УДК 004.4
DOI https://doi.org/10.32782/IT/2023-3-6

Олена МАРЧЕНКО
старший викладач кафедри інформатики та програмної інженерії, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», проспект Берестейський, 37, м. Київ, 03056
***ORCID:** 0000-0001-5754-4920*

Бібліографічний опис статті: Марченко, О. (2023). Кібербезпека та захист інформації: аналіз впливу ризиків та загроз із використанням сучасних ефективних стратегій кіберзахисту. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 50–59, doi: https://doi.org/10.32782/IT/2023-3-6

КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ: АНАЛІЗ ВПЛИВУ РИЗИКІВ ТА ЗАГРОЗ ІЗ ВИКОРИСТАННЯМ СУЧАСНИХ ЕФЕКТИВНИХ СТРАТЕГІЙ ЗАХИСТУ КІБЕРПРОСТОРУ

Сучасні тенденції розвитку та впровадження захисту від кібернетичних атак відіграють важливе значення у боротьбі проти кіберзлочинців, які завдають великої шкоди для сектора інформаційної безпеки кіберпростору (БКП). Актуальність проведення даного дослідження полягає в тому, що у зв'язку з військовою агресією в Україні кібернетичне середовище та безпека знаходяться у вразливому стані, так як методи та системи БКП постійно вдосконалюються, а разом з ними розвиваються методи вірусного програмного забезпечення для отримання конфіденційної та секретної інформації шляхом завантаження шкідливих компонентів. Найбільш вразливим є сектор критичної інфраструктури, який забезпечує функціонування громадян та країни в цілому надаючи необхідні послуги за допомогою цифрових технологій. З метою виявлення та дослідження загроз БКП проведено аналіз, який складається з методології, опису основних ризиків для запобігання загроз у системі БКП й пошуку ефективних рішень, де надається аналіз використання продуктів антивірусного програмного забезпечення для цифрових систем БКП. Актуальною проблемою даного дослідження є вивчення потенційних загроз та викликів інформаційному простору з проведенням аналізу ефективних рішень для підвищення БКП в Україні. Наукова новизна даного дослідження полягає у пошуку методології, згідно з якою буде можливо провести аналіз виявлення потенційних загроз для БКП. У даній роботі проаналізовані потенційні загрози та виклики для системи БКП, що обґрунтовано наступним: розглянута та проаналізована методологія побудови захисту системи, яка складається з шести основних етапів: моделювання, аналіз, планування, розробка, побудова та експлуатація. На основі проведеного дослідження було проаналізовано 6 різних пакетів антивірусного програмного забезпечення, де результати показали, що антивірус Kaspersky має значну перевагу у використанні на відміну від інших пакетів антивірусних програм. Серед наведених продуктів найкращі показники має Kaspersky, який заблокував 732 файли з рівнем захисту у 100% без виявлення помилок та попереджень, коли продукт Norton має найнижчі показники ефективності.

***Ключові слова:** безпека кіберпростору, інформаційні технології, кібернетичні загрози, кібернетичний захист.*

Olena MARCHENKO
Senior Lecturer of the Department of Computer Science and Software Engineering, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», 37 Beresteysky Avenue, Kyiv, 03056
***ORCID:** 0000-0001-5754-4920*

To cite this article: Marchenko, O. (2023). Kiberbezpeka ta zakhyst informatsiyi: analiz vplyvu ryzykiv ta zahroz iz vykorystanniam suchasnykh efektyvnykh stratehiy kiberzakhystu [Cybersecurity and information protection: analysis of the impact of risks and threats using modern effective cyber defence strategies]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 50–59, doi: https://doi.org/10.32782/IT/2023-3-6

CYBERSECURITY AND INFORMATION PROTECTION: ANALYSIS OF THE IMPACT OF RISKS AND THREATS USING MODERN EFFECTIVE CYBERSPACE PROTECTION STRATEGIES

Modern trends in the development and implementation of protection against cyberattacks are important in the fight against cyber criminals who cause great damage to the cyberspace information security (CSS) sector. The relevance of this study lies in the fact that due to the military aggression in Ukraine, the cyber environment and security are in

a vulnerable state, as the methods and systems of CSS are constantly improving, and along with them, the methods of virus software for obtaining confidential and secret information by downloading malicious components are developing. The most vulnerable sector is the critical infrastructure sector, which ensures the functioning of citizens and the country as a whole by providing essential services through digital technologies. In order to identify and study threats to the CSS, the author conduct an analysis consisting of a methodology, a description of the main risks to prevent threats in the CSS system and the search for effective solutions, where the author analyse the use of antivirus software products for digital CSS systems. The urgent problem of this study is to examine potential threats and challenges to the information space and to analyse effective solutions to improve CSS in Ukraine. The scientific novelty of this study lies in the search for a methodology that, based on the analysis, will allow identifying potential threats to the BCP. This paper analyses the potential threats and challenges to the CSS system, which is substantiated by the following: the methodology for building a system protection, which consists of six main stages: modelling, analysis, planning, development, construction and operation, is considered and analysed. Based on the research, 6 different antivirus software packages were analysed, where the results showed that Kaspersky antivirus has a significant advantage in use in contrast to other antivirus software packages. Among the products, Kaspersky has the best performance, blocking 732 files with a 100% protection level without detecting errors or warnings, while Norton has the lowest performance.

Key words: *cyberspace security, information technology, cyber threats, cyber defence.*

Вступ. Широкі можливості використання кіберпростору та додатків посприяли розвитку інформаційним технологіям (ІТ), однак одночасно з цим виникла вразливість до атак з будь-якої точки світу, що спонукає для розробки та впровадження ефективних технологій захисту від кібератак. Сучасні тенденції з використанням ІТ свідчать про те, що в кіберпросторі спостерігається інтенсивна діяльність, яка може приносити як прибуток одним людям, так і збитки іншим людям (Kafol, 2017, с. 87-90). Використання та зростання соціальних мереж з ресурсами для обміну даних посприяв розвитку онлайн-злочинності та кіберзлочинності, де інформаційна безпека зазнає нових проблем та викликів з питань безпеки кіберпростору (БКП) (Rajasekharaiah, 2020, с. 3-5). Загрози, які існують у кіберпросторі, стає дедалі важче виявляти, а їхнє запобігання вимагає як сучасних знань та обладнання, так і значних фінансових ресурсів. Тому завданням держави є прикладання зусиль (інституційних та фінансових) на заходи з БКП, які спрямовані для боротьби та протистояння з кібератаками (Karpiuk, 2021, с. 235-236).

Зловмисники, які завдають кібератаки на систему ІТ намагаються отримати несанкціонований доступ до апаратної та програмної системи з метою викрадення, змінення та знищення даних. Як зазначено на веб-сайті Microsoft, кібератаки поширюються окремими особами або організаціями з політичними, кримінальними або особистими намірами, щоб отримати або знищити доступ до секретної інформації (Mocean, 2022, с. 26-27). Тому погляди на БКП зазнають сучасних трансформацій, оскільки змінюється тип шкоди завдяки еволюції, де характер шкоди може бути руйнівним від шпигунства та DDoS-так до внесення серйозної фізичної шкоди інфраструктурі та впливу на громадську думку, наприклад втручання у внутрішні справи країни та втручання у державні вибори (Trasuk, 2020, с. 60). Окрім трансформації, неабиякого впливу відіграє адаптація, яка є серйозним викликом як для міжнародної спільноти, так і для кожної держави, для їхніх законодавчих, адміністративних та судових органів з метою досягнення імперативів БКП на користь прав громадян та держави в цілому (Bejan, 2020, с. 5).

Тому сучасні питання БКП стають національно-стратегічною проблемою, яка зачіпає всі сфери життя суспільства й потребує швидкої, ефективної та результативної боротьби з кібернетичними загрозами (КЗ), що вимагає визначення правильних та стратегічних цілей. Розробка національної стратегії БКП є першим та головним кроком у боротьбі з КЗ, де для розробки успішної та оптимальної національної стратегії необхідно проаналізувати наявні національні стратегії з безпеки та використати успішні практики протидії з метою уникнення КЗ (Tanriverdiyev, 2022, с. 19-21).

Запровадження управління національною БКП з метою задоволення потреб в державному органі для забезпечення координації й усунення невизначеності обумовлюється створенням ефективної організації, яка буде забезпечувати та контролювати всі можливі аспекти БКП для кожної країни (Senol, 2020, с. 1-3). Національна безпека відіграє важливу роль для мережевих технологій й забезпечує безпеку критичної інфраструктури. Забезпечення БКП критичної інфраструктури, тобто її захист від кібератак – є головною метою стратегії з БКП сучасних держав. Критична інфраструктура містить фізичні та віртуальні системи, забезпечення безпеки яких є невід'ємною частиною стратегії національної безпеки для сталого економічного розвитку держави (Daricili, 2021, с. 260-262).

Тому питання БКП досі залишається актуальним серед громадян та професіоналів усіх існуючих видів діяльності, які використовують цифрові технології. Тому для того, щоб визначити основні аспекти БКП необхідно розглянути планування та впровадження програм з підвищення обізнаності серед населення, які містять ключові стратегії, термінологію та оцінку ризиків (Dash, 2022, с. 1-2).

Актуальність проблеми. Актуальність безпеки інформаційного простору та БКП було одним з пріоритетних питань державної політики, а з врахуванням того факту, що сили оборони є невід'ємною складовою державної безпеки дослідження їх інформаційної безпеки є надзвичайно необхідним. Доцільність такого дослідження підтверджується тим, що в сучасних умовах розвитку інформаційних технологій сили оборони України повинні адаптуватися до сучасних викликів та загроз з метою забезпечення належного захисту інформації стратегічного значення для держави (Zolotar, 2021, с. 18-21).

Незважаючи на те, що Україна, як і інші країни, стикається з кібератаками, сучасні виклики для України пов'язані через військову агресію з боку країни-агресора, коли зловмисники (хакери) намагаються завдати шкоди та збитків урядовим установам, критичній інфраструктурі, приватним компаніям та громадянам України. Тому захист критичної інфраструктури спрямований на такі критичні об'єкти, як енергетично-паливний сектор, транспортний сектор та логістика, телекомунікації та інші важливі сектори, які забезпечують функціонування для повсякденного життя для громадян (Tymoshov, 2022, с. 138-140).

Іншим факторами є кіберзлочинність та недостатня свідомість (необізнаність), де шахрайство в Україні в умовах війни також залишається серйозною проблемою, включаючи «фішинг», обман, крадіжку даних, які врешті-решт призводять до втрати майна та грошових заощаджень з банківського рахунку (Alawida, 2022, с. 8176-8180). Недостатня свідомість характеризується тим, що безліч організацій та користувачів не володіють достатніми знаннями та свідомістю щодо загроз з питань БКП, що робить їх більш вразливими (Zwilling, 2020, с. 1-2).

Сучасні ефективні стратегії КЗ в Україні базуються на поєднанні технічних заходів, законодавчих рамок та освіти. Законодавча база характеризується тим, що Україна впроваджує законодавчі акти, які регулюють КЗ і кіберзлочинність, наприклад, Закон України «Про основні принципи забезпечення кібербезпеки», що встановлює правові засади захисту кіберпростору. На основі технічних заходів деякі організації в Україні використовують сучасні технології та рішення для захисту інформації та забезпечення конфіденційності даних, що обумовлюється використанням брандмауерів, антивірусів, систем виявлення вторгнень та інших інструментів. Однак збільшення свідомості про кібернетичні загрози та навчання персоналу відіграють найважливіше значення у стратегіях КЗ, що обумовлюється наданням знань університетами для навчання фахівців з обслуговування БКП (Negulescu, 2023, с. 66-73). З метою уникнення загроз проводяться регулярні та планові перевірки, де організації проводять регулярні аудити та планові перевірки систем КЗ для виявлення слабких місць та вразливостей (Oruj, 2023, с. 101-103).

З метою забезпечення безпеки кіберпростору необхідно дослідити стратегію, яка зможе забезпечити потреби держави, що характеризується вивченням методологічного підходу та аналізом ризиків виникнення загроз. Актуальною проблемою даного дослідження є вивчення потенційних загроз та викликів інформаційному простору з проведенням аналізу ефективних рішень для підвищення БКП в Україні.

Аналіз останніх досліджень та публікацій. Сучасні ІТ характеризуються використанням різних методів для трансформації майбутнього, наприклад, у роботі (Ferrag, 2020) авторами проведений огляд підходів глибокого навчання для виявлення вторгнень у БКП на основі використання набору даних, коли у роботі (Ma, 2021, с. 8000-8002) авторами досліджуються «розумні» технології, зокрема можливості «розумного» міста, які покращують життя для населення, але можуть містити ряд проблем з БКП. Проблеми безпеки пов'язані з тим, що «розумні» технології використовують системи Інтернету речей (IoT), де звичайні периферійні пристрої, датчики та системи моніторингу можуть бути вразливими для DDoS-атак з боку зловмисників. Незважаючи на цей недолік в Україні все ще бракує спеціального обладнання та систем, щоб забезпечити місто «розумними» технологіями, зокрема лише для задоволення потреб громадянина, який завдяки смартфону дистанційно керує з'єднаними пристроями та технікою. Однак індивідуальне використання таких технологій може викликати загрози безпеки, наприклад, зв'язуючи смартфон з електронним браслетом Mi Band й використовуючи функцію NFC (*Near field communication*) зловмисники можуть запо-

діяти шкоду, якщо отримають доступ конфіденційної інформації для дистанційного керування пристроями (Vieau, 2022, с. 12-16).

Розвиток ІТ та їх використання збільшує взаємопов'язану цифрову систему, що супроводжується інтенсивним використанням даних. Скрізь де доступні цифрові дані існує загроза кібератак, що збільшує потребу у профілактиці та пошуку нових методів боротьби з новими загрозами та проблемами. У роботах (Parpulova, 2021; Süzen, 2020) досліджується Індустрія 4.0, де основним «паливом» є дані кіберпростору (оцифрування даних) для критичної інфраструктури. Сфера транспортування енергоресурсів є надзвичайно важливою для будь-якої країни, однак на думку авторів рахуються вразливими, так як нафтохімічні трубопроводи є дорогими у будівництві та спроєктовані без особливого захисту від кібератак у будівництві. Вразливості БКП, які найбільш очевидні в системах Індустрії 4.0 складаються з протоколів систем управління й незахищеного з'єднання, що свідчить про знехтування деякими стратегіями БКП.

Однак разом з Індустрією 4.0 також активно розвивалися технології у галузі робототехніки та машинобудування, де цифрова революція призвела до того, що роботи стали інтегрованими для використання у різних сферах, наприклад, господарство, медицина, промисловість (Yaacoub, 2022). Однак, на думку авторів (Kucharska, 2020), деякі непередбачені аварії, які можуть спричинити зловмисники може призвести до негативних наслідків, які можуть загрожувати безпеці людей. Авторами відзначається, як зловмисники можуть викрадати роботів та контролювати їх свідомістю, що може призвести до економічних та фінансових збитків для країни.

Інформаційний захист та корпоративна стійкість до інформаційного витоку інформації та шахрайства в усіх його проявах є запорукою успіху для ефективного функціонування будь-якої організації, незалежно від типу та форми власності. Деякі з досліджень не можуть гарантувати кібербезпеку на практиці, але можуть доповнити та розширити наявні методи та технології. Авторами на основі огляду літератури у роботі (Loishyn, 2021, с. 1449) проведений аналіз за період 1999-2020 років, який дозволив простежити чітку тенденцію хакерських методів, де кіберзлочинці об'єднуються в онлайн-групи (наприклад, Anonymous, Red Hacker Alliance), які спільними зусиллями проводять атаку на зацікавлені об'єкти. Отримані дані у цій роботі свідчать про те, що об'єктами кібератак можуть бути державні організації, комерційні організації, банківські установи, приватні рахунки та акаунти, але характер та методи діяльності хакерів можуть мати не лише економічні цілі, але й політичні, що може прирівнюватися у деяких випадках до кібертерористів.

Серед практичних та ефективних методів підвищення безпеки інформаційного простору можуть слугувати оптимізація та посилення стратегічного лідерства, що є ключовими аспектами для забезпечення реалізації бачення БКП. У роботі (Lehto, 2021, с. 139-140) авторами зазначається, що стратегічне лідерство у сфері БКП передбачає визначення та постановку цілей, які засновані на захисті цифрового операційного середовища, а також передбачає координацію дій та готовність, що дозволяє проводити управління масштабними перебоями. Однак для того, щоб забезпечити БКП та досягти поставлених стратегічних цілей, суспільство має залучати різні сторони та узгоджувати ресурси й напрямки дій якомога ефективніше.

Основна термінологія з БКП, ризики та стратегії наведені у роботах (Chelani, 2022, с. 6-7; Mocean, 2023, с. 29-30; Yaacoub, 2021, с. 121-131; Suzen, 2020, с. 8-10; Negulescu, 2022, с. 68-72), де надається основна інформація та методологія для пошуку стратегій, які можуть ефективно використовуватися для БКП. Деякі світові дослідження досі вивчають негативний вплив заподіяної шкоди кіберзлочинцями, однак авторами у роботі (Guchua, 2022, с. 1) зауважено, що сьогоднішні захисні механізми не можуть цілком виправдати ефективно в ситуаціях, що склалася з державою-агресором, так як держава-агресор може переймати нові технології та використовувати їх для шкоди іншим країнам.

Метою даного дослідження є виявлення загроз для БКП з проведенням аналізу, який обумовлений: а) методологією; б) вивченням та описом основних ризиків, які можуть виникнути у БКП; в) пошуком ефективних рішень з використанням антивірусного програмного забезпечення для цифрових систем БКП. Для досягнення поставленої мети необхідно вирішити наступні **задачі**: проаналізувати основні методи та стратегії, які використовувалися за останні 5-10 років; проаналізувати основні ризики виникнення загроз у БКП; визначити основні вразливі критерії (параметри) у системі БКП. **Предметом дослідження** є кіберпростір та інформаційні технології. **Наукова новизна** даного дослідження полягає у пошуку методології, згідно з якою буде можливо провести аналіз виявлення потенційних загроз для БКП.

Виклад основного матеріалу дослідження. У даній роботі використовувалася методологія БКП на основі роботи (Kafol, 2017) з метою розкриття потенціалу можливостей протидії загрозам, які можуть виникнути з боку зловмисників – кіберзлочинців й проаналізуємо матеріал досліджень деяких робіт, які пов'язані з ризиками та виникненням шкідливих факторів. Кібернетичні атаки проаналізовані у дослідженні (Mocean, 2022), де буде описано основні фактори утворення ризиків сучасних БКП. З метою кращого вивчення та проведення аналізу використані джерела з термінологією (Tsaruk, 2020; Süzenm 2020), які допоможуть більш детально розкрити вразливі параметри у системі БКП.

Методологія. Превентивна методологія, яка досліджується й охоплює 3 елементи, а саме запобігання, виявлення та реагування, які здатні захищати 3 унікальні атрибути інформації: конфіденційність, цілісність та доступність. Ключовими аспектами такої методології є: таксономія – звіт (класифікація комунальних мереж з урахуванням типу та комунікаційних технологій з чутливістю до кібернетичних загроз); моделювання та імітація – програмне забезпечення цифрової моделі з віртуальним середовищем для моделювання та збору даних про кібератаки; програмне забезпечення для виявлення загроз (мережа, хост та процеси) та засобів кореляції подій; КЗ на основі методологічної основи з управляючими принципами. Окрім того, методи оцінки ризиків та вразливостей містять стандартні процедури та інструкції для запобігання кібератакам забезпечуючи конфіденційність та захист даних.

Побудова методології складається з 6 основних етапів, а саме: імітування (моделювання), аналіз, планування, розробка, побудова та експлуатація. Створення захисту для системи БКП враховує початкову фазу з імітуванням та аналізом на початковому етапі. Фаза планування, яка знаходиться між початковою фазою та фазою впровадження є ключовою для розробки та планування техніко-економічних критеріїв зі створенням належного рівня захисту. Інші три фази (розробка, побудова та експлуатація) є фазами впровадження й складаються з елементів, які необхідні для створення ресурсів та активів з метою захисту організації від кібератак. Цикл зворотного зв'язку призначений для того, щоб на початковій фазі можна було повернутися від фази аналізу до фази моделювання для перевірки параметрів. На етапі реалізації необхідно постійно повертатися від оперативної фази до фази розробки по колу, щоб постійно вдосконалювати захист від постійно мінливого ворожого середовища. Існує також необхідність постійно повертатися від фази реалізації до початкової фази для того, щоб оцінити, чи стратегія з тактикою ще стійкі. На рис. 1 показано методологію з шести основних етапів.

Етап моделювання складається з наступних операцій:

– побудова моделі топології системи або мережі (ключові об'єкти, які здатні увімкнути комп'ютери та технічні пристрої, наприклад, прилади обліку електроенергії, споживачі електроенергії тощо);

– ймовірнісні змінні визначаються для різних подій, які мають відношення до потенційних кібератак на різних вузлах, з'єднаннях, де ймовірності у результаті оцінюються й призначаються для різних змінних;

– моделювання дискретних подій для мережевої моделі та ймовірнісних змінних, які причетні до кібератак;

– результати моделювання підлягають агрегації для статичного виявлення вразливих місць мережевих об'єктів.

Проведення аналізу відбувається на основі систематичного та цілісного підходу, де спочатку кожен об'єкт у модельованій топології аналізується ізольовано. У разі, якщо він піддається високим ризикам безпеки, це є індикатором того, що необхідно вжити відповідних заходів безпеки для уникнення та зменшення ризиків. Часткові ризики окремого об'єкта оцінюються на основі частоти змодельованих кібератак на цей об'єкт.

Під час проведення аналізу необхідно провести оцінку серйозності ризиків, якщо об'єкти модельованої мережі взаємопов'язані з багатьма іншими об'єктами, які також піддаються високій частоті змодельованих кібератак, то серйозність ризику для об'єкта є критично важливим. У подібних випадках приймаються та впроваджуються заходи з уникнення ризиків, які повинні призвести до модифікації та поліпшення топології мережі, а також до ітеративного повторення кроку моделювання.

Проведення планування є важливим при розробці бажаного рівня безпеки, де техніко-економічне обґрунтування необхідно проводити для оцінки підходу з висвітленням результатів попередніх двох етапів для визначення економічної доцільності дій. Для планування залучаються всі зацікавлені сторони, а визначені ризики повинні враховуватися в стратегіях їх зменшення. Економічна та технічна ефективність сценаріїв оцінюється шляхом застосування багатокритеріальної моделі, що підтри-

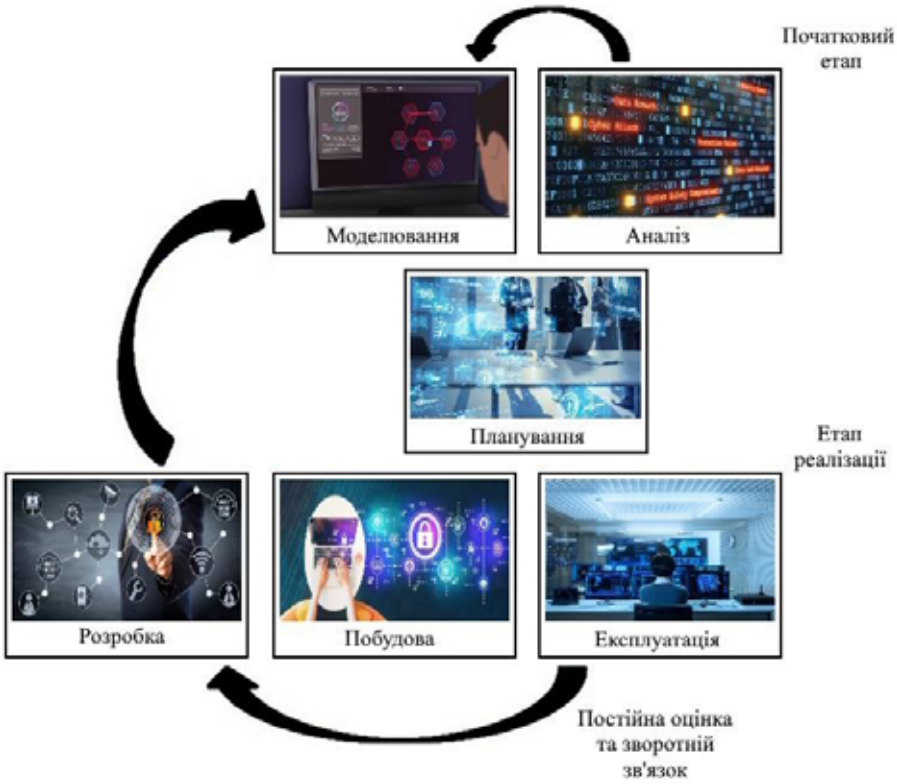

Рис. 1. Побудова методології на основі шести етапів

Джерело: сформовано авторкою на основі (Kafol, 2017)

має неповну або нечітку інформацію, а також з врахуванням різних структур і стилів переваг в умовах групового прийняття рішень.

На етапі планування необхідно ретельно та систематично розглянути три ключові елементи процесу забезпечення кібербезпеки. На основі виявлених та проаналізованих ризиків можна визначити стійкі стратегії запобігання, а ефективні стратегії реагування та механізми можуть використовуватися для подолання виявлених загроз безпеці, атак та проблем у системі БКП.

Фаза розробки є першим кроком процесу впровадження, де процес розробки повинен здійснюватися у всіх сферах з людськими ресурсами, апаратними та програмними компонентами. Визначення ключових елементів для операційного центру безпеки (ОЦБ) є важливою частиною цього етапу, а також глибини та способу функціонування.

Етап побудови є другорядною частиною процесу впровадження і складається з придбання та встановлення елементів ОЦБ, який обладнаний для моніторингу, управління освітленням, сигналізацією та бар'єрами.

Етап експлуатації починається з введення системи в експлуатацію та запуску ОЦБ у виробництво, де мають вирішуватися операційні, організаційні та культурні питання. Зусилля, які спрямовані на підвищення ефективності роботи ОЦБ, зосереджені на створенні інструментів для аналітиків або розумінні людських та організаційних факторів. Пробна експлуатація повинна окреслити потенційні проґалини та загрози безпеці. На етапі експлуатації необхідно постійно оцінювати ефективність і зворотний зв'язок з етапом розробки, встановлений для усунення потенційних прогалин. Важливо підкреслити, що останні три фази повинні постійно повторюватися, щоб реагувати на зміни у кібернетичному середовищі та підтримувати і покращувати рівень кібербезпеки. Якщо зворотний зв'язок та реагування відбувається швидше, ніж змінюється середовище, рівень безпеки підвищується, а якщо повільніше – знижується.

Структура виявлення вразливих компонентів у системі БКП. Розглянемо коротко структуру з виявлення вразливих компонентів у системі БКП на рис. 2, де кожен вразливий фактор може слугувати кібернетичною атакою. На рисунку 2 детально показані вразливі місця, які можуть бути цілями кібератак, починаючи з електронної пошти і закінчуючи атакою на об'єкти інфраструктури.

Акаунти електронної пошти: підробка електронної пошти з використанням методів викрадення паролів по словнику; бомбардування,

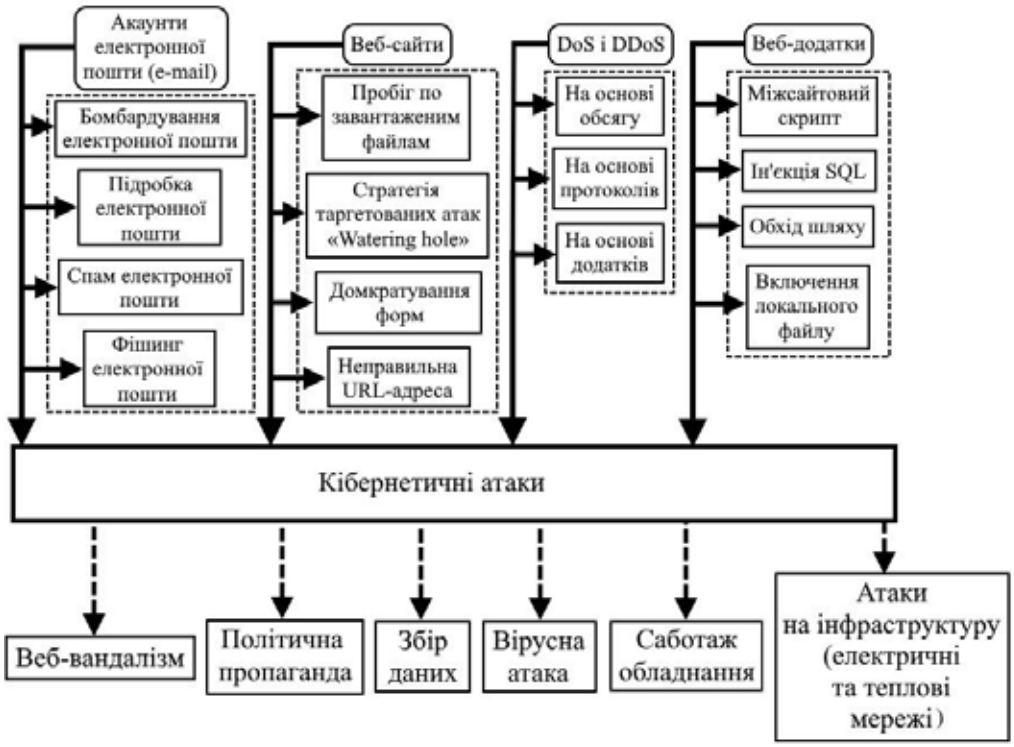

Рис. 2. Вразливі компоненти до кібератак в системі КПБ

Джерело: сформовано авторкою на основі (Mocean, 2023)

наприклад, Hacker Bomber; спам; фішинг (підміна сайту надійних організацій та установ), де користувачеві надсилають електронний лист з підробленою адресою, яка не відноситься до безпечних сайтів й вводить користувача в оману;

DoS-атаки відбуваються з використанням десятків тисяч скомпрометованих комп'ютерів для перевищення пропускної здатності веб-сервера за рахунок трафіку. Після запуску атаки важко зупинити, тому що інформаційні потоки надходять з різних місць. У випадку такої атаки, веб-сторінки швидко переповнюються фальшивими доступом запущеними зі скомпрометованих комп'ютерів, розкиданих по всьому світ

Вразливості, які виникають з веб-сайтами та веб-додатками обумовлюється: недостатньою аутентифікацією з авторизацією; SQL-ін'єкцією (зловмисні SQL-коди); міжсайтовим скриптингом (XSS), вразливостями на сервері (що потребує оновлення веб-серверів та фреймворків для уникнення використання вразливостей); незахищеними завантаженням файлів; вразливостями на боці клієнта та інше.

Проаналізуємо види кібератак:

– веб-вандалізм (призводить до пошкодження веб-сторінок й відмови в доступі до певних сторінок, де атаки швидко протидіють й завдають менш значної шкоди;

– пропаганда (повідомлення політичного змісту та характеру, які можуть поширюватися будь-ким, хто має доступ до мережі Інтернет, наприклад, втручання у вибори, фальсифікація голосів, опублікування фейкових результатів);

– збір даних (секретна інформація, яка не захищена може перехоплюватися й змінюватися, що прирівнюється до шпигунства);

– атаки комп'ютерних вірусів (після активації вірус завдає шкоди, змінює або знищує інформацію, створює фіктивні транзакції з передачею даних;

– саботаж обладнання (військова діяльність, яка використовує комп'ютери та супутники для координації і відноситься до вразливих таких атак;

– атаки на критичну інфраструктуру (комунальні послуги, енергоресурси, торгівля, транспорт та логістика відноситься до вразливих об'єктів).

Використання антивірусного програмного забезпечення. Вибір антивірусного програмного забезпечення залежить від ситуації, потреб та пристроїв. Розглянемо декілька відомих пакетів антивірусного програмного забезпечення:

1. Bitdefender, який характеризується своєю ефективністю та низьким впливом на продуктивність системи.

2. Kaspersky, який має сильну репутацію через виявлення та захист від широкого спектру загроз.

Таблиця 1

Порівняння ефективності виявлення загроз безпеки для БКП

Продукт	Блок та захист	Захист	Попередження
Avast	728	99,3%	3
Bitdefender	732	99,8%	4
ESET NOT32	729	99,4%	11
Kaspersky	732	100%	0
McAfee	729	99,5%	7
Norton	727	98,9%	16

3. Norton, який містить додаткові інструменти для онлайн-безпеки та КЗ.

4. McAfee, який пропонує захист від антивірусів та інших загроз, а також надає інструменти для безпеки в Інтернеті.

5. ESET NOT32, який відомий за своєю швидкістю та ефективністю виявлення загроз.

6. Avast, який містить безкоштовну версію та включає в себе додаткові функції (захист від шпигунського програмного забезпечення та файрвол – брандмауер).

Таким чином, для системи БКП можуть застосовуватися різні види антивірусного програмного забезпечення, однак варто врахувати те, що безліч експериментів у кіберпросторі проводилися з використанням Kaspersky.

Як видно з табл. 1, найбільш ефективним антивірусним програмним забезпеченням є Kaspersky, в якому з виявлених 732 загроз було заблоковано та переміщено у карантин із захистом 100%, коли у Norton найменший показник захисту 98,9% й найбільший показник попереджень з виявленням потенційних 16 загроз. Отже, для використання систем БКП антивірусне програмне забезпечення Kaspersky може забезпечити ефективну та безпечну роботу у кіберпросторі.

Висновки і перспективи подальших досліджень. У даній роботі проаналізовані потенційні загрози та виклики для системи БКП, що обґрунтовано наступним: розглянута та проаналізована методологія побудови захисту системи, яка складається з шести основних етапів: моделювання, аналіз, планування, розробка, побудова та експлуатація. Окрім зазначених етапів в побудову даної методології входить також цикл зворотного зв'язку, функція якого є повернення на початкову фазу аналізу або до фази імітування з метою перевірки параметрів.

Проаналізовано структуру з метою виявлення вразливих компонентів у системі БКП. З'ясовано, що система БКП може зазнавати як найменший шкідливий вплив з використанням веб-сайтів, веб-додатків, так і критичний з проведенням DoS та DDoS-атак, що може значно навантажувати систему через використання значної кількості скомпрометованих комп'ютерів для перевищення пропускної здатності веб-сервера. Проаналізовані види кібератак, які можуть вживатися з окремою метою, наприклад, пропаганда є спробою внутрішнього втручання у парламентські або президентські вибори, а атаки на критичну інфраструктуру можуть значно вплинути на функціонування міста, що пояснюється роботою цифрових технологій та комунікацій, наприклад, транспорт, електропостачання. В окремих випадках кібербезпека є важливою з точки зору оборони держави, коли необхідно використовувати ІТ для моніторингу подій, які можуть загострюватися у результаті військової агресії двох сусідніх країн.

На основі проведеного дослідження було проаналізовано 6 різних пакетів антивірусного програмного забезпечення, де результати показали, що антивірус Kaspersky має значну перевагу у використанні на відміну від інших пакетів антивірусних програм. Серед наведених продуктів найкращі показники має Kaspersky, який заблокував 732 файли з рівнем захисту у 100% без виявлення помилок та попереджень, коли продукт Norton має найнижчі показники ефективності.

ЛІТЕРАТУРА:

1. Kafol C., & Bregar A. Cyber Security–Building a Sustainable Protection. *DAAAM International Scientific Book*, 2017. Pp. 81-90.

2. Rajasekharaiah K.M., Dule C.S., & Sudarshan E. Cyber security challenges and its emerging trends on latest technologies. *In IOP Conference Series: Materials Science and Engineering,* 2020.Vol. 981, No. 2, p. 022-062. IOP Publishing, 1-7.

3. Karpiuk M. Organisation of the National System of Cybersecurity: Selected Issues. *Studia Iuridica Lublinensia*, 2021. Vol. 30(2), pp. 233-244.

4. Mocean L., & Vlad M.P. Cybersecurity in the post covid era. *Fiat Iustitia*, 2022. Vol. (2), pp. 26-36.

5. Tsaruk O., & Korniiets M. Hybrid nature of modern threats for cybersecurity and information security. *Smart Cities and Regional Development (SCRD) Journal*, 2020. Vol. 4(1), pp. 57-78.

6. Bejan F. Cybersecurity and Cybercrime: Challenges Of An Invisible Space. *Perspectives of Law and Public Administration*, 2022. Vol. 11(1), pp. 5-10.

7. Tanriverdiyev E. The state of the cyber environment and national cybersecurity strategy in developed countries. *Studia Bezpieczeństwa Narodowego*, 2022. Vol. 23(1), pp. 19-26.

8. Senol M., & Karacuha E. Creating and implementing an effective and deterrent national cyber security strategy. *Journal of Engineering*, 2020, pp. 1-19.

9. Daricili A.B., & Celik S. National Security 2.0: The Cyber Security of Critical Infrastructure. *PERCEPTIONS: Journal of International Affairs*, 2022. Vol. 26(2), pp. 259-276.

10. Dash B., & Ansari M.F. An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy, 2022. Pp. 1-6.

11. Zolotar O.O., Zaitsev M.M., Topolnitskyi V.V., Bieliakov K.I., & Koropatnik I.M. Prospects and Current Status of Defence Information Security in Ukraine. *Hasanuddin Law Review*, 2022. Vol. 8(1), pp. 18-29.

12. Alawida M., Omolara A.E., Abiodun O.I., & Al-Rajab M. A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University-Computer and Information Sciences*. 2022.

13. Zwilling M., Klien G., Lesjak D., Wiechetek Ł., Cetin F., & Basim H. N. Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 2022. Vol. 62(1), pp. 82-97.

14. Tymoshov Y. Ukraine's national security sector: challenges and threats in the information space. *Reality of Politics. Estimates-Comments-Forecasts,* 2022. Vol. 21(3), pp. 137-149.

15. Negulescu O.H., Doval E., & Stefanescu A.R. Actual and future digital threats and their impact on civil and military cybersecurity management. *Przegląd Nauk o Obronności*, 2023. Vol. (15), pp. 60-84.

16. Oruj Z. Cyber Security: contemporary cyber threats and National Strategies. *Distance Education in Ukraine: Innovative, Normative-Legal, Pedagogical Aspect*s, 2023. Vol. (2), pp. 100-116.

17. Ferrag M.A., Maglaras L., Moschoyiannis S., & Janicke H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 2020. Vol. 50, 102419, pp. 1-19.

18. Ma C. Smart city and cyber-security; technologies used, leading challenges and future recommendations. *Energy Reports*, 2021. Vol. 7, pp. 7999-8012.

19. Vieau M. Innovative Methods Cybersecurity Professionals Can Use to Reduce Threats against RFID Authentication Systems (Doctoral dissertation, Colorado Technical University). 2022.

20. Parpulova N., & Zinoviev V. Cybersecurity in the Transportation of Energy Resources. *Godishnik na UNSS*, 2021. Vol. (2), pp. 131-146.

21. Süzen A.A. A risk-assessment of cyber attacks and defense strategies in industry 4.0 ecosystem. *International Journal of Computer Network and Information Security*, 2020. Vol. (1), pp. 1-12.

22. Yaacoub J.P.A., Noura H.N., Salman O., & Chehab A. Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*, 2022. Pp. 1-44.

23. Kucharska A. Cybersecurity challenges in Poland in the face of energy transition. *Rocznik Instytutu Europy Środkowo-Wschodniej*, 2020. Vol. 18(1), pp. 141-159.

24. Loishyn A.A., Hohoniants S., YaTkach M., Tyshchenko M.H., Tarasenko N.M., & Kyvliuk V.S. Development of the Concept of Cybersecurity of the Organization. *TEM Journal*, 2021. Vol. 10(3), pp. 1-7.

25. Lehto M., & Limnéll J. Strategic leadership in cyber security, case Finland. *Information Security Journal: A Global Perspective*, 2021. Vol. 30(3), pp. 139-148.

26. Ghelani D., Hua T.K., & Koduru S.K.R. Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. *Authorea Preprints,* 2022. Pp. 1-9.

27. Guchua A., & Zedelashvili T. The Problem of Security Protection of Strategic *Objects in the Conditions of Modern Cybersecurity*, 2022. Pp. 1-8.

REFERENCES:

1. Kafol, C., & Bregar, A. (2017). Cyber Security–Building a Sustainable Protection. *DAAAM International Scientific Book*, 81-90.

2. Rajasekharaiah, K.M., Dule, C.S., & Sudarshan, E. (2020). Cyber security challenges and its emerging trends on latest technologies. *In IOP Conference Series: Materials Science and Engineering* (Vol. 981, No. 2, p. 022-062). IOP Publishing, 1-7.

3. Karpiuk, M. (2021). Organisation of the National System of Cybersecurity: Selected Issues. *Studia Iuridica Lublinensia*, 30(2), 233-244.

4. Mocean, L., & Vlad, M.P. (2022). Cybersecurity in the post covid era. *Fiat Iustitia*, (2), 26-36.

5. Tsaruk, O., & Korniiets, M. (2020). Hybrid nature of modern threats for cybersecurity and information security. *Smart Cities and Regional Development (SCRD) Journal*, 4(1), 57-78.

6. Bejan, F. (2022). Cybersecurity And Cybercrime: Challenges Of An Invisible Space. *Perspectives of Law and Public Administration*, 11(1), 5-10.

7. Tanriverdiyev, E. (2022). The state of the cyber environment and national cybersecurity strategy in developed countries. *Studia Bezpieczeństwa Narodowego*, 23(1), 19-26.

8. Senol, M., & Karacuha, E. (2020). Creating and implementing an effective and deterrent national cyber security strategy. *Journal of Engineering*, 2020, 1-19.

9. Daricili, A.B., & Celik, S. (2022). National Security 2.0: The Cyber Security of Critical Infrastructure. *PERCEPTIONS: Journal of International Affairs*, 26(2), 259-276.

10. Dash, B., & Ansari, M.F. (2022). An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy, 1-6.

11. Zolotar, O.O., Zaitsev, M.M., Topolnitskyi, V.V., Bieliakov, K.I., & Koropatnik, I.M. (2022). Prospects and Current Status of Defence Information Security in Ukraine. *Hasanuddin Law Review*, 8(1), 18-29.

12. Alawida, M., Omolara, A.E., Abiodun, O.I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University-Computer and Information Sciences*.

13. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 62(1), 82-97.

14. Tymoshov, Y. (2022). Ukraine's national security sector: challenges and threats in the information space. *Reality of Politics. Estimates-Comments-Forecasts,* 21(3), 137-149.

15. Negulescu, O.H., Doval, E., & Stefanescu, A.R. (2023). Actual and future digital threats and their impact on civil and military cybersecurity management. *Przegląd Nauk o Obronności*, 2022(15), 60-84.

16. Oruj, Z. (2023). Cyber Security: contemporary cyber threats and National Strategies. *Distance Education in Ukraine: Innovative, Normative-Legal, Pedagogical Aspect*s, (2), 100-116.

17. Ferrag, M.A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50, 102419, 1-19.

18. Ma, C. (2021). Smart city and cyber-security; technologies used, leading challenges and future recommendations. *Energy Reports*, 7, 7999-8012.

19. Vieau, M. (2022). Innovative Methods Cybersecurity Professionals Can Use to Reduce Threats against RFID Authentication Systems (Doctoral dissertation, Colorado Technical University).

20. Parpulova, N., & Zinoviev, V. (2021). Cybersecurity in the Transportation of Energy Resources. *Godishnik na UNSS*, (2), 131â-146.

21. Süzen, A.A. (2020). A risk-assessment of cyber attacks and defense strategies in industry 4.0 ecosystem. I*nternational Journal of Computer Network and Information Security*, (1), 1-12.

22. Yaacoub, J.P.A., Noura, H.N., Salman, O., & Chehab, A. (2022). Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*, 1-44.

23. Kucharska, A. (2020). Cybersecurity challenges in Poland in the face of energy transition. *Rocznik Instytutu Europy Środkowo-Wschodniej*, 18(1), 141-159.

24. Loishyn, A.A., Hohoniants, S., YaTkach, M., Tyshchenko, M.H., Tarasenko, N.M., & Kyvliuk, V.S. (2021). Development of the Concept of Cybersecurity of the Organization. *TEM Journal*, 10(3), 1-7.

25. Lehto, M., & Limnéll, J. (2021). Strategic leadership in cyber security, case Finland. *Information Security Journal: A Global Perspective*, 30(3), 139-148.

26. Ghelani, D., Hua, T.K., & Koduru, S.K.R. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. *Authorea Preprints,* 1-9.

27. Guchua, A., & Zedelashvili, T. (2022). The Problem of Security Protection of Strategic *Objects in the Conditions of Modern Cybersecurity*, 1-8.