за наказом, проведення повного спектру військових дій у кіберпросторі, щоб вирішити проблеми у всіх галузях, гарантуючи Американську/Союзницьку свободу дій в кіберпросторі та унеможливлюючи це ж саме для супротивника [9].

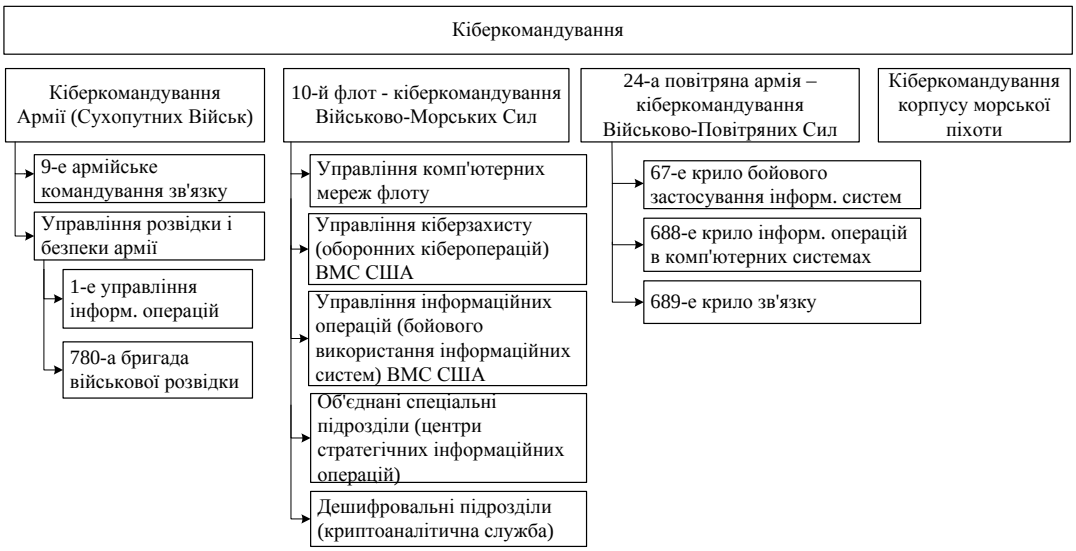

Рис. 1. Структура Кіберкомандування США

Завданнями кіберкомандування США є:

1) планування, проведення та координація кібероперацій з метою забезпечення і запобігання зовнішньої агресії, забезпечення свободи дій оперативних і сухопутних (берегових, інших) формувань військ (сил) при досягненні переваги у кіберпросторі.

2) забезпечення технічної підтримки, надійності, безпеки та захисту каналів управління, включаючи комп'ютерні та космічні системи в секторі відповідальності.

3) керівництво діяльністю сил і засобів радіоелектронної боротьби, радіоелектронної розвідки та служби дешифрування.

4) досягнення можливостей включення військ (сил) в об'єднанні командування збройних сил кібер-, інформаційних, криптологічних і космічних та інших операцій.

5) приведення глобальної комп'ютерної мережі військ (сил) у відповідність до загальних оперативних потреб кіберзахисту Збройних Сил країни.

Вирішення цих питань потребують ретельної комплексної підготовки військ (сил) та високої відповідальності, професійних якостей, навченості особового складу, надійності та

ефективності роботи інформаційно-телекомунікаційної складової системи кібербезпеки країни. Для цього в Сполучених Штатах Америки протягом десяти років створювалась потужна система кібербезпеки держави, яка має спроможності, як бойового застосування, так і підготовки та розвитку військ, сил в мирний час. Система кібербезпеки США складається з різних фахівців, як військових, так і цивільних, які в змозі виконувати складні завдання з забезпечення захисту кіберпростору.

Наприклад, управління кіберзахисту (оборонних кібероперацій) ВМС США, яке базується на військово-морській базі Норфолка (штат Віргінія), відповідає за бесперебійне функціонування мережі FORCENET, відбиття кібератак та ліквідацію наслідків після атак в межах військово-морського сегменту кіберпростору, а це розгалужена мережа з 700 тисяч комп'ютерів. Чисельність командування складає 200 військовослужбовців та цивільних співробітників. Умовно кажучи, за кількісною оцінкою, на кожного фахівця цього управління приходиться 3,5 тисячі комп'ютерів. Перевагами побудови кібервійськ за зразком США є те що у кожного роду військ своя складова представлена в кіберпросторі, що дає можливості командувачам відповідних родів військ скоротити ланцюг в системі управління із забезпечення дій своїх сил (військ). Недоліком є розпорошеність сил кібервійськ і необхідність створення ще одного органу військового управління у вигляді "кіберкомандування" для управління наявними у всіх збройних силах кібервійськ, що призводить до додаткових фінансових витрат.

Федеративна республіка Німеччини. На відміну від Збройні Сили Сполучених Штатів Америки Збройні Сили Німеччини мають суттєво менші інтереси за географічним та геополітичним аспектами, складаються приблизно з 179 тис. осіб, резерву – 145 осіб на 2009 рік та включають сухопутні війська, -повітряні сили і військово-морські сили, об'єднаних сил забезпечення та медико-санітарної служби. Структуру Командування кібер- та інформаційного простору Збройних Сил Німеччини можна навести на рис. 2. В активній компоненті передбачено підрозділ, який відповідає за активну протидію атакам хакерів-одинаків та хакерських угруповань. Це найменший в кібервійськах підрозділ, лише 60 військовослужбовців. Для проведення кібероперацій з протидії кібератакам (атакам у відповідь) потрібно заручитися мандатом бундестагу. Але це розглядається, як крайній засіб, який обов'язково пов'язаний з наданням обґрунтованих доведень причин та наслідків, і як правило після застосування дипломатичних методів.

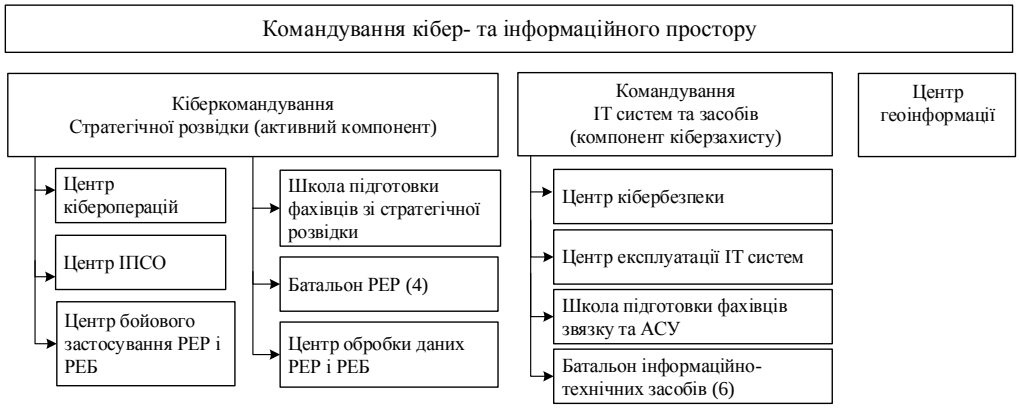

Рис. 2. Структура Командування кібер- та інформаційного простору Бундесверу

Міністром оборони Німеччини було визначено стратегію розвитку на найближчі чотири роки, в якої визначено потребу у створенні кібервійськ чисельністю 1800 чоловік (це тільки фахівців з кібербезпеки) [10]. Мотивування фахівців з кіберзахисту в Бундесвері закріплено концептуально, з застосуванням некласичних методів, таких як вільний робочий графік, окреме житло, віддалена робота, пільгове отримання офіцерських звань та інші додаткові способи мотивації.

В рамках підготовки кадрів для кібервійськ було вирішено ввести нову навчальну спеціальність в університеті бундесверу в Мюнхені. Крім того, міністерство оборони виділило в цілому близько 27,5 млн євро на нову структуру - Центр кіберінновацій (Cyber Innovation Hub), який повинен шукати перспективні стартапи та експертів в сфері інформаційних технологій, чиї ідеї та дослідження можуть бути застосовані військовими [11]. Перевагами побудови кібервійськ за зразком ФРН є зосередження кібервійськ під єдиним командуванням, що полегшує управління ними та частково скорочує витрати на управлінський апарат (відносно побудови за типом США). Недоліком є збільшення циклу управління при забезпеченні дій в інтересах родів військ збройних сил.

Об'єднане Королівство. Плануванням і координацією кібероперацій у Великобританії займається Міжвидова кібергрупа (Joint Forces Cyber Group), створена у 2013 році відповідно до завдань «Стратегії кібербезпеки Сполученого Королівства». Цій групі підпорядковані об'єднані кіберпідрозділи, розташовані в Центрі урядового зв'язку Великобританії, Міністерстві оборони, а також кіберрезервісти й інформаційна служба. Як відомо, Центр урядового зв'язку виконує схожі з Агентством національної безпеки США функції ведення радіоелектронної і мережної розвідки, криптографічного захисту інформації та криптоаналітичної роботи. У 2016 році у Великобританії для посилення кібербезпеки було створено Національний центр кібербезпеки, як один з підрозділів Міжвидової кібергруппи. Враховуючи, що ці підрозділи входять до Центру урядового зв'язку Великобританії, очевидно, що його ресурси використовуються для нарощування потенціалу не тільки військових структур [12].

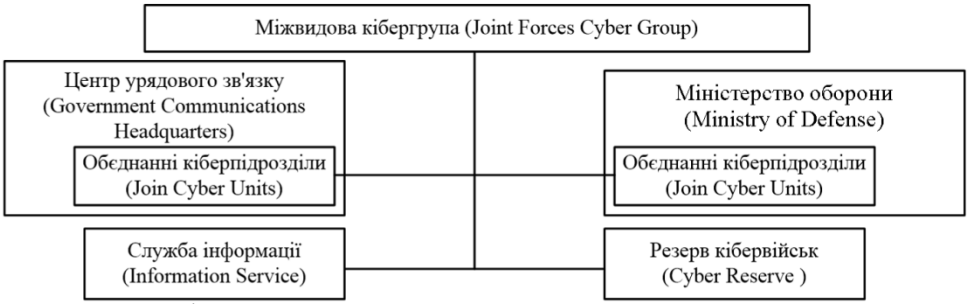

Рис. 3. Структура "Кіберкомандування" Великобританії

Перевагами побудови кібервійськ за зразком Об'єднаного королівства є гнучкість структури, виділення сил під конкретні задачі. Недоліком є підпорядкованість сил призначених для дій в кіберпросторі не тільки міністерству оборони але і розвідувальним структурам, що може призвести до розпорошення сил.

Франція. Відповідно до національної кіберстратегії "Оборона та безпека інформаційних систем: стратегія Франції" 2011 року уряд поставив завдання: забезпечення світового лідерства в питаннях кібероборони, охорона апарату прийняття рішень у Франції шляхом захисту суверенної інформації, підвищення рівня кіберзахищеності об'єктів критичної інфраструктури, забезпечення безпеки в кіберпросторі [13]. У стратегії 2015 року Франція ставить новий стратегічний пріоритет – створення "цифрової республіки" та встановлює п'ять завдань:

1) захист основоположних інтересів Франції в кіберпросторі: державні інформаційні системи і критично важливі елементи інфраструктури;

2) забезпечення взаємної довіри, конфіденційності, захисту персональних даних шляхом розробки продуктів кіберзахисту, надання юридичної та технічної допомоги;

3) підвищення досвідченості та зріст потенціалу системи кібербезпеки в національному масштабі;

4) розвиток доброзичливої атмосфери для розвитку бізнесу, інвестицій в IT-технології та інновації;

5) розробка плану подальших дій для досягнення європейської стратегічної цифрової автономії.

Слідуючи викладеній стратегії у Білій книзі 2013 року, в грудні 2016 року було створено кіберкомандування, яке призначено, як для оборонних дій, так і для активних контрдій (контратак), з використанням наступального потенціалу кіберкомандування. Сьогодні урядом передбачено до кінця 2019 року укомплектувати кіберкомандування 2600 фахівцями в області кібербезпеки. При цьому фінансові витрати на нову структуру складатимуть більш 400 млн. євро на рік. На відміну від широкомасштабного підходу США, Великобританії і Німеччини, а саме комбінування кібероперацій з радіоелектронної розвідкою, радіоелектронною протидією, у Франції було створено компактну вузькоспеціалізовану структуру кібервійськ вищого стратегічного рівня [14].

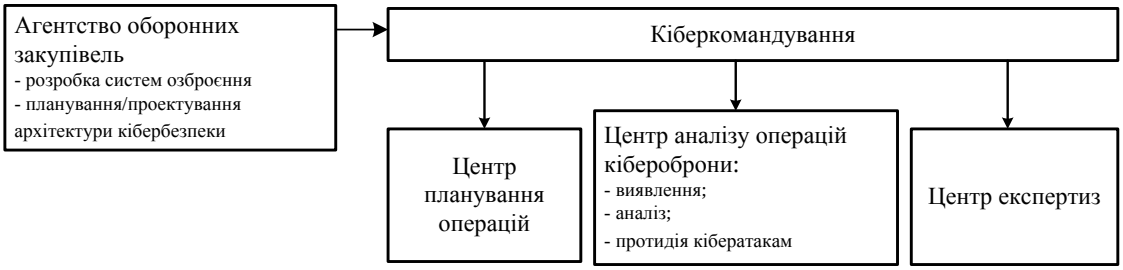

Рис. 4. Структура Кіберкомандування Франції

Переваги підходу кібервійськ Франції полягають у зменшеному розмірі сил, а значить і зменшенні фінансових витрат. Недоліком виступає таж сама мінімізація сил, що обмежує кількість виконуємих задач.

Російська Федерація. Війська інформаційних операцій – формування збройних сил Російської Федерації, що знаходиться в підпорядкуванні Міністерства оборони Російської Федерації (Міноборони Росії) (рис. 3).

Рис 5. Структура військ інформаційних операцій ЗС РФ.

За оцінками аналітиків Zecurion Analytics, за рівнем розвитку кібервійськ, з щорічними витратами на кібервійська в розмірі 300 млн. доларів і чисельністю військ близько 1 тис. осіб., Росія може входити в топ-5 держав світу після США, Китаю, Великобританії та Південної Кореї [15].

Основними завданнями військ інформаційних операції РФ є: централізоване проведення операцій кібервійни, управління і захист військових комп'ютерних мереж Росії, захист російських військових систем управління і зв'язку від кібертероризму та надійне закриття інформації, що в них проходить, від ймовірного противника. Керування інформаційними операціями покладено на Управління з міжрегіональних і культурних зв'язків із зарубіжними країнами, яке знаходиться в складі Адміністрації президента Російської Федерації. Основними функціями управління є збір і аналіз інформації, що

цікавить про зарубіжні країни в соціально-економічній і політичній сферах, проведення інформаційних заходів з питань зовнішньої політики за кордоном, організація зовнішньої взаємодії із зарубіжними політичними і громадськими діячами, міжнародними та іноземними організаціями, засобами масової інформації. Система інформаційної безпеки РФ має координуючий орган при Раді безпеки – Міжвідомчу комісію Ради безпеки РФ з інформаційної безпеки, що створює вагомий потенціал для організації, проведення і забезпечення інформаційних операцій. За відсутністю достатньої інформації щодо структури та функцій кібервійськ РФ переваги та недоліки структури кібервійськ визначити важко.

Україна. В Україні питання створення та розвитку кібервійськ відбуваються досить повільно. Це пов'язано з використанням застарілих підходів до побудови та управління складними системами, недофінансуванням та низькою мотивацією фахівців в сфері кіберзахисту, уповільнення проникнення новітніх ІТ-технологій в державні структури та системи управління, застаріла система комплектування кадрів в системі управління, інформаційних системах державного сектору, особливо в секторі оборони, яка не враховує сучасної динаміки зростання потреб фахівців в сфері ІТ-технологій, змін вимог інформаційного середовища та систем управління критичною інфраструктурою. Реалізація кіберзахисту в ЗСУ має частковий характер. В зв'язку з чим, враховуючі досвід провідних країн та існуючих керівних документів, до основних функції системи кібербезпеки (СКБ) необхідно віднести:

- управління СКБ ІТС ЗСУ;
- адміністрування СКБ ІТС ЗСУ;
- організаційне, нормативно-правове та технічне забезпечення СКБ ІТС ЗСУ;
- забезпечення захисту інформації від витоку через технічні канали витоку інформації в ІТС ЗСУ;
- забезпечення криптографічного захисту інформації в ІТС ЗСУ;
- забезпечення своєчасного реагування СКБ на кіберзагрози ІТС ЗСУ;
- забезпечення відтворення сталого функціонування ІТС ЗСУ після кібервпливів;
- забезпечення завчасної підготовки та навчання військ кіберзахисту.

Відповідно до програми щодо Постійного структурного співробітництва з питань безпеки і оборони PESCO було визначено два стратегічних напрямки, а саме створення загальної мережної платформи для обміну інформацією щодо кіберзагроз між державами та створення єдиної розгалуженої системи центрів реагування та протидії загрозам в кіберпросторі – системи колективного реагування на кіберінциденти. Приєднання до цих проектів означає необхідність створення відповідної системи кібербезпеки в державі з урахуванням вимог Європейської комісії стосовно кібезахисту об'єктів критичної інфраструктури та доведення її можливостей виконувати всі завдання з кіберзахисту на відповідному рівні. В зв'язку з чим, виникає питання щодо потенційних можливостей країни стосовно досягнення та підтримки необхідного рівня забезпечення та спроможностей в сфері кіберзахисту. Для порівняння потенційних можливостей в сфері захисту власної критичної інфраструктури від кіберзагроз було розглянуто рівні фінансування та чисельні характеристики деяких розвинутих країн. Так, наприклад в США з розміром ВВП в 2018 20 494 млрд $ доля на кібервійська склала 7 млрд. $ на рік (чисельність кібервійськ 9000), а у Франції з розміром ВВП 2 963 млрд $ доля на кібервійська склала 220 млн. $ на рік (чисельність кібервійськ 4400), у Німеччині з розміром ВВП 4 356 млрд $ доля на кібервійська склала 250 млн. $ на рік (чисельність кібервійськ 12000), у Ізраїля з розміром ВВП 337 доля на кібервійська склала 150 млн. $ на рік. За обсягом ВВП Україна ближче знаходиться за всіх до Ізраїля, тобто і доля ВВП на кібербезпеку в ЗСУ повинна наближатись до 150. Слід зауважити, що дійсна чисельність кібервійськ, до яких входять підрозділи різного призначення, державами не розголошується, тому наведені значення можуть відрізнятись від реальних.

Висновки. Таким чином, з проведеного аналізу кіберкомандувань розвинутих країн світу, їх потенційних можливостей, фінансування та чисельності кібервійськ було визначено,

що найбільш потужними країнами в сфері кіберзахисту є Китай та Сполучені Штати. Тому для створення паритету в кіберпрсторі одним зі шляхів є створення колективних систем кібербезпеки, наприклад, таких як Європейська, до якої входить 25 країн.

Створення сучасних колективних систем кібербезпеки також реалізується шляхом розміщення на території різних країн центрів реагування на кіберзагрози та сповіщення щодо кіберінцидентів. В зв'язку з цим, в провідних країнах були створені кіберкомандування та постійно продовжується нарощування кіберпотужностей військ (сил). В ході аналізу було запропоновано варіант функціонального складу кіберкомандування ЗСУ, в якому виділено основні функції покладені на сили кіберзахисту ЗС України. В ході подальших досліджень планується розробити структуру та завдання кіберкомандування ЗС України, що відповідає сучасним викликам, які стоять перед системою кібербезпеки ЗС України.

ЛІТЕРАТУРА

1. Закон України Про основні засади забезпечення кібербезпеки України від 08.07.2018 (Із змінами, внесеними згідно із Законом № 2469-VIII від 21.06.2018, ВВР, 2018, № 31, ст. 241.).

2. Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection [COM(2006) 786 final – Official Journal p. 126 of 7.6.2007].

3. Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури», введеного в дію Указом Президента України від 16 січня 2017 року № 8.

4. Рішення Ради національної безпеки і оборони України від 16 лютого 2017 року «Про невідкладні заходи з нейтралізації загроз енергетичній безпеці України та посилення захисту критичної інфраструктури», Введене в дію Указом Президента України від 16 лютого 2017 року № 37/2017.

5. «Загрози критичній інфраструктурі та їх вплив на стан національної безпеки (моніторинг реалізації Стратегії національної безпеки)». Аналітична записка Національного інституту стратегічних досліджень. Березень 2017 р.

6. World Politics, Security and International Law in Cyber Space. Australian Centre for Cyber Security. UNSW, Canberra. http://www.unsw.adfa.edu.au.

7. Heinbockel W.J. Supply Chain Attacks and Resiliency Mitigations. Guidance for System Security Engineers / Heinbockel W.J., Laderman E.R., Serrao G.J. // Mitre technical report – October 2017 http://www.mitre.org/sites/default/files/publications/pr-18-0854-supply-chain-cyber-resiliency-mitigations.pdf.

10. Веб-ресурс: http://pircenter.org/media/content/files/11/13645785400.pdf.

11. Achieve and Maintain Cyberspace Superiority. Command Vision for US Cyber Command.
https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver= 2018-06-14-152556-010.

12. Веб-ресурс: https://www.dw.com/ru/хакеры-на-службе-государства-германия-создает-киберармию/a-38312718.

13. Веб-ресурс: https://www.dw.com/ru/как-бундесвер-готовит-специалистов-по-кибербезопасности/a-43207097.

14. Веб-ресурс: https://www.gov.uk/government/organisations/joint-forces-command/about/recruitment.

15. Веб-ресурс: https://novostipmr.com/ru/news/16-12-13/vo-francii-v-2017-godu-poyavyatsya-kibervoyska.

16. Веб-ресурс: https://rns.online/articles/Frantsiya-mobilizuet-kibervoiska-2016-12-14/

17. Веб-ресурс: https://sprotyv.info/analitica/hakerom-ty-mozhesh-i-ne-byt-no-kibervoinom-objazan?highlight= Zecurion%20Analytics.