significantly from those used by developers. They are aimed at identifying the mismatch between the software requirement and the actual work by decomposing the product into levels and tasks.
In the case of the automotive industry, the test team practically performs supervision to ensure that the development complies with the guidelines. In this case, monitoring refers to a broad-spectrum analysis of the product at levels beginning from mathematical primitives, implemented in the form of mathematical and computer models.

4. Optimal decision on the establishment of validation and verification in order to minimize the risks of litigation costs.

From experience in projects related to vehicle control systems, we can make recommendations regarding testing [1, 2]:

- The testing process must be part of the development process. It must comply with the V-model. Testing should start simultaneously with development and include all levels of implementation and integration.
- Testing should be performed by a separate team responsible for compliance with the compliance between requirement and implementation. This team must also monitor compliance with standards and guidelines
- The project should have a dedicated testing architect position, and this position should be introduced into the project from the beginning.
- Automotive projects should be conducted based on AGILE, SAFe methodology to achieve the highest transparency between the teams.

REFERENCES:

1. Humennyi, Dmytro. "MATLAB SIMULINK MODEL TESTING BASED ON ISO 26262-6."
2. Humennyi, Dmytro. “On the one issue with cumulative coverage of the Simulink-based MIL unit testing for application layer of automotive field”
3. VDA QMC Working Group “Automotive SPICE Process Assessment / Reference Model”

ОЛЕКСАНДР ЧЕРНОНОГ[1]
ІГОР КОЗУБЦОВ, *доктор педагогічних наук*[2]

[1]*Міністерство оборони України, Державний експерт експертної групи кібербезпеки Директорату політики цифрової трансформації та інформаційної безпеки у сфері оборони, skgzua@gmail.com.*
[2]*Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, провідний науковий співробітник науково-дослідного відділу, kozubtsov@gmail.com.*

КІБЕРДОРОЗВІДКА В УМОВАХ ГІБРИДНОЇ ВІЙНИ: АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСАДИ

CYBER EXPLORATION IN CONDITIONS OF HYBRID WAR: ADMINISTRATIVE AND LEGAL FRAMEWORK

ABSTRACT

In the first days of the full-scale military aggression of the Russian Federation against Ukraine, personnel management in the Armed Forces of Ukraine was unsatisfactory and purposeful. Therefore, such a system in the Armed Forces of Ukraine needs to be reformed. The purpose of the new personnel management system should be "a model of future results as some initial image that should be sought to achieve results."

KEY WORDS: personnel management, the Armed Forces of Ukraine, professionalism, efficiency.

АНОТАЦІЯ

В перші часи повномасштабної військової агресії Російської Федерації проти України кадровий менеджмент в Збройних Силах України проявився у незадовільному цілеспрямованому характері. Тому, таку систему у Збройних Сил України необхідно переформовувати. Тому нова система кадрового менеджменту повинна мати вигляд «моделі майбутнього результату як деякий вихідний образ, до якого слід прагнути, щоб досягти результату».

КЛЮЧОВІ СЛОВА: кібердорозвідка, умови, гібридна війна, адміністративно-правові засади, Збройні Сили України.

Постановка завдання. З початку повномасштабної військової агресії Російської Федерації проти України одночасно з вогневим ураженням об’єктів критичної інфраструктури нанесено кібератаки на об’єкти критичної інформаційної інфраструктури (ОКІІ). Завдяки вмілим діям і своєчасній підготовці українського сегменту Інтернету до кібероборони, було досягнуто успіху в тому, що більша частина ОКІІ продовжила функціонувати в штатному режимі не зазнаючи втручання та наслідків від DDoS-атак. Зважаючи на те, що Україна не планувала і не здійснила акту вторгнення на територію Російської Федерації, вимушена була застосувати весь потенціал

кібероборони. Однак приємним для нас і не очікуваним для Російської Федерації став факт небайдужості фахівців ІТ-сфери з числа цивільного населення, які синергетично згуртувалися і створили передумови до проведення активних заходів у кіберпросторі. В зв'язку з тим, що Україна незважаючи на війну продовжує дотримуватися міжнародних норм ведення війни, в тому числі у кіберпросторі. Однак, приклад активної громадянської позиції щодо необхідності застосування активних форм дій в кіберпросторі підтверджує тезу про вирішальну роль у необхідності домінування над супротивником – Російською Федерацією та одночасно, у вирішені адміністративно-правових прогалин законодавства України.

Аналіз останніх публікацій. До вивчення спектру адміністративно-правових засад кібероброни під різними кутами зору присвячено досить багато наукових робіт. Найбільш активну позицію проявили науковці: Ю.Г. Даник, С.Г. Вдовенко, І.В. Діордіца, Є.О. Живило, В.В. Куцаєв, О.О. Черноног та ін.

Однак, з погляду зазначеної проблеми застосування активних заходів (кібердорозвідки) в кіберпросторі, потенційного ворога на даний час вивчено не достатньо, проте враховуючи отриманий досвід в ході відбиття зовнішньої агресії Російської Федерації проти України, є в такому нагальна необхідність.

Мета доповіді. Мета доповіді - висвітлити ключові адміністративно-правові засади та потребу в організації кібердорозвідки в умовах гібридної війни.

Результат дослідження.

Адміністративно-правовою основою, для організації активних та пасивних заходів в кіберпросторі, можна вважати подію із затвердженням у 2016 р. Президентом України Стратегії кібербезпеки України, в якій, зокрема, вперше в оборонну термінологію було введено поняття «кібероборона» [1].

Згодом, у підготовленому проекті Указу Президента України від 2021 «Про рішення Ради національної безпеки і оборони України», «Про Стратегічний оборонний бюлетень України» [2], запропоновано термінологію доповнити поняттям кібердорозвідка – збір інформації щодо вразливостей програмного забезпечення, телекомунікаційного обладнання, автоматизованих систем управління силами, зброєю та/або технологічними процесами визначеної цілі. Але в затвердженому Указі Президента України від 17.09.2021 №473/2021 [3] під кібердорозвідкою запропоновано розуміти діяльність щодо виявлення вразливостей програмного забезпечення, телекомунікаційного обладнання, автоматизованих систем управління силами, зброєю та/або технологічними процесами визначеної цілі (об'єкта кіберінфраструктури).

У Стратегічному оборонному бюлетені України в додатку 3. «Матриця основних спроможностей сил оборони» систематизовані Інституційні спроможності центральних органів виконавчої влади та інших державних органів, які здійснюють керівництво, спрямовують та координують діяльність військових формувань, що входять або виділяють відповідні сили і засоби до складу сил оборони, та оперативні, бойові і спеціальні спроможності сил оборони. Так згідно якого за реалізацію здатності ведення кіберрозвідки та кібердорозвідки в інформаційно-телекомунікаційних мережах та системах державного, приватного і військового призначення (об'єктів критичної інфраструктури) противника для здобуття інформації про кіберінфраструктуру противника, їх призначення, місцезнаходження, технологічних процесів, уразливості, встановлення прихованого контролю, перехоплення та дешифрування керуючих і ресурсних даних та інформації покладаються на: Головне управління розвідки Міноборони, Збройні Сили України, Державна прикордонна служба України.

Таким чином, впровадження зазначених документів визначило базис адміністративно-правових норм майбутньої кібердорозвідки як діяльності в кіберпросторі [3]. Однак з початком повномасштабної військової агресії Російської Федерації проти України Державні органи та організаційні структури, які є носіями спроможностей [3] виявились в теорії спроможними. Потужну і превентивну допомогу в реалізації кібердорозвідки, як показала практика, надали самоорганізовані не байдужі ІТ-фахівці, які в певній мірі підтвердили раціональність ранішого припущення, щодо необхідності створення гібридних підрозділів військово-цивільного співробітництва.

Відсутність централізованого управління призвело до децентралізованого створення телеграм каналів, до прикладу Кібер Армія та інші, які станом дня 25.02.2022 р. нараховували понад 250 тисяч учасників. Прогностичність дій вбачала за необхідність у пошуку та виявлення вразливостей програмного забезпечення, телекомунікаційного обладнання, автоматизованих систем управління силами, зброєю та/або технологічними процесами визначеної цілі (об'єкта кіберінфраструктури).

ЛІТЕРАТУРА:

1. Стратегія кібербезпеки України: указ Президента України від 15 березня 2016 р. №96. URL: https://zakon.rada.gov.ua/laws/show/96/2016/ed20160315.
2. Проект Указу Президента України від 2021 «Про рішення Ради національної безпеки і оборони України», «Про Стратегічний оборонний бюлетень України». URL: https://www.mil.gov.ua/content/pdf/up_rrnb.pdf.
3. Указ Президента України від 17.09.2021 № 473/2021 «Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року», «Про Стратегічний оборонний бюлетень України». URL: https://zakon.rada.gov.ua/laws/show/473/2021.