4. Z. Li, J. Yang, Z. Liu, X. Yang, G. Jeon, and W. Wu, “Feedback network for image super-resolution,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2019. P. 3867–3876.

5. Z. Liu, L. Wang, C. Li, W. Siu, and Y. Chan, “Image super-resolution via attention based back projection networks,” in Proceedings of the IEEE International Conference on Computer Vision Workshop, 2019.

6. Бедратюк Г.І. Аналіз якості методів повороту зображення за допомогою моментних інваріантів. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2020. № 2. С. 56-6.

DOI https://doi.org/10.30525/978-9934-26-109-1-2

РОЗВИТОК КІБЕРЗАХИСТУ – ОДНА ІЗ СКЛАДОВИХ БЕЗПЕКИ УКРАЇНИ

Лаврут О. О.
доктор технічних наук, доцент,
професор кафедри тактики
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

Лаврут Т. В.
кандидат географічних наук, доцент,
старший науковий співробітник науково-дослідного відділу
(систем управління військами)
Наукового центру Сухопутних військ
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного

Колесник В. О.
старший науковий співробітник
Національна академія сухопутних військ
імені гетьмана Петра Сагайдачного
м. Львів, Україна

Ми живемо в епоху глобалізації, коли інформаційні технології та телекомунікаційні системи охоплюють усі сфери життєдіяльності людини, держави. Зростають обсяги інформації, що циркулює,

змінюються технічні засоби, зростають і ризики інформаційної безпеки в забезпеченні живучості інформаційно-телекомунікаційних систем як в цивільній сфері, так і в силових структурах [5, с. 91-101; 6, с. 42-49; 7, с. 128-134]. Питання кібербезпеки завжди було актуальним у світі. За ефективністю та наслідками застосування кіберзброю можна прирівняти до зброї масового ураження.

Від початку протистояння з Росією, кіберпростір став ще одним майданчиком, на якому розгортаються воєнні дії. Як показує досвід, особливого кібервпливу дійсно зазнають населення та інфраструктура будь-якої держави. Сьогодні кожна людина є суб'єктом кіберпростору. Ноутбук, планшет, мобільний телефон – потенційно уразливі гаджети. Найпростіша загроза, з якою може стикнутися будь-яка людина в світі, розсилання посилань та фішинглвих листів із незрозумілими пропозиціями. Такі листи можуть завантажувати шкідливе програмне забезпечення, блокувати телефон чи комп'ютер з метою проникнення в систему, у якій працює людина, вимагання грошей, використання їх особистих даних тощо. Саме тому починаючи з 2020 року в Україні розпочалася реформа сфери кіберзахисту [4].

Національна система кібербезпеки України є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури [3].

Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України [3].

Наша держава вимушена швидко реагувати на виникнення нових загроз та вести пошук ефективних заходів кіберзахисту. Так в Україні вже створений Державний центр кіберзахисту (Кіберцентру UA30) – установа, яка безпосередньо займається захистом державних інформаційних ресурсів. Він надає послуги не тільки державним органам, але громадянам і бізнесу. В травні цього року за участі Президента України відбулося його офіційне відкриття.

Кіберцентр UA30 матиме чотири пріоритети: захист державних реєстрів; захист громадян, приватної інформації та бізнесу; розвиток

культури кібергігієни; формування кадрового резерву кібербезпеки. Основна задача центру – робота над тим, щоб переважна більшість держреєстрів були під його захистом до 2024 року.

Державним центром кіберзахисту вживаються заходи з протидії кібератакам. Також власникам інформаційних систем, керівникам підрозділів, які відповідають за інформаційну безпеку державних органів України постійно надаються рекомендації щодо протидії кібератакам, а також проводить робота щодо попередження зараження інфраструктури шкідливим програмним забезпеченням.

Вирішити питання кіберзахисту в державі можна лише завдяки комплексному підходу. Так, заступник Голови Держспецзв'язку Олександр Потій під час виступу на науково-практичній конференції «Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання» презентував Організаційно-технічну модель кіберзахисту [1]. Він пояснив, що якщо розглядати кіберзахист як цілеспрямовану діяльність із забезпечення безпеки кіберпростору, то необхідно визначити структуру такої діяльності, суб'єкти кіберзахисту, цілі кіберзахисту та відповідну інфраструктуру, яка цю діяльність буде підтримувати [1]. Організаційно-технічна модель кіберзахисту складатиметься з трьох вертикально та горизонтально інтегрованих інфраструктур (рис. 1).

Механізми імплементації цієї моделі та її ресурсне забезпечення – є найважливішими компонентами, які охоплюють всі рівні архітектури. Розробка і удосконалення нормативної бази шляхом прийняття відповідних законодавчих актів, нормативних актів, стандартів, наказів на всіх рівнях дозволить в подальшому імплементувати цю модель.

Сьогодні в Україні питаннями кіберзахисту опікуються також у Міністерстві оборони України, Службі безпеки України, де створені відповідні підрозділи. Розпочато процес приєднання України до Об'єднаного центру передових технологій з кібероборони НАТО, який забезпечує боротьбу з кібератаками та кіберзахист інформаційних систем [8].

В рамках розвитку даного напрямку Ситуаційний центр забезпечення кібербезпеки Служби безпеки України ввів в дію національну платформу Malware Information Sharing Platform «Ukrainian Advantage» (MISP-UA) для ефективної протидії кіберзагрозам і обміну даними щодо ризиків [2].

Використання системи дає можливість кіберфахівцям Служби передбачати шляхи атак, потенційні загрози та інструменти нейтралізації для подальшого реагування. За своїм функціональним

наповненням платформа дозволяє зміцнити стан кібербезпеки різних секторів державного управління та економіки України. З її допомогою відбувається державно-приватна взаємодія для спільного захисту інформаційного та кіберпростору держави загалом.

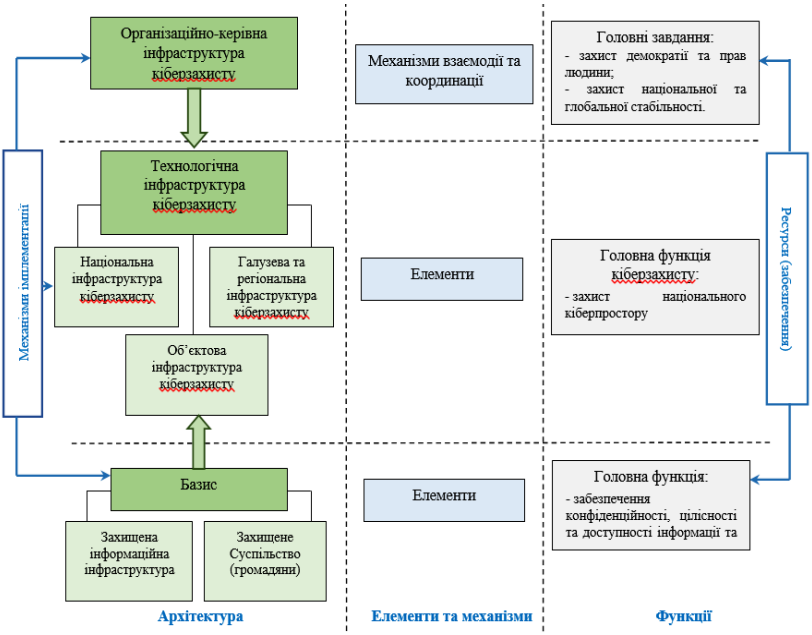

Рис. 1. Організаційно-технічна модель кіберзахисту

Україна зараз на передовій боротьби з викликами в кіберпросторі. Однак, покладатися лише на те, що всі питання кіберзахисту вирішить держава не варто. Кожна людина, кожен громадянин має знати, як убезпечити та захистити себе, свої конфіденційні дані, банківські рахунки тощо.

Таким чином, питання кіберзахисту є актуальним. Його вирішення повинно відбуватись комплексно як на рівні звичайних користувачів, так і на державному рівні в рамках створення сучасної законодавчої бази, відповідних програмних і технічних рішень. Збільшення інвестування в кібербезпеку дасть можливість запобігти атакам на великі державні і приватні компанії та протистояти намірам дестабілізувати суспільство.

Література:

1. В Україні презентовано Організаційно-технічну модель кіберзахисту. URL: https://softline.org.ua/news/v-ukraini-prezentovano-orhanizatsiino-tekhnichnu-model-kiberzakhystu.html (дата звернення 27.06.2021).

2. Для протидії кіберзагрозам СБУ вводить в дію оновлену версію платформи MISP-UA. URL: https:// ssu.gov.ua/novyny/7800 (дата звернення 29.06.2021).

3. Закон України «Про основні засади забезпечення кібербезпеки України». *Відомості Верховної Ради (ВВР*. 2017, № 45, ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 27.06.2021).

4. Кібероборона України: стан, проблеми та актуальні заходи щодо її забезпечення. URL: http://opk.com.ua/кібероборона-україни-стан-проблеми-т/ (дата звернення 29.06.2021).

5. Лаврут О.О. Новітні технології та засоби зв'язку у Збройних Силах України: шлях трансформації та перспективи розвитку / О.О. Лаврут, Т.В. Лаврут, О.К. Климович, Ю.М. Здоренко. *Наука і техніка Повітряних Сил Збройних Сил України*. 2019. Вип. 1 (34). С. 91–101. DOI: 10.30748/nips.2019.34.13.

6. Лаврут О.О., Климович К.О., Тарасюк М.Л., Антонюк О.Л. Стан та перспективи застосування сучасних технологій та засобів радіозв'язку в Збройних Силах України. *Системи озброєння і військова техніка*. 2017. Вип. 1(49). С. 42-49.

7. Пузиренко О.Г., Івко С.О., Лаврут О.О. Аналіз процесу управління ризиками інформаційної безпеки в забезпеченні живучості інформаційно-телекомунікаційних систем. *Системи обробки інформації*. 2014. Вип. 8 (124). С. 128-134.

8. Розпочався процес включення України до Центру кіберзахисту НАТО. URL: https://www.pravda.com.ua/news/2021/06/7/7296338/ (дата звернення 27.06.2021).