УДК 004.056:004.9

КІБЕРБЕЗПЕКА ЧЕРЕЗ ПРИЗМУ СИСТЕМНОГО АНАЛІЗУ

У. П. Пановик[1], Р. Л. Ткачук[2]

[1]Українська академія друкарства, вул. Під Голоском, 19, Львів, 79020, Україна

[2] Львівський державний університет безпеки життєдіяльності, вул. Клепарівська, 35, Львів, 79007, Україна

Кібербезпека охоплює широкий спектр заходів, спрямованих на захист інформаційних систем, комп'ютерних мереж і даних від несанкціонованого доступу, знищення, крадіжки або пошкодження. Аналіз безпеки є критичним етапом у розробленні безпекових заходів, що дає змогу виявити уразливість системи та встановити вимоги безпеки на ранніх етапах проєктування. Зростання складності сучасних систем вимагає нового підходу до аналізу безпеки. Традиційні методи не дають достатньої потужності для виявлення небезпечних інцидентів, які відображаються у взаємодії між фізичними системами, людьми та соціальними об'єктами. Встановлено, що використання системного аналізу дає можливість простежувати кібербезпеку як складну систему з взаємодіючими компонентами для виявлення, аналізу та управління ризиками, пов'язаними з інформаційною безпекою. Розглянуто методи системного аналізу для синтезу кібербезпеки, розроблення стратегії загроз для систем та шляхів їх вирішення. Застосовано метод 5W1H та методологія STPA-Sec, які дали змогу узагальнити та пояснити комплексні аспекти кібербезпеки через аналіз взаємодії компонентів системи, функціональної структури та інформаційних потоків. Проведене дослідження розкриває важливість системного підходу до аналізу кібербезпеки та показує, що використання методів системного аналізу сприяє виявленню загроз та вирішенню проблем безпеки. Це дає змогу покращити ефективність стратегії та управління загрозами кібербезпеки

Ключові слова: *кібербезпека, системний підхід, синтез та аналіз, методи системного аналізу, метод 5W1H, методологія STPA-Sec.*

Постановка проблеми. Кібербезпека є величезним аспектом у сучасному цифровому світі, де загрози та атаки від хакерів та зловмисників зростають у розмірі та складності. Однак, у контексті швидко зростаючих загроз та складних кібератак, традиційні методи захисту виявляються недостатніми. Складний характер кіберзагроз вимагає нового комплексного підходу до

виявлення, оцінки та запобігання атакам. Для ефективного забезпечення кібербезпеки та розуміння комплексності цієї проблеми необхідне використання системного аналізу. Цей підхід дає змогу розглядати кібербезпеку як складну систему, що включає людей, процеси, технології та середовище. Він дає можливість визначити вплив кібератак на систему загалом, виявити слабкі місця та розробити ефективні стратегії захисту. Вивчаючи компоненти, взаємозв'язки та динаміку системи, системний аналіз виявляє взаємозв'язки та вразливості, оцінює ризики, прогнозує наслідки збоїв та розробляє ефективні заходи безпеки, сприяє підвищенню рівня кібербезпеки від загроз, забезпечує стійкість системи та захист конфіденційності, цілості та доступності даних. Він допомагає розробити комплексний підхід до захисту з огляду на технічні, організаційні та людські аспекти. Актуальним завданням є розкрити потенціал системного аналізу в побудові ефективних стратегій кібербезпеки та визначити його переваги для захисту цифрових систем у сучасному світі.

Аналіз останніх досліджень та публікацій. Останні дослідження та публікації відображають збільшення уваги до взаємозв'язку між кібербезпекою та системним аналізом. Вони підтверджують, що системний аналіз є потужним інструментом для розуміння, аналізу та управління кібербезпекою. Наприклад, у публікації [1] розглядаються ключові принципи системного мислення і їх застосування до кібербезпеки. Автор висвітлює різні аспекти моделювання, включно з аналізом структури системи, взаємодією між її компонентами та впливом зовнішніх факторів. А автори статті [2] розглядають важливість використання моделей для представлення системи з погляду безпеки. Вони пропонують різні технології, такі як атакування та захист моделей, аналіз уразливостей та оцінку ризиків, які допомагають виявляти потенційні загрози та розробляти ефективні стратегії безпеки.

У [6] автори стверджують, що кібербезпека має бути розглянута як системна проблема, і пропонують підхід, що базується на ризикоорієнтованому мисленні та системному аналізі. У ній наголошується на необхідності використання розумних системних підходів до кібербезпеки, зокрема, використання інструментів ризикоорієнтованого аналізу, математичного моделювання та інших методів системного аналізу. У [3] автори визначають важливість захисту критичної інфраструктури від кіберзагроз та пропонують системний підхід до розроблення та функціонування центрів кібербезпеки. Вони розглядають різні аспекти системного аналізу, включаючи архітектурні рішення, організаційні структури та технологічні рішення, необхідні для ефективного захисту інфраструктури.

А для розуміння широкого контексту системного аналізу та його значення для кібербезпеки цінним джерелом є книга [4], яка присвячена основам системного аналізу та проєктування, забезпечуючи повне розуміння процесу та залучених методів.

Мета статті – дослідити методи та підходи системного аналізу, які можуть бути використані для забезпечення кібербезпеки сучасного інформаційного простору.

Виклад основного матеріалу дослідження. Системний аналіз – це методологічний підхід до розв'язання складних проблем, який зосереджується на дослідженні та аналізі складних систем. З допомогою системного аналізу можна збирати та аналізувати інформацію про певну проблему з розумінням її складності, інтерактивності та взаємозв'язку між її складовими елементами. Системний аналіз передбачає аналіз системи; її декомпозицію, потоковий аналіз, системне моделювання, статистичний аналіз, експертну оцінку та інші. Вони надають системний підхід до збору та аналізу інформації про проблему, допомагають визначити складні зв'язки та зробити обґрунтованим рішення для її рішення.

Збір та аналіз інформації про певну проблему в системному аналізі можна здійснити з допомогою різних методів, які є добрими інструментами для реалізації поставлених завдань. Вибір конкретного методу залежить від характеру проблеми, доступних ресурсів та потреби аналізу. Наприклад, мозковий штурм (Brainstorming), метод Дельфі (Delphi Method) Однак, для активації творчого мислення можна застосувати швидкий та простий метод 5W1H, який базується на запитання, що починаються зі слів What?, When?, Why?, Who?, Where? та How? Відповіді на ці запитання дають можливість набути більшого розуміння дослідницької системи, ідентифікацію потреб і проблем, а також розроблення рішень та стратегій:

- What? (Що?) – запитання, що вимагає сутності проблеми або ситуації та спрямоване на визначення ключових аспектів, подій, процесів або об'єктів.
- Where (Де?) – запитання, що стосується просторових аспектів системи або ситуації та спрямоване на визначення місця, локації або контексту, у якому відбуваються події або функціонує система.
- When? (Коли?) – запитання, яке ставиться до будь-яких часових параметрів проблеми або ситуація та орієнтоване на визначення хронології подій, термінів, змін.
- Who? (Хто?) – запитання, яке спрямоване на ідентифікацію осіб або груп, які є більшими для розуміння ситуації або проблеми.

- Why (Чому?) – запитання, що спрямоване на розуміння причини та мотивів, які лежать в основі проблеми або ситуації.
- How? (Як?) – запитання, що спрямоване на розуміння процесів, механізмів та способів функціонування системи. Воно дає можливість досліджувати методи й засоби, з допомогою яких відбуваються або реалізуються події системою.

Отже, застосуємо цю технологію аналізу даних у сфері кібербезпеки.

Що таке кібербезпека? «Кібербезпека – захищеність життєво важливих інтересів людини та громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [9]. Отже, кібербезпека – це галузь знань, що зосереджується на захисті комп'ютерних систем, мереж, програмного забезпечення та даних від загроз, що пов'язані з інформаційною безпекою. Вона містить заходи, що спрямовані на запобігання несанкціонованому доступу, витоку даних, крадіжці інформації, а також виявлення та реагування на кібератаки. Кібербезпеку можна розглядати через різні аналітичні площини: технічну, організаційну та соціальну. Технічна сторона кібербезпеки фокусується на технологічних аспектах захисту систем, мереж і даних та охоплює використання різноманітних захисних технологій, таких як мережеві файли, антивірусне програмне забезпечення, системи виявлення вторгнень і шифрування даних. Організаційний аспект розглядається з погляду організаційних процесів і політики та бере участь у створенні політики безпеки, проведенні аудиту безпеки, навчанні персоналу та інсталяції процедур реагування на інциденти. А соціальна площина зосереджується на впливі людського фактора на кібербезпеку та охоплює питання свідомості безпеки та взаємодії між людьми та технологіями.

Основними цілями кібербезпеки є: запобігання несанкціонованому доступу до системи й даних; захист від шкідливих програм та злочинних атак; забезпечення конфіденційності, цілісності та доступності інформації; запобігання витоку конфіденційної інформації; забезпечення безпеки критичної інфраструктури та послуг тощо. Провал цих місій може призвести до серйозних наслідків: втрати конфіденційності, крадіжки інтелектуальної власності, фінансових втрат, порушення приватності користувачів та втрати репутації організацій.

Для побудови надійної системи захисту та зниження ризиків кібератак та інших загроз безпеки необхідне використання системної інженерії безпеки,

дотримання стандартів та найкращих практик. Інженерія безпеки є процесом проєктування та розроблення системи з урахуванням аспектів безпеки від початку до кінця. Вона охоплює визначення вимог безпеки, аналіз загроз, розроблення заходів захисту та оцінювання ризиків. Основною метою є забезпечення стійкості системи до кібератак та інших загроз. Для досягнення цієї мети важливо використовувати стандарти, що розроблені для забезпечення безпеки інформаційних систем. На сьогодні є міжнародні та національні стандарти [7, 8], що встановлюють вимоги та рекомендації щодо безпеки інформаційних систем, дотримання яких забезпечує відповідний рівень безпеки та ризикоорієнтований підхід до захисту від кібератак.

Де здійснюється захист інформації? Безпека виконується на різних рівнях: системи, інформаційної системи та інформаційної технології (рис.1). Безпека на рівні системи охоплює заходи, які застосовуються для захисту деяких комп'ютерних систем або мереж, включно з операційною системою, серверами, робочими станціями, мобільними пристроями тощо. Це передбачає розроблення та впровадження механізмів автентифікації, авторизації, шифрування даних, захисту від вторгнення та інших технічних заходів безпеки від кібератак.

Кібербезпека в інформаційних системах орієнтована на захист інформації, яка обробляється в рамках конкретних систем. Це можуть бути системи управління базами даних, електронні системи обробки та зберігання інформації, CRM-системи тощо. Кібербезпека в цьому контексті включає заходи для захисту конфіденційності, цілісності та доступності даних. Безпека на рівні інформаційних технологій охоплює ширший спектр технологій та інфраструктури, які використовують для обробки, передачі та зберігання даних. Це включає мережеву безпеку, захист даних у хмарних сервісах, використання криптографії, структуру мережі та інші аспекти, пов'язані з інформаційними технологіями. З огляду на це, безпека в кіберпросторі стає комплексним завданням, яке поєднує технічні заходи, політику, процедури, свідомість користувачів та поточний моніторинг потреби та вдосконалення.

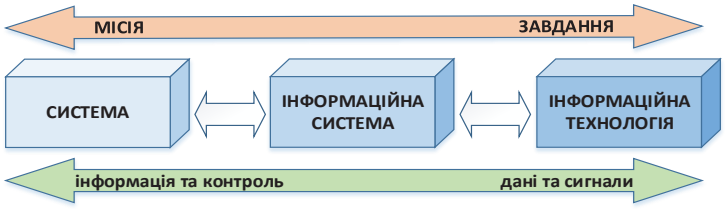

Рисунок 1. Рівні інформаційного захисту

Коли необхідно застосовувати заходи щодо кібербезпеки? Кібербезпека є необхідною в будь-яких ситуаціях, де є ризик від кібератак або порушення безпеки інформації. До кібербезпеки апелюють на різних етапах життєвого циклу системної інженерії. Уже на етапі розроблення архітектури системи необхідно виконати заходи кібербезпеки. Важливо застосувати поточні загрози та ризики, з якими може зіштовхнутися система, та включити в архітектуру відповідні механізми захисту. На етапі розроблення та впровадження системи необхідно використовувати найкращі практики кібербезпеки. Це включає перевірку безпеки програмного забезпечення, налагодження системи ввімкнення та захисту мережі, а також забезпечення безпеки під час міграції даних. Після впровадження системи в експлуатацію необхідно забезпечити постійний моніторинг та управління кібербезпекою. Це включає виявлення та відстеження поточних загроз, оновлення системи безпеки, проведення аудитів безпеки та навчання персоналу щодо заходів безпеки. Також, необхідно приділити увагу кібербезпеці в момент виходу система з експлуатації, що включає забезпечення безпечного видалення даних та забезпечення захисту інформації, яка може залишитися в системі після зняття її з експлуатації.

Загалом, кібербезпека має бути врахована на кожному етапі життєвого циклу системної інженерії для забезпечення захищеної та безпечної роботи системи.

Хто? На кого зорієнтована кібербезпека? На кібербезпеці зосередженні:

— IT-спеціалісти, які беруть участь у налагодженні та управлінні технічними аспектами безпеки, такими як мережева безпека, захист даних, керування доступом, виявлення вторгнень тощо. Вони також відповідають за встановлення та керування системами безпеки, виявлення та реагування на кібератаки та забезпечення безпеки програмного забезпечення;

— керівництво організації, яке займає важливу роль у визначенні стратегій та політики безпеки організації. Вони приймають рішення щодо розподілу ресурсів на заходи з кібербезпеки, забезпечення дотримання нормативних вимог, а також встановлення культури безпеки всередині організації;

— користувачі, які мають усвідомлювати наслідки загроз і використовувати безпечні практики, такі як складні паролі, актуалізацію програмного забезпечення, обережність під час роботи з електронною поштою та сумнівними вебсайтами;

— внутрішні аудитори, які оцінюють ефективність та відповідність системи організації безпеки встановленим стандартам та політикам. Вони виявляють слабкі місця та пропонують вдосконалення системи безпеки.

Чому виникають проблеми в кібербезпеці? Причини уразливості кібербезпеки можуть бути різними. З постійним розвитком технологій з'являються нові загрози та вразливості. Хакери та зловмисники постійно шукають нові способи атаки. Розширене використання хмарних сервісів, Інтернет-речей (IoT), мобільних пристроїв та інших нових технологій створює нові вектори атак та ризиків. Кіберзлочинці розробляють нові методи та інструменти для здійснення атак, використовуючи соціально-інженерні методи, фішинг, атаки з використанням шкідливих програм тощо. Це призводить до збільшення кількості та складності атак, що знижує ефективність кібербезпеки. До того ж багато людей не мають достатньої свідомості щодо загрози кібербезпеки та навичок безпечного використання технологій. Недостатнє навчання з кібербезпеки та несвідомої поведінки користувачів може створити вразливість у системах та полегшити успішні атаки.

Кіберзагрози постійно еволюціонують, швидко змінюються та адаптуються до нових технологій та захисних заходів, що створює виклики для організацій, які не досягають швидкої адаптації та впровадження нових заходів безпеки. Сучасні організації мають складні інформаційні системи та мережі, що ускладнює забезпечення безпеки. Багатофакторна аутентифікація, захист від DDoS-атак, захист від внутрішніх загроз та інші аспекти безпеки потребують складних інфраструктурних рішень та ресурсів. Деякі організації можуть бути обмежені в обсязі фінансування та ресурсів, які вони приділяють кібербезпеці. Це може призвести до недостатнього оновлення обладнання та програмного забезпечення, недостатньої підтримки та системи моніторингу безпеки, а також обмеженого доступу до фахівців із кібербезпеки. Врахування цих факторів і прийняття відповідних заходів безпеки є причиною мінімізації ризиків та забезпечення надійного кібербезпекового середовища.

Як забезпечити безпеку системи? Для виявлення потенційних небезпек та розроблення ефективних заходів безпеки для захисту систем від загроз можна застосувати методологію STPA-Sec, яка була розроблена для забезпечення системного підходу до аналізу безпеки систем. Теоретико-системний аналіз процесів для безпеки (Theoretic process analysis for security, STPA-Sec) – це методологія аналізу безпеки систем, яка розроблена Асоціацією системної безпеки (Systems Security Association, SSA). STPA-Sec базується на основній моделі Теоретико-системного аналізу процесів (System theoretic process

analysis, STPA), яка була розроблена професором Nancy Leveson [5]. Якщо модель STPA призначена для аналізу безпеки систем у широкому спектрі галузей, то STPA-Sec зосереджується на аналізі безпеки інформаційних систем, мереж та процесів.

Принцип роботи STPA-Sec базується на теорії систем, що дає змогу розглядати систему як комплекс елементів, що взаємодіють між собою (рис. 2). Процес STPA-Sec починається з визначення цілей та об'єктів аналізу. Спочатку визначається система, для якої проводиться аналіз безпеки. Це може бути конкретна інформаційна система, мережа, програмне забезпечення або процес, для яких потрібно провести аналіз безпеки. Аналізується взаємодія між компонентами системи, залучаючи їх структуру, функції та інформаційні потоки. Цей етап допомагає зрозуміти, як компоненти системи впливають на безпеку й можуть бути вразливими перед можливими загрозами. STPA-Sec використовує системний підхід для ідентифікації потенційних загроз безпеці та можливих точок вразливості. Надалі моделюється функціональна структура системи. Аналізується функціональна структура системи, її компоненти, процеси взаємодії та інформаційні потоки. Цей крок допомагає виявити потенційні шляхи атак та вразливості системи. Застосовуються методи системного аналізу, такі як аналіз функціональних потоків, діаграми подій та інші інструменти для визначення потенційних проблем безпеки та можливих наслідків подій. На основі виявлених небезпек та їх впливів розробляються контрольні заходи безпеки. Це можуть бути технічні, організаційні або процесні заходи, які мають на меті запобігти атакам, зменшити ризики та забезпечити безпеку системи. Застосовуються технології системної інженерії для проєктування та реалізації заходів, таких як політики безпеки, механізми контролю доступу, шифрування, моніторинг системи тощо.

На основі встановлених небезпек та контролю безпеки STPA-Sec проводить оцінку ризиків через визначені сценарії змін. Здійснюється оцінка ризиків, пов'язаних з ідентифікованими небезпеками, і приймаються рішення щодо впровадження контролю безпеки. Результати оцінки ризиків допомагають визначити пріоритети та вибрати найбільш ефективні заходи безпеки. STPA-Sec підтримує цикл постійного вдосконалення безпеки системи, що включає періодичну перевірку ефективності запроваджених заходів, виявлення нових загроз і ризиків, а також внесення змін у систему для забезпечення найвищого рівня безпеки.

STPA-Sec дає можливість розглядати систему як комплексний об'єкт із погляду безпеки. Вона поєднує системний аналіз, системну інженерію та

безпекові практики для ефективного виявлення та управління загрозами безпеці.

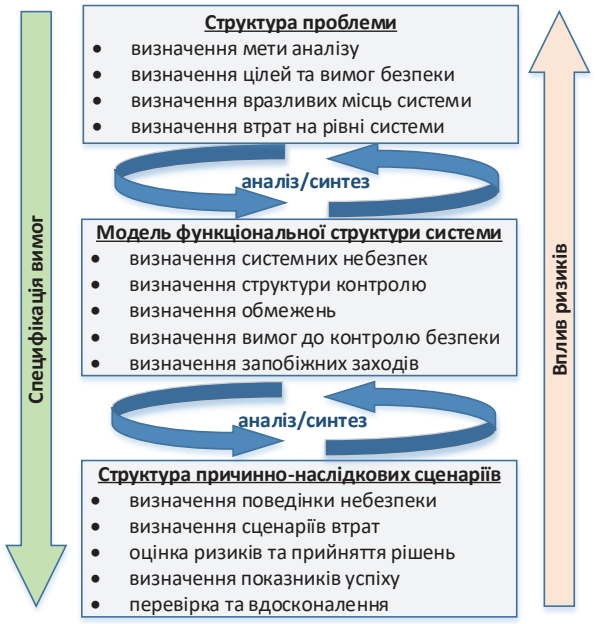

Рисунок 2. Узагальнена структура методу STPA-Sec

Висновок. Проведено аналіз кібербезпеки з допомогою методу 5W1H, який дає змогу повною мірою розглянути різні аспекти кібербезпеки – від визначення інформаційної безпеки й до опису причин, наслідків та шляхів впровадження заходів безпеки. Це дало можливість розкрити кібербезпеку як систему з інтерактивними компонентами та взаємозв'язками, окреслити її важливість та взаємовідносини з іншими формами організації безпечних систем. Описана системна методологія STPA-Sec, яка є потужним інструментом для оцінки кібербезпеки. Вона дає можливість ідентифікувати небезпеки систем, визначити причини виникнення проблем та розробити ефективні заходи безпеки. Застосування описаних методів у контексті кібербезпеки надає глибше розуміння проблеми безпеки, можливість виявляти слабкі місця та розробляти ефективні стратегії безпеки. Отже, використання системного аналізу для розуміння кібербезпеки є кроком у напрямку покращення безпеки в інформаційних системах та мережах. Такий підхід через ідентифікацію спричинених проблем, забезпечує ефективне управління ризиками та розробленні стратегій, що відповідають сучасним викликам безпеки у сфері кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Dingyu Yan (2020). A Systems Thinking for Cybersecurity Modeling ArXiv: 2001.05734v1. URL: https://arxiv.org/pdf/2001.05734.pdf
2. Drouot Bastien, Valery Monthe, Sylvain Guérin, Joël Champeau (2022). Security Analysis: From model to system analysis. Crisis2022: International Conference on Risks and Security of Internet and Systems, Sousse, Tunisia. URL: https://hal.science/hal-03866297
3. Igor Skiter, Hennadii Hulak, Viktor Grechaninov, Vitalii Klymenko, Nikolay Ievlev (2021). System Approach to the Creation of Cybersecurity Centers of Critical Infrastructure. CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, 2021, Kyiv, Ukraine. URL: https://ceur-ws.org/Vol-3187/short3.pdf
4. John W. Satzinger, Robert B. Jackson, and Stephen D. Burd. Systems Analysis and Design in a Changing World. Cengage Learning, 2015.
5. Young W, Leveson N. (2014). Inside risks-an integrated approach to safety and security based on system theory: Applying a more powerful new safety methodology to security risks. Communications of the ACM 57(2):232–242. http://dx.doi.org/10.1145/2556938
6. Zachary A. Collier, Igor Linkov, James H. Lambert, (2013). Four domains of cybersecurity: a risk-based systems approach to cyber decisions, Environment Systems and Decisions, Springer, vol. 33(4). P. 469-470. URL: https://doi.org/10.1007/s10669-013-9484-z
7. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT)
8. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).
9. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017, № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

REFERENCES

1. Dingyu Yan (2020). A Systems Thinking for Cybersecurity Modeling ArXiv: 2001.05734v1. URL: https://arxiv.org/pdf/2001.05734.pdf (in English)
2. Drouot Bastien, Valery Monthe, Sylvain Guérin, Joël Champeau (2022). Security Analysis: From model to system analysis. Crisis2022: International Conference on Risks and Security of Internet and Systems, Sousse, Tunisia. URL: https://hal.science/hal-03866297 (in English)

3. Igor Skiter, Hennadii Hulak, Viktor Grechaninov, Vitalii Klymenko, Nikolay Ievlev (2021). System Approach to the Creation of Cybersecurity Centers of Critical Infrastructure. CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, 2021, Kyiv, Ukraine. URL: https://ceur-ws.org/Vol-3187/short3.pdf (in English)
4. John W. Satzinger, Robert B. Jackson, and Stephen D. Burd. Systems Analysis and Design in a Changing World. Cengage Learning, 2015. (in English)
5. Young W, Leveson N. (2014). Inside risks-an integrated approach to safety and security based on system theory: Applying a more powerful new safety methodology to security risks. Communications of the ACM 57(2):232–242. http://dx.doi.org/10.1145/2556938 (in English)
6. Zachary A. Collier, Igor Linkov, James H. Lambert, (2013). Four domains of cybersecurity: a risk-based systems approach to cyber decisions, Environment Systems and Decisions, Springer, vol. 33(4). P. 469-470. URL: https://doi.org/10.1007/s10669-013-9484-z (in English)
7. DSTU ISO/IEC 27001:2015 Informatsiini tekhnolohii. Metody zakhystu cystemy upravlinnia informatsiinoiu bezpekoiu. Vymohy (ISO/IEC 27001:2013; Cor 1:2014, IDT) (in Ukrainian).
8. DSTU ISO/IEC 27002:2015 Informatsiini tekhnolohii. Metody zakhystu. Zvid praktyk shchodo zakhodiv informatsiinoi bezpeky (ISO/IEC 27002:2013; Cor 1:2014, IDT) (in Ukrainian).
9. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy. Zakon Ukrainy vid 05.10.2017, № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (in Ukrainian).

DOI 10.32403/2411-9210-2023-1-49-197-208

CYBERSECURITY THROUGH THE PRISM OF SYSTEMS ANALYSIS

U. Panovyk[1], R. Tkachuk[2]
[1]*Ukrainian Academy of Printing,*
19, Pid Holoskom St., Lviv, 79020, Ukraine
Lviv State University of Life Safety,
35, Kleparivska St., Lviv, 79007, Ukraine

ulianapanovuk@gmail.com

The concept of cybersecurity is becoming extremely important in today's digital world. Cybersecurity covers a wide range of measures to protect information systems, computer networks, and data from unauthorized access, destruction, theft, or damage. Security analysis is a critical step in security design that allows one to identify system vulnerabilities and establish security requirements early in the design

process. The increasing complexity of modern systems requires a new approach to security analysis. Traditional methods do not provide sufficient power to detect dangerous incidents that are reflected in the interaction between physical systems, people, and social objects. The article establishes that the use of system analysis makes it possible to trace cybersecurity as a complex system with interacting components to identify, analyze and manage risks related to information security. Methods and approaches of system analysis that can be used to identify potential threats assess risks, develop a strategy for threats to systems, and ways to eliminate them are considered. Systems analysis methods are used, such as the 5W1H method and the STPA-Sec methodology, to summarize and explain complex aspects of cybersecurity. Thanks to the 5W1H questions, the technique allows one to solve all aspects of cybersecurity. It also collects comprehensive information about the system, its components, threats and vulnerabilities, and processes and procedures affecting security. The STPA-Sec system methodology is a powerful tool for identifying security threats and points of vulnerability through the analysis of the interaction of system components, functional structure, and information flows. Based on the results of the analysis, security control measures are developed to prevent attacks and ensure system security. The application of STPA-Sec provides a comprehensive approach to the security system and reduces the risks of its violation. The research presented in this article highlights the importance of a systems approach to cybersecurity analysis and shows that using systems analysis techniques can help identify threats and address security issues. This makes it possible to increase the effectiveness of the strategy and management of cybersecurity threats.

Keywords: cybersecurity, system approach, synthesis and analysis, methods of system analysis, 5W1H method, STPA-Sec methodology.

Стаття надійшла до редакції 06.03.2023.
Received 06.03.2023.