УДК 004.056.53 **doi: 10.26906/SUNZ.2022.3.116**

В. Д. Голь, А. Ю. Раківська, Д. Ю. Раківський

Інститут спеціального зв’язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна

ЗАСОБИ КІБЕРЗАХИСТУ НА РІВНІ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ

Анотація. У статті проаналізовано та запропоновано концептуальні засади впровадження організаційно-технічної моделі кіберзахисту, призначення та цілі. Розглянуто архітектуру організаційно-технічної моделі кіберзахисту, яка є структурованою системою, що складається з трьох інфраструктур кіберзахисту, а саме: організаційно-керуючої інфраструктури кіберзахисту, як сукупності суб’єктів забезпечення кібербезпеки, що формують та реалізують державну політику у сфері кібербезпеки; технологічної інфраструктури кіберзахисту, як сукупності сил та засобів кіберзахисту, а також інфраструктури, що забезпечує функціонування сил кіберзахисту, інформаційно-комунікаційних мереж та їх ресурсів, що використовуються в інтересах сил кіберзахисту та базисної інфраструктури кіберзахисту, як сукупності об’єктів критичної інформаційної інфраструктури, критичних активів, комунікаційних і технологічних систем, що віднесені до об’єктів критичної інфраструктури. Запропоновано виділити місце в організаційно-технічній моделі, яке буде об’єднувати в собі роботу та реалізацію засобів кіберзахисту на рівні мережної інфраструктури.

Ключові слова: кіберзагроза, система інформаційної безпеки, комплексна система захисту інформації, комплекс засобів захисту, об’єкти критичної інфраструктури.

Вступ

Постановка проблеми. Питання безпеки інформаційних систем державних органів влади наразі є одними з найбільш актуальних. Наразі потреба безпеки даних потребує конкретних рішень та заходів, адже окремі державні органи експлуатують інформаційно-телекомунікаційні системи всупереч вимогам законодавства. Саме впровадження в дію рівнів та використання властивостей організаційно-технічної моделі (ОТМ) забезпечить на організаційному, технологічному і базисному рівнях взаємодію між суб’єктами національної системи кібербезпеки, відповідними технічними підрозділами цих суб’єктів, які спираються на відповідну захищену інформаційну інфраструктуру.

Аналіз останніх досліджень і публікацій. Організаційно-технічні побудови систем кібербезпеки різних країн розглядались в національних стратегіях кібербезпеки, рекомендаціях ENISA, ITU, NATO. Робіт і досліджень доволі багато [1-14], але на даний час в Україні недостатньо досліджень саме з питань розбудови ОТМ кіберзахисту (ОТМК) та з розвитку національної системи кібербезпеки в цілому. Отже головною задачею в сфері комунікаційних мереж і спеціального зв’язку стає розробка концептуальних засад формування та впровадження ОТМ кіберзахисту України.

Метою статті є проведення аналізу та дослідження принципу роботи і використання організаційно-технічної моделі кіберзахисту, ґрунтуючись на застосуванні засобів мережного захисту.

1. Структура організаційно-технічної моделі кіберзахисту

Кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем (Закон України «Про основні засади забезпечення кібербезпеки України» від 5.10.2017 № 2163-VIII).

Вищезазначений Закон України визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки.

Відповідно до [4-6] одним з шляхів забезпечення функціонування національної системи кібербезпеки є впровадження організаційно-технічної моделі (ОТМ) національної системи кібербезпеки як комплексу заходів, сил і засобів кіберзахисту, спрямованих на оперативне реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мініммізацію вразливості комунікаційних систем. Місія ОТМК – через розвиток зрілості (maturity) національної системи кібербезпеки забезпечити її стійкість (resilience) задля безпечного та сталого функціонування українських об’єктів критичної інфраструктури, систем надання електронних послуг, інформаційної інфраструктури, нейтралізації кібератак. Завдана шкода від атак щоразу зростає в геометричній прогресії, що змушує компанії вживати нових заходів кіберзахисту. Саме тому заступник Голови Держспецзв’язку Олександр Потій 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 [4]. На основі посилення рівня захисту кібернетичної системи була презентована «Організаційно-технічна модель кіберзахисту» ([4], яка складатиметься з трьох вертикально та горизонтально інтегрованих інфраструктур (рис. 1).

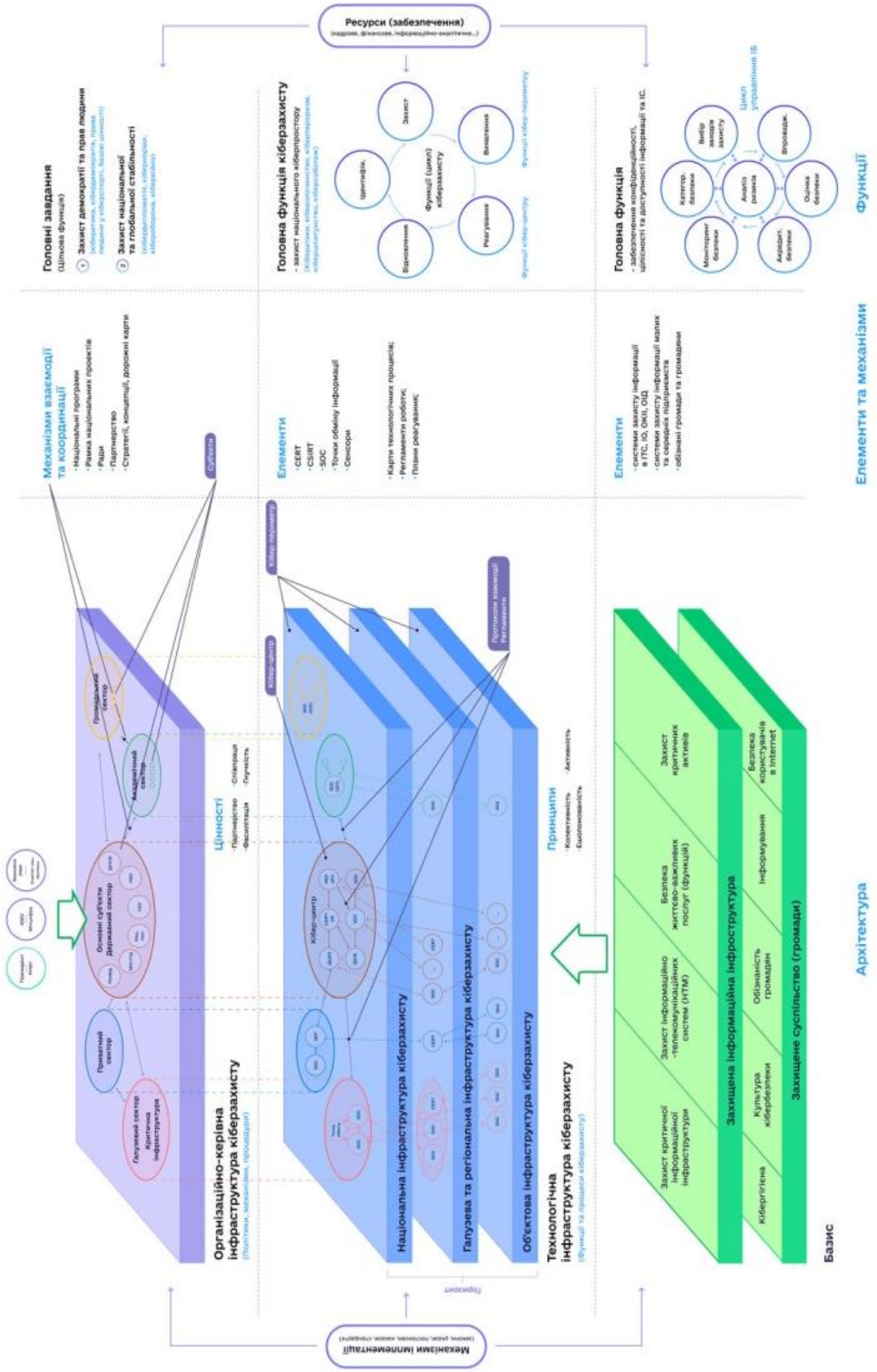

Рис. 1. Організаційно-технічна модель кіберзахисту (джерело [4])

Технологіями та засобами кіберзахисту, які використовуються для реалізації ОТМК, є системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, інформаційні технології, технічні, програмні та програмно-апаратні засоби (пристрої, обладнання, комплекси), які використовуються в інтересах забезпечення кіберзахисту державних інформаційних ресурсів, комунікаційних та технологічних систем, а також об'єктів критичної інформаційної інфраструктури [4]. Сфера впровадження заходів на цьому рівні притаманна спеціалістам з телекомунікаційних систем. Головним завданням технологічної інфраструктури є оперативний та ефективний захист кіберпростору в частині протидії кібератакам, кіберзлочинам, кібертероризму, кібершпигунству, а також забезпечення кібероборони та кіберрозвідки, в т.ч. через {5]:

– збір, аналіз, оцінювання, узагальнення та поширення інформації про інциденти;

– допомогу іншим суб'єктам кіберзахисту у випадку кіберінцидентів;

– взаємне інформування суб'єктів кіберзахисту про нові загрози;

– створення умов для відповідального та довіреного обміну інформацією між суб'єктами кіберзахисту всіх секторів кіберзахисту. Реалізація цього завдання ґрунтується на впровадженні на всіх рівнях циклу функцій кіберзахисту який включає:

– ідентифікацію – визначення користувачів та ресурсів, оцінки ризиків, оцінки вразливостей, каталогізації національних електронних інформаційні ресурсів та визначення об'єктів (активів), що підлягають кіберзахисту:

– захист – контроль доступу, захисту даних (конфіденційність, цілісність, доступність), опис процесів та процедур, захисту від атак, технічної підтримки, тренування персоналу;

– виявлення – збір подій та виявлення аномалій, моніторинг інцидентів безпеки, побудова процесу детектування та обміну інформацією;

– реагування – аналіз інцидентів безпеки, оцінки їх наслідків, протидії та блокуванню засобами захисту, покращення системи захисту;

– відновлення – відновлення після кібератаки, забезпечення проведення відповідного їх розслідування, розробки та забезпечення реалізації заходів щодо вдосконалення системи кіберзахисту та підвищення рівня кібербезпеки. [6]

В роботі ОТМК застосовуються різні рівні моделі OSI, прикладний, фізичний, мережний. В обслуговуванні задіяні фахівці з галузі телекомунікацій, які керують процесами відповідно до кожного рівня базової структури.

Перший рівень – це організаційно-керуюча інфраструктура кіберзахисту. Другий рівень – це технологічний рівень або технологічна інфраструктура кіберзахисту, яка складається з сукупності сил та засобів кіберзахисту. Третій рівень – це базисна інфраструктура кіберзахисту, що забезпечує основні спроможності кіберзахисту.

Механізми імплементації цієї моделі і ресурсне забезпечення – це два дуже важливі компоненти, які охоплюють всі рівні архітектури. Механізм імплементації – це відповідні розробка і удосконалення нормативної бази шляхом прийняття відповідних законодавчих актів, нормативних актів, стандартів, наказів на всіх рівнях – з верхнього до нижнього рівнів управління» [14] Для реалізації моделі спеціалістами з телекомунікаційних мереж було запропоновано виділити місце в ОТМК, яке буде об'єднувати в собі роботу та реалізацію засобів кіберзахисту на рівні мережної інфраструктури.

2. Засоби захисту мережної інфраструктури

Розглянемо більш детально засоби захисту мережної інфраструктури, що пропонуються для ОТМК на рівні мережної інфраструктури.

Cisco FirePOWER – це програмні послуги для платформи Cisco ASA. Особливості: негайне виявлення вірусів із зовнішніх мереж, виявлення спроб сканування ресурсів та структури внутрішньої мережі, повний контроль над гостьовими сервісами та підключеннями, визначення надійних політик захисту до та під час атак. Є потужним рішенням з управління мережними активами та їх вразливістю.

BlackBerry Cyber Suite пропонує забезпечення захисту в середовищі «з нульовою довірою» (Zero Trust), де кожна кінцева точка має забезпечити довіру та підтвердити її під час кожного події чи транзакції. Особливості: реалізація архетипних архітекторів Zero Trust для просування алгоритмів, працює на кінцевих точках усіх типів, використовуючи повне охоплення та краще розуміння поведінки дов, забезпечує безперервний моніторинг та виявлення загроз, щоб забезпечити цілісність даних, забезпечує постійну контекстно-залежну автентифікацію пристроїв, мереж, програм та людей, створює відкриту платформу, що дозволяє безпроблемну інтеграцію з іншими рішеннями.

Cisco ASA CX використовує можливості мережної архітектури безпеки Cisco SecureX Framework, що враховує контекст мереж корпоративних підрозділів і центрів обробки даних, а також у хмарних мережних сегментах. Особливості: це рішення дає адміністраторам можливість встановлювати пристрої і додатки з високим рівнем захисту і керованості. Адміністратори отримують чіткі дані про тип пристрою, встановленої на ньому операційній системі, місцезнаходження пристрою і поточний рівень безпеки.

Відключення невживаних портів – це простий спосіб захисту мережі від несанкціонованого доступу. Наприклад, якщо комутатор Catalyst 2960 має 24 порти і при цьому використовуються три підключення Fast Ethernet, рекомендується відключити 21 невживаний порт. Процес включення і виключення портів може зайняти багато часу, але він підвищує безпеку мережі.

Функція безпеки порту. Перед введенням комутатора в експлуатацію необхідно забезпечити безпеку усіх портів (інтерфейсів) комутатора. Один із способів захисту портів – використання функції безпеки портів (функція Port Security). Ця функція

обмежує кількість допустимих MAC-адрес на один порт, а також дозволяє доступ для MAC-адрес санкціонованих пристроїв і забороняє доступ для інших MAC-адрес.

Протокол Secure Shell (SSH) надає віддалений вхід в систему аналогічно Telnet, за винятком того, що він використовує безпечніші мережні служби. SSH – це протокол, який використовує клієнт-серверну модель для аутентифікації віддалених систем та забезпечення шифрування даних, обмін якими відбувається у рамках віддаленого доступу. Використання SSH підключення має низку переваг: безпечна робота на віддаленому ПК із використанням командної оболонки; використання різних алгоритмів шифрування (симетричного, асиметричного та хешування); можливість безпечного використання будь-якого мережного протоколу, що дозволяє передавати захищеним каналом файли будь-якого розміру.

ACL (Access Control List) – це набір текстових виразів, які щось дозволяють або щось забороняють. Зазвичай ACL дозволяє або забороняє IP-пакети, але також може заглядати всередину IP-пакета, переглядати тип пакета, TCP і UDP. ACL поділяються на два типи: Standard – можуть перевіряти лише адреси джерел; Extended – можуть перевіряти адреси джерел, а також адреси одержувачів, у разі IP ще тип протоколу та TCP/UDP порти.

CDP (Cisco Discovery Protocol) – протокол другого рівня, розроблений компанією Cisco Systems, що дозволяє виявляти підключене (безпосередньо або через пристрої першого рівня) мережне обладнання cisco, його назву, версію IOS та IP-адреси. Підтримується багатьма пристроями компанії, майже підтримується сторонніми виробниками.

Отримувана інформація включає типи підключених пристроїв, інтерфейси маршрутизатора, до яких сусідні пристрої підключені, інтерфейси, що використовуються для створення з'єднань, а також моделі пристроїв.

NAT – команда, забезпечує безпеку комп'ютерів, серверів та мережних пристроїв, блокуючи безпосередній доступ до Інтернету з реальної IP-адреси вузла. NAT дозволяє заблокувати доступ до приватної мережі ззовні. NAT ховає приватні IP-адреси від загальнодоступних мереж. Контроль доступу в деяких випадках бажаний, але може виявитися і недоліком у тому випадку, якщо потрібен віддалений доступ до пристрою в приватній мережі з Інтернету.

Динамічне перетворення NAT дозволяє вузлам з приватними IP-адресами з Інтернету підключатися до загальнодоступної мережі, наприклад, мережі Інтернет. Статичне перетворення мережних адрес (NAT) дозволяє вузлам із загальнодоступної мережі підключатися до окремих вузлів із приватної мережі. Це означає, що для настроювання NAT для зовнішнього доступу слід використовувати динамічний варіант NAT. Якщо пристрій із внутрішньої мережі має бути доступний ззовні, використовується статичний варіант NAT. Великий недолік NAT – додаткове навантаження, що створює перетворення IP-адреси та порту.

Протоколи формування захищеного каналу (PPTP, L2F і L2TP). Протокол PPTP забезпечує тунелювання і шифрування переданих даних. Протоколи L2F і L2TP підтримують тільки функції тунелювання. Для захисту даних у цих протоколах необхідно використовувати певний додатковий протокол, зокрема IPSec.

PAP та CHAP – протоколи автентифікації, що використовуються у протоколі PPP. PAP – Password Authentication Protocol. CHAP розшифровується як Challenge Handshake Authentication Protocol.

Принцип роботи PAP. Клієнт хоче підключитися до сервера, він відправляє серверу пароль, сервер відповідає або «Так», або «Ні». Запитуючи чи підходить пароль, відбувається передача самого паролю, з яким зловмисник надалі може робити все, що завгодно. Такі ситуації дозволяє уникнути протокол CHAP.

Принцип роботи CHAP. Клієнт хоче звернутися до сервера, сервер передає клієнту випадковий рядок, клієнт бере пароль і рядок і обчислює від нього MD5 хеш, який повертає серверу. Сервер робить ті самі операції (якщо знає правильний пароль). Якщо хеші співпадають – клієнт авторизований. Якщо клієнт не знає пароль – хеші не збігатимуться, якщо замість сервера зловмисник – буде отримано лише хеш. Таким чином, у реальних мережах краще використовувати протокол CHAP.

Стек протоколів IPSec використовується для аутентифікації учасників обміну, тунелювання трафіку і шифрування IP-пакетів. Основне призначення протоколу IPSec (Internet Protocol Security) – забезпечення безпечної передачі даних по мережах IP. Оскільки архітектура IPSec сумісна з протоколом IPv4, її підтримку досить забезпечити на обох кінцях, з'єднання; проміжні мережні вузли можуть взагалі нічого «не знати» про IPSec. Протокол IPSec може захищати трафік як поточної версії протоколу IPv4, вживаної сьогодні в Internet, так і трафік нової версії IPv6, яка поступово впроваджується в Internet. Архітектура засобів безпеки IPSec Основне призначення протоколів IPSec – забезпечення безпечної передачі даних по мережах IP. Застосування IPSec гарантує:

• цілісність передаваних даних (тобто дані при передачі не спотворені, не втрачені і не продубльовані);

• автентичність відправника (тобто дані передані саме тим відправником, який довів, що він той, за кого себе видає);

• конфіденційність передаваних даних (тобто дані передаються у формі, що запобігає їх несанкціонованому перегляду).

VPN (англ. Virtual Private Network – віртуальна приватна мережа) – узагальнена назва технологій, що дозволяють забезпечити одне або кілька мережних з'єднань (логічну мережу) поверх іншої мережі (наприклад, Інтернет). Незважаючи на те, що комунікації здійснюються по мережах з меншим або невідомим рівнем довіри (наприклад, по публічних мережах), рівень довіри до побудованої логічної

мережі не залежить від рівня довіри до базових мереж завдяки використанню засобів криптографії (шифрування, аутентифікації, інфраструктури відкритих ключів, засобів для захисту від повторів і змін переданих по логічній мережі повідомлень).

Отже всі вищенаведені технології, протоколи та програми можуть бути запропоновані для включення до організаційно-технічної моделі кібербезпеки, що наведена на рис. 1, на рівні мережної інфраструктури

Висновок

У статті проаналізовано та досліджено принцип роботи і використання організаційно-технічної моделі кіберзахисту, ґрунтуючись на застосуванні засобів мережного захисту. Запропоновано ряд засобів, які будуть функціонувати на мережному рівні в моделі ОТМК. Розглянуто принципи роботи та алгоритм налаштування засобів захисту, що застосовуються на мережному рівні моделі ОТМК.

СПИСОК ЛІТЕРАТУРИ

1. Бакалинський О. Модель та методи визначення проектних характеристик систем управління інформаційною безпекою: монографія. Київ : ТОВ «Три К», 2020. 162 с.
2. Семенченко А.І., Мялковскій Д.В. Розвиток інституційних спроможностей суб'єктів забезпечення системи кібербезпеки та кіберзахисту України. *Теорія та практика державного управління*. 2020. Вип. 3(70). С.40-54.
3. Demertzis K., Iliadis L. Cognitive Web Application Firewall to Critical Infrastructures Protection from Phishing Attacks. *Journal of Computations & Modelling*. 2019. Vol. 9, no. 2. Pp. 1-26.
4. Потій О., Семенченко А., Дубов Д., Бакалинський О., Мялковський Д. Концептуальні засади впровадження організаційно-технічної моделі кіберзахисту України. *Захист інформації*. 2021. Том 23, № 1. С. 48-53. DOI: https://doi.org/10.18372/2410-7840.23.15434
5. Деякі питання об'єктів критичної інфраструктури, Постанова Кабінету Міністрів України № 1109 від 9 жовтня 2020 р. - режим доступу: https://zakon.rada. gov.ua/laws/show/1109-2020-%D0%BF#Text
6. Деякі питання об'єктів критичної інформаційної інфраструктури, Постанова Кабінету Міністрів України № 943 від 9 жовтня 2020 р. - режим доступу: https:// zakon.rada.gov.ua/laws/show/943-2020-%D0%BF# Text
7. Klimushin, P., Solianyk, T., Kolisnyk, T., & Mozhaiv, O. (2021). Potential application of hardware protected symmetric authentication microcircuits to ensure the security of internet of things. Advanced Information Systems, 5(3), 103–111. https://doi.org/10.20998/2522-9052.2021.3.14
8. Ruban, I., Bolohova, N., Martovytskyi, V., & Yaroshevych, R. (2021). Methodology for assessing the effectiveness of methods for embedding digital watermarks. Advanced Information Systems, 5(3), 112–118. DOI: https://doi.org/10.20998/2522-9052.2021.3.15
9. Mozhaiev M., Kuchuk N., Usatenko M. The method of jitter determining in the telecommunication network of a computer system on a special software platform. *Innovative technologies and scientific solutions for industries*, 2019. Vol. 4 (10), pp. 134-140. doi: https://doi.org/10.30837/2522-9818.2019.10.134
10. Mozhaev, O., Kuchuk, H., Kuchuk, N., Mykhailo, M., Lohvynenko, M. (2017), "Multiservice network security metric", 2nd International Conference on Advanced Information and Communication Technologies, AICT 2017 – Proceedings, pp. 133-136, DOI: https://doi.org/10.1109/AIACT.2017.8020083
11. Semenov, S., Weilin, C., Zhang, L., & Bulba, S. (2021). Automated penetration testing method using deep machine learning technology. Advanced Information Systems, 5(3), 119–127. https://doi.org/10.20998/2522-9052.2021.3.16
12. Ruban, I., Bolohova, N., Martovytskyi, V., & Koptsev, O. (2021). Digital image authentication model. Advanced Information Systems, 5(1), 113–117. DOI: https://doi.org/10.20998/2522-9052.2021.1.16
13. Cherneva, G., & Khalimov, P. (2021). Mutation testing of access control policies. Advanced Information Systems, 5(1), 118–122. DOI: https://doi.org/10.20998/2522-9052.2021.1.17
14. Гончар С.Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури: монографія. Київ : Альфа реклама, 2019. 176 с.

Received (Надійшла) 19.05.2022
Accepted for publication (Прийнята до друку) 10.08.2022

Provide a cyber defense officer at the level of infrastructure

Vladislav Hol, Adel Rakivska, Dmytro Rakivsky

Abstract. Domestic and foreign regulations related to the protection of web applications are analyzed. The article analyzes and proposes conceptual principles of implementation of organizational and technical model of cyber defense, purpose and goals. The architecture of organizational and technical model of cybersecurity is considered, which is a structured system consisting of three cybersecurity infrastructures, namely: organizational and managerial cybersecurity infrastructure, as a set of cybersecurity entities that form and implement state policy in cybersecurity; cyber security technological infrastructure, as a set of cyber security forces and means, as well as infrastructure that ensures the functioning of cyber security forces, information and communication networks and their resources used in the interests of cyber security forces and basic cyber security infrastructure, as a set of critical information infrastructure assets, communication and technological systems of enterprises, institutions and organizations that are classified as critical infrastructure. Therefore, the application and implementation of organizational and technical model of cyber defense is aimed at analyzing security incidents, assessing their consequences, counteracting and blocking means of protection and improving security systems, rapid response to cyber threats, cyber incidents, countermeasures and minimize vulnerabilities in communication systems. It is through the application of the level of protection of the information and telecommunications system that the confidentiality, integrity and accessibility of information and information systems is ensured.

Keywords: cyber threat, information security system, complex information protection system, complex of protection means, objects of critical infrastructure.