DOI 10.20535/2411-1031.2021.9.2.249889
УДК [(004.056.53::550.34.013.4)+355.405.1](477)

ЮЛІЯ КОЖЕДУБ,
СЕРГІЙ ВАСИЛЕНКО,
АНДРІЙ МАКСИМЕЦЬ,
ВІРА ГИРДА

КОНЦЕПТУАЛЬНА МОДЕЛЬ ЗАХИСТУ ІНФОРМАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Досліджено проблему вибору моделі захисту інформації на об'єктах критичної інформаційної інфраструктури України. Проведено аналіз сучасних моделей захисту комп'ютерних систем і мереж, що є основою об'єктів критичної інформаційної інфраструктури. Показано, що ці моделі враховують специфічні особливості їх функціонування. Вони уможливлюють оцінювання різних сценаріїв розвитку подій інформаційної безпеки, аналізування стану роботи комп'ютерних систем і мереж. Представлені моделі захисту використовуються протягом розробки архітектури системи захисту об'єктів критичної інформаційної інфраструктури. Особливу увагу приділено питанням, що пов'язані з особливостями виникнення загроз інформаційної безпеки та показано шляхи їх формування. Такий аналіз доцільний для вибору заходів захисту інформації, що циркулює в комп'ютерних системах і мережах об'єктів критичної інформаційної інфраструктури. Крім того, причини та умови формування загроз інформаційної безпеки є важливими як джерело цінної інформації для встановлення основного і додаткового набору заходів захисту інформації. Вони обираються у межах моделей захисту інформації об'єктів критичної інформаційної інфраструктури. Основою для їх упровадження є матриця оцінювання стану інформаційної безпеки, складена зі залученням експертів. Зважаючи на це, визначено складові моделі захисту інформації об'єктів критичної інформаційної інфраструктури. Вона складається з трьох складників: загроз інформаційної безпеки, елементів інформаційної інфраструктури, основних і додаткових заходів захисту. За допомогою складеної матриці формалізовано взаємозв'язок складових моделі. Серед елементів виокремлено ймовірності реалізування загроз безпеці елементів інформаційної інфраструктури. Для їх визанчення використано експертний метод. Сформульовано сукупності умов впливу (зовнішніх і внутрішніх) чинників, станів (робочого і аварійного) функціонування, складу елементів об'єктів критичної інформаційної інфраструктури. На основі цього формується лінгвістичний опис вимог для створення моделі захисту інформації, що обробляється у них.

Ключові слова: модель захисту інформації, об'єкт критичної інформаційної інфраструктури, загроза інформаційної безпеки, заходи захисту, матриця оцінювання стану інформаційної безпеки.

Постановка проблеми. Кіберпростір нині стає новим полем протистояння. І напади на об'єкти, які забезпечують життєдіяльність як окремих організацій, населених пунктів, так і цілих держав, можуть бути руйнівними. Утім, руйнація або аварії на таких об'єктах також можуть становити дуже серйозні загрози для здоров'я і навіть життя людей, які мешкають на відповідних територіях. Тим більше, коли це організації таких галузей як енергетика, хімічна промисловість, транспорт, банківського та фінансового сектору, інформаційні технології та телекомунікації, охорони здоров'я, комунального господарства, які є стратегічно важливими для функціонування економіки і безпеки людини, суспільства, держави – усі ті об'єкти, які відносять до критичної інфраструктури [1].

Найважливішою характеристикою об'єктів критичної інформаційної інфраструктури (ОКІІ) є їх ключове значення для безпеки суспільства і держави (рис. 1). До них можуть належати як військові, так і цивільні [2].

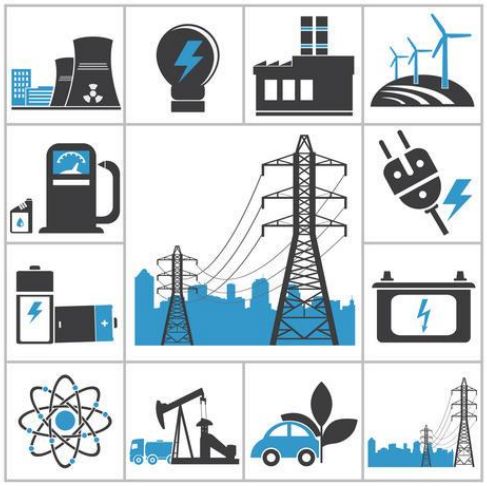

Рисунок 1 – Об’єкти критичної інфраструктури [3]

Окрім національних, виокремлюють і міжнародні ОКІІ, серед яких є такі: система доменних імен глобальної мережі Інтернет, комунікаційні супутники, міжконтинентальні кабелі і маршрутизатори [3], [4].

Перехід від традиційної технології циркуляції інформації до інформаційних форматів в організації відбувається стрімко. За умов формування “цифрової економіки” спостерігається зростаюче поширення мережевих, інформаційних інфраструктур, оскільки вони більш економічні, ефективні, ергономічні [5]. Складність і взаємозалежність інформаційних систем веде до того, що наслідки порушення їх нормальної роботи можуть бути непередбачуваними і в найгіршому випадку спричинити “ефект доміно” для економіки однієї країни або ж цілого континенту. Інформаційні інфраструктури більш вразливі порівняно із традиційними, саме вплив на них є найбільш небезпечним для людини, суспільства, держави та може спровокувати заворушення, нестабільність, масові хвилювання серед населення [6]. Сучасні системи включають в себе елементи традиційної фізичної інфраструктури, робота яких забезпечується програмним забезпеченням. Роботу віртуальних елементів таких як програмне забезпечення, в більшості випадків скадно порушити за допомогою фізичних впливів, проте на їх функціонування можна вплинути за допомогою, наприклад [7], шкідливого програмного забезпечення.

Узагальнення та систематизація досліджень щодо захисту інформації критичної інфраструктури дає змогу констатувати необхідність приділяння особливої уваги не лише оцінюванню впливу на життєво важливі об’єкти, а й можливих наслідків цих впливів для політичної, економічної, екологічної та інших сфер діяльності країни [8].

Аналіз останніх досліджень і публікацій. У [9] використовується модель дерева атак та моделювання загроз як основа представлення систем захисту. У процесі моделювання отримано елементи загрози та шляхи атаки, а також запропоновано необхідні вимоги та технологію для засобів контролю безпеки, щоб реагувати на ці загрози. У [10] використано модель прийняття рішень щодо інвестиційного забезпечення інформаційної безпеки в умовах неповної інформації шляхом зміни моделі Гордона і Льоба, та порівняння відмінностей між рівнями інвестицій. У [11] показано та розроблено нову модель процесу, яка пояснює як модель урядової інформаційної безпеки (англ. Information Security Governance, ISG) можна застосовувати у фінансових організаціях. Її вдосконалено, використовуючи пілотний приклад, а також зроблено висновки щодо застосовності у подальшій роботі.

Відповідно до [12] інформація про ОКІІ безпосередньо і опосередковано отримується, перевіряється, обробляється, зберігається, маркується та використовується процедурно в системі наглядового контролю і збору даних (НКІЗД, англ. Supervisory Control and Data Acquisition, SCADA). Системи НКІЗД не обов’язково є державними (федеральними) інформаційними

системами. Історично вони були окремими структурними елементами, не підключеними до Інтернету, що забезпечували управління та контроль за ОКІІ. Системи НКІЗД наразі під'єднані до Інтернету, а тому стають більш уразливими до реалізації загроз. Застосовна до них концепція "безпека незрозумілості" або "безпека через неясність" ("Security by obscurity" або "Security through obscurity") вже не є результативним варіантом захисту ОКІІ.

Безпека через неясність (англ. Security through obscurity) – принцип, який використовується для забезпечення безпеки в різних сферах діяльності людини [13]. Основна ідея полягає в тому, щоб приховати внутрішню структуру системи чи її принцип функціонування. Розробники систем захисту вважають, що якщо недоліки невідомі, то зловмисник не зможе їх виявити. Можна використовувати безпеку через неясність як один з рівнів захисту системи, оскільки дає час усунути знайдену уразливість, тоді як публічне розкриття продуктів і версій робить їх основною метою для застосування виявлених уразливостей. Першим кроком зловмисника зазвичай є збір інформації – це завдання ускладнюється при використанні принципу забезпечення безпеки через неясність.

Існує загальний консенсус, навіть серед тих спеціалістів, хто бере участь у розробці систем захисту через незрозумілість, що принцип "безпека через незрозумілість" ніколи не повинен використовуватись як основний захід захисту. Це, у кращому випадку, другорядний і, зрозуміло, що розкриття інформації про безпеку через невідомість не має призводити до компрометації. Національний інститут стандартів і технологій США (англ. National Institute of Standards and Technology, NIST) рекомендує використовувати безпеку через незрозумілість, не більш ніж в одному документі: "система безпеки не повинна залежати від прихованості реалізації або її компонентів" [13].

До того ж безпека через неясність суперечить принципу "KISS" (англ. акронім зі слів "Keep it simple, stupid", "Роби простіше!"). Принцип проєктування, розроблений у Військово-морських силах США в 1960 р., формулює, що більшість систем працюють найкраще, якщо вони є простими, а не ускладнюються. Тому під час проєктування простота повинна бути однією з ключових цілей, і, відповідно, слід уникати непотрібної складності [14], [15].

Метою статті є розроблення концептуальної моделі захисту інформації ОКІІ, що відображатиме загрози інформаційної безпеки, елементи інформаційної системи та заходи захисту через матрицю оцінювання стану інформаційної безпеки для ОКІІ.

Виклад основного матеріалу досліджень. Сучасний світ значною мірою залежить від засобів автоматизації виробничих процесів, серед іншого це й об'єкти інформаційної діяльності, інформація в яких потребує захисту, наприклад, – автоматизовані системи управління технологічними процесам. Атомні й гідроелектростанції, нафто- і газопроводи, мережі розподілу електроенергії, транспортні системи національного і світового рівня, які належать до ОКІІ, функціонують на базі таких автоматизованих систем і від захищеності систем управління цими системами залежить безпека держави [7].

Очевидно, що в умовах сучасного надзвичайно інтенсивного розвитку інфраструктури є безліч критично важливих об'єктів, таких, наприклад, як великі гідротехнічні споруди, нафто- і газопроводи, мережі атомних і теплових електростанцій, теплоенергоцентралей, пункти зберігання стратегічних запасів нафти і газу, шкідливі хімічні виробництва, транспортні вузли, аеродроми, виведення з ладу яких може призвести до непередбачуваних важких і навіть катастрофічних наслідків: оцінювались варіанти техногенних катастроф або руйнівних стихійних лих. У перелік виявлених критично важливих об'єктів не увійшли традиційні типи військових об'єктів, оскільки, за оцінками дослідників, ці об'єкти мають досить високий ступінь захищеності й практично є малоуразливими до впливу звичайних засобів ураження [7].

Значний обсяг оброблюваної інформації на стратегічних об'єктах країни, її важливість, і як наслідок, наявність привабливості для проведення атак, кожен інформаційний потік, діяльність кожного інформаційного вузла, автоматизованої системи, кожного співробітника такого об'єкта і загалом організації, діяльність і в цілому функціональність її роботи є метою для здійснення загроз інформаційній безпеці [7].

Об'єднання інформаційних потоків та інформаційної технології утворює цілісну інформаційну систему ОКІІ. В процесі своєї діяльності, з урахуванням її специфіки та розвитку технологій, для ОКІІ розробляють власні автоматизовані інформаційні системи, які обробляють інформаційні потоки. Слід зазначити, що особливість таких систем полягає в орієнтації не на масивні розрахунки, а на обсяг і важливість інформації. Втрата, модифікація та/чи розголошення такої інформації, матиме, в окремих випадках, катастрофічний характер для функціонування ОКІІ. В основі створення моделей захисту для таких об'єктів важливими характеристиками є зберігання і доступ до даних [8].

Створюючи технічні об'єкти потрібно вирішити дві основні проблеми [8]:

– забезпечити функціонування об'єктів відповідно до призначення;

– забезпечити ефективне функціонування, що визначається надійністю і безпекою як об'єкта в цілому, так і його компонентів.

Кожна з проблем стосується завдань, що їх відносять до різних наукових галузей та дисциплін, за якими потрібно приймати рішення. Щоб прийняти правильне рішення, необхідно сформувати альтернативи, з яких, відповідно до прийнятих критеріїв, вибрати раціональну. За цього, такі критерії прийняття рішень має бути узгоджено на всіх етапах і стадіях створення технічного об'єкта, наприклад, від обґрунтування вибору матеріалу для кожного важливого елемента до обґрунтування властивостей надійності і безпеки об'єкта в цілому (рис. 2).

Рисунок 2 – Етапи і методи збору даних при виборі моделей захисту

Дослідження на різних рівнях структури складної системи і на різних етапах її створення та застосування повинні мати відповідну методологічну основу. Це дає змогу активно використовувати на кожному етапі життєвого циклу моделі системи позитивні результати, що одержуються при дослідженні та забезпеченні її надійності і безпеки.

Один із рівнів побудови архітектури моделі системи – концептуальний, який передбачає розробку концептуальної моделі (або моделі предметної області) цієї системи. Компонентами такої моделі є об'єкти та їх взаємозв'язки. Концептуальна модель (КМ) забезпечує

представлення даних через вираження, організацію, упорядкування й обмін. За допомогою КМ даних показують об'єкти предметної області та взаємозв'язки між ними. Щоб забезпечити адекватне виконання процесу моделювання, потрібно наперед продумати складові рівнів забезпечення (рис. 3) [16]:

1. Апаратного – засоби обчислювальної техніки – сервера, робочі станції, обладнання локальних обчислювальних мереж, засоби телекомунікації і зв'язку.
2. Програмного – системне (операційні системи, системи управління базами даних, сервісні програми) і прикладне (програмні модулі, автоматизовані робочі місця, офісні системи); математичне: предметне (алгоритми, методи перетворення інформації, моделі, що відображають процеси, методи вирішення задач) і прикладне (алгоритми, методи, моделі автоматизованої системи).
3. Інформаційного – внутрішньо-машинного (сукупність даних на машинних носіях у вигляді спеціально організованих масивів, файлів, баз даних, банків даних, їх інформаційні зв'язки) і позамашинне (сукупність інформації: системи показників, методи класифікації і кодування елементів інформації, документів, документообігу інформаційних потоків).
4. Функціонального – сукупність операцій, функцій, завдань, визначених предметною спрямованістю діяльності автоматизованої системи.
5. Технологічного – сукупність проєктних рішень, що визначають технологію обробки, створення технологічних умов для виконання процесів в автоматичному режимі, набір технологічних інструкцій і рекомендацій, що їх деталізують; також технологічне забезпечення об'єднує інформаційне і функціональне забезпечення в загальну технологію роботи.

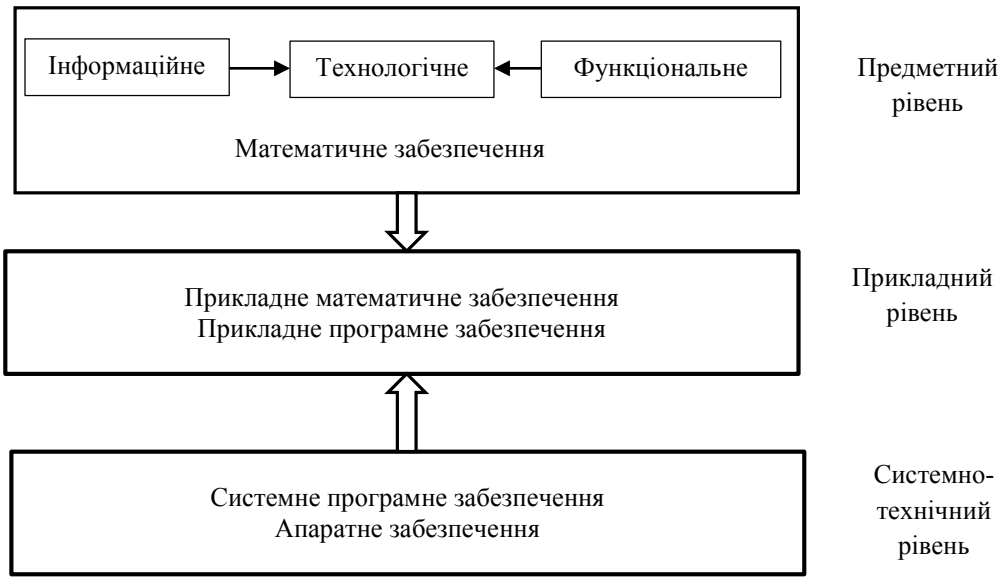

Рисунок 3 – Взаємодія рівнів забезпечення інформаційної інфраструктури

Для моделі "Процес розслідування" (рис. 4) характерним є високий рівень абстракції, а сферою застосовності – будь-який дослідницький процес [17]. Знання формується запитаннями. Ці запитання основані на спостереженнях про об'єкти досліджуваного процесу (їх взаємодію та/чи функціонування). Запитання треба поставити так, щоб можна було його перевірити. Гіпотеза складається з припущення і причини виникнення запитання. Відповідь – це зібрані докази, які підтверджують або спростовують гіпотезу. Зрозуміло, що спростування гіпотези прискорює дослідницький процес. Звісно, що відповіді можуть породжувати інші запитання, якщо досліджують складний і динамічний процес. Висновки дають змогу описати подію, що відбулась. За допомогою цієї моделі можна вирішити такі завдання в сфері захисту інформації: пошук фактів компрометації; навчання аналітиків SOC (англ. Security Operations Center, SOC; укр. Центр забезпечення безпеки). SOC – це команда, що складається в

основному з аналітиків безпеки, в завдання якої входить виявлення та аналіз інцидентів кібербезпеки, оперативне реагування, запобігання їх виникненню і складання звітності) [17].

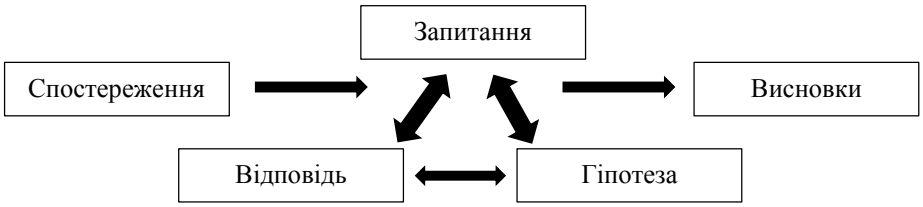

Рисунок 4 – Модель “Процес розслідування”

Усі моделі з високим рівнем абстракції здаються простими, але саме для таких моделей є деталі, що підвищують ефективність їх застосування [17]. Зокрема, це наявність причини ініціалізації процесу дослідження, вербалізація гіпотези, формалізація висновків.

Для наступної моделі “Алмаз” так само властивий високий рівень абстракції. Сферою застосування її є будь-який дослідницький процес в рамках роботи з подіями й інцидентами інформаційної безпеки та кібератаками (рис. 5).

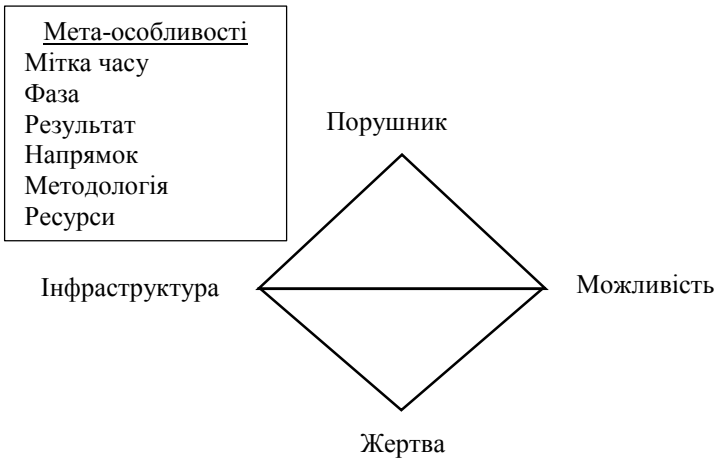

Рисунок 5 – Модель “Алмаз”

Основні положення і принципи моделі “Алмаз” [17]: кожну подію створює порушник (це може бути і група людей, наприклад виконавець і замовник), який виконує дії для вирішення свого завдання, порушник завжди уособлює TTP (англ. Tactic, Technique, Procedure; укр. Тактики, Техніки, Процедури). Він використовує можливості, властиві елементам інфраструктури, проти жертви і слугують для досягнення порушником своєї мети.

Будь-яка система, а значить і будь-який інформаційний актив, має уразливості. Кожна шкідлива активність складається з фаз, успішне проходження яких призводить до успіху активності в цілому. Кожна подія інформаційної безпеки потребує виконання однієї чи більше умов для того, щоб бути “успішною”. Такі можливості характеризуються якістю і кількістю. Завжди є взаємозв’язок між порушником і жертвою, навіть якщо він опосередкований чи неявний, наприклад, жертву (а це може бути як матеріальний актив, так і людина) вибирають з поміж інших, яка є більш “сприятливою”. Зловмисну активність може бути спрямовано на одну жертву чи на декількох, або охоплювати навіть подолання захисних заходів).

Для наступної моделі “MITRE ATT&CK” (англ. Adversarial Tactics, Techniques and Common Knowledge; укр. Тактики, Техніки та Загальновідомі Факти про порушників) рівень абстракції середній, а сферою застосування є інформаційна безпека комп’ютерних мереж. Для функціонування цієї моделі є вимога: в організації повинні бути розгорнуті сенсори на кінцевих пристроях, що забезпечують постійний моніторинг стану інформаційної безпеки [17].

Основні положення цієї моделі [17]: будується з точки зору атакуючого, базується на реальних інцидентах (відкритих звітах). Захисні дії співвіднесені з атакувальними за законом Парето, що дає змогу перейти від реактивних дій до проактивних, – перекривши короткострокові цілі порушників, створюється можливість глибшого захисту, вибирають і застосовують певний набір тактик і технік (рис. 6).

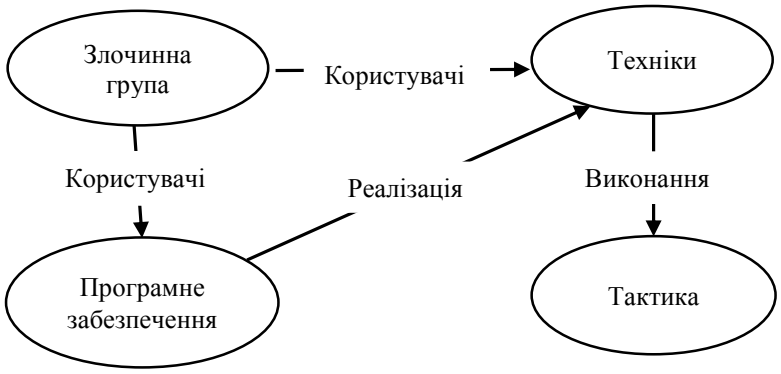

Рисунок 6 – Модель “MITRE ATT&CK”

Модель захисту ОКІІ повинна визначати: ймовірність ліквідації (усунення, запобігання) загрози інформаційної безпеки конкретного типу конкретному елементу системи захисту ОКІІ залежно від застосовуваних засобів захисту інформації; ступінь впливу кожного елемента інформаційної структури на загальну інформаційну безпеку ОКІІ. Модель повинна показати сукупність взаємопов’язаних моделей, що описують загрози інформаційної безпеки як сукупність властивостей (інформаційних (ідентифікаційних) ознак) зовнішніх і внутрішніх чинників, умов та подій з елементами системи захисту та елементами інформаційної структури (рис. 7) [7]. Важливо розрізняти: заходи, стани, етапи і процеси, що задіяні в життєвому циклі інформації (наприклад, збирання, аналіз, накопичення, зберігання, захист).

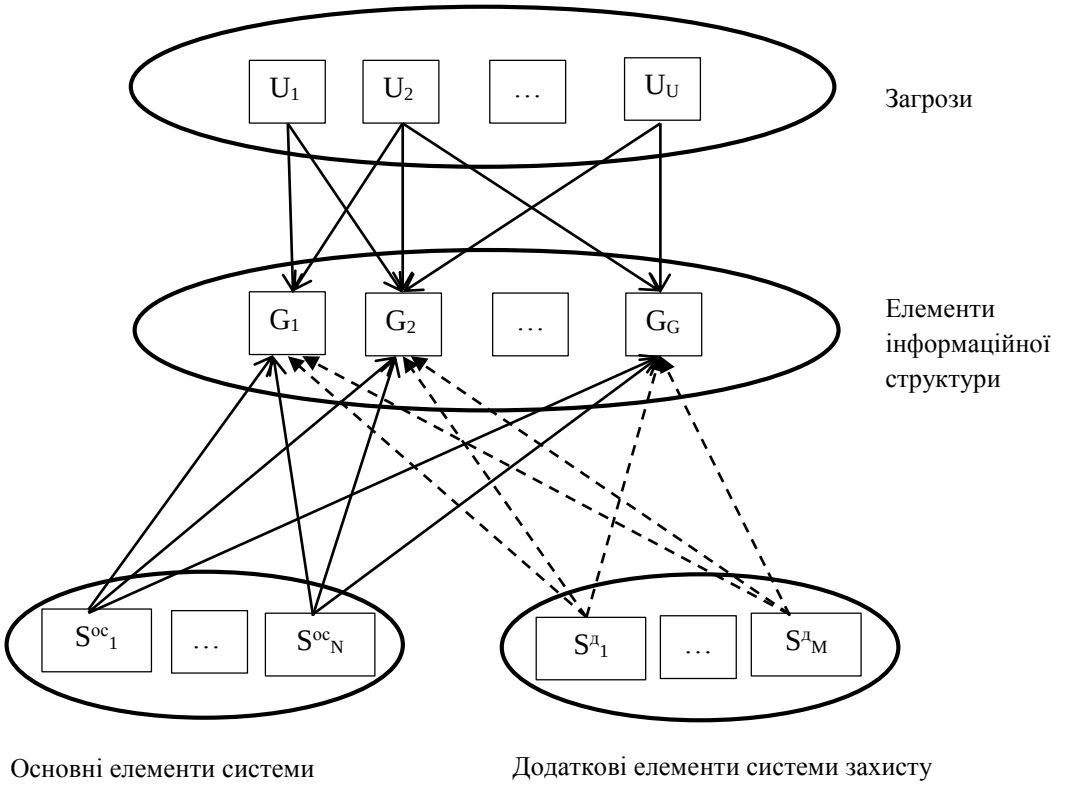

Рисунок 7 – Модель структури системи захисту

Механізм моделювання процесу формування загроз ускладнено причинно-наслідковими і суб'єктивно-об'єктивними причинами. Структуру загрози будь-якого походження та її життєвий цикл на показано на рис. 8, 9 [7].

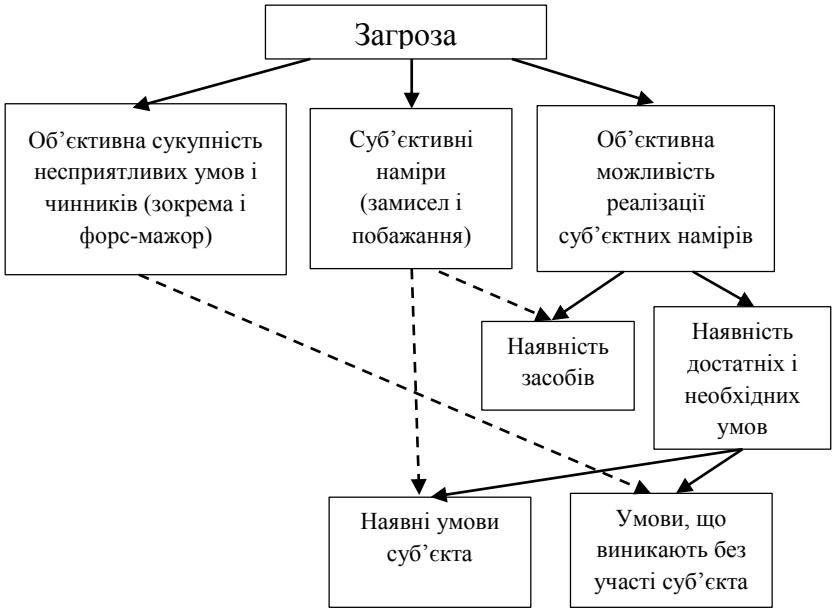

Рисунок 8 – Структура моделювання процесу формування загроз

Найважливішим етапом в організації захисту інформації при виникаючих загрозах інформаційної безпеки є визначення складу основних і додаткових засобів захисту (рис. 10). Основні засоби захисту інформації – це мінімальний набір, що забезпечує заданий політикою інформаційної безпеки рівень інформаційної безпеки організації [7], [18], [19]. Під додатковим розуміють певну частину з комплекту засобів захисту інформації організації, що не включено в основну частину. Основний або базовий комплект може бути визначено послідовним вирішення завдання оптимального вибору з широкого діапазону при покроковому скороченні засобів захисту інформації. Крок скорочення – одна одиниця засобу конкретного типу.

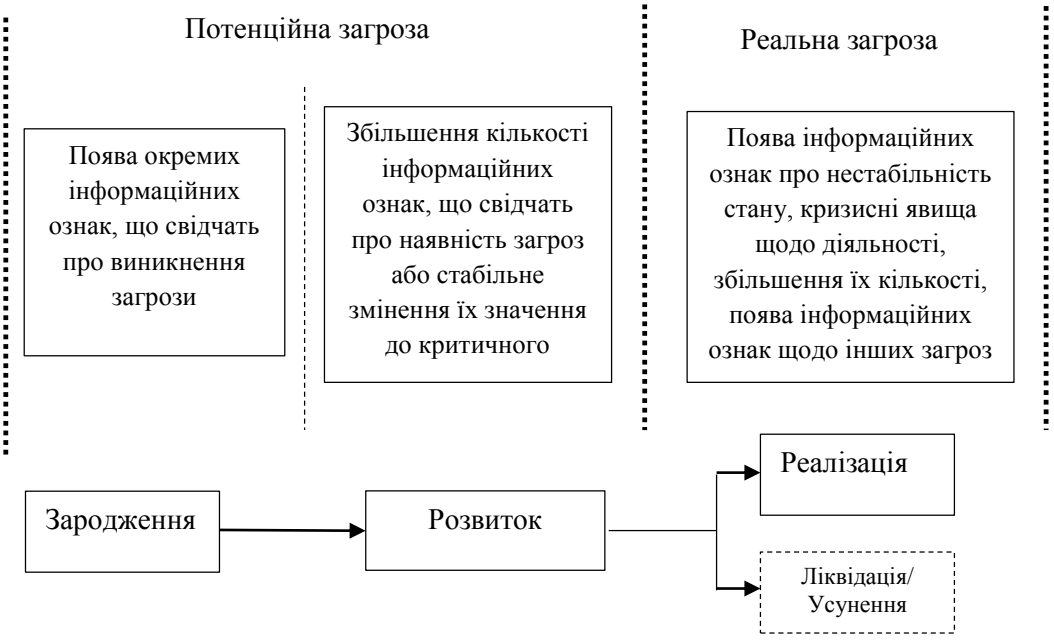

Рисунок 9 – Життєвий цикл загрози

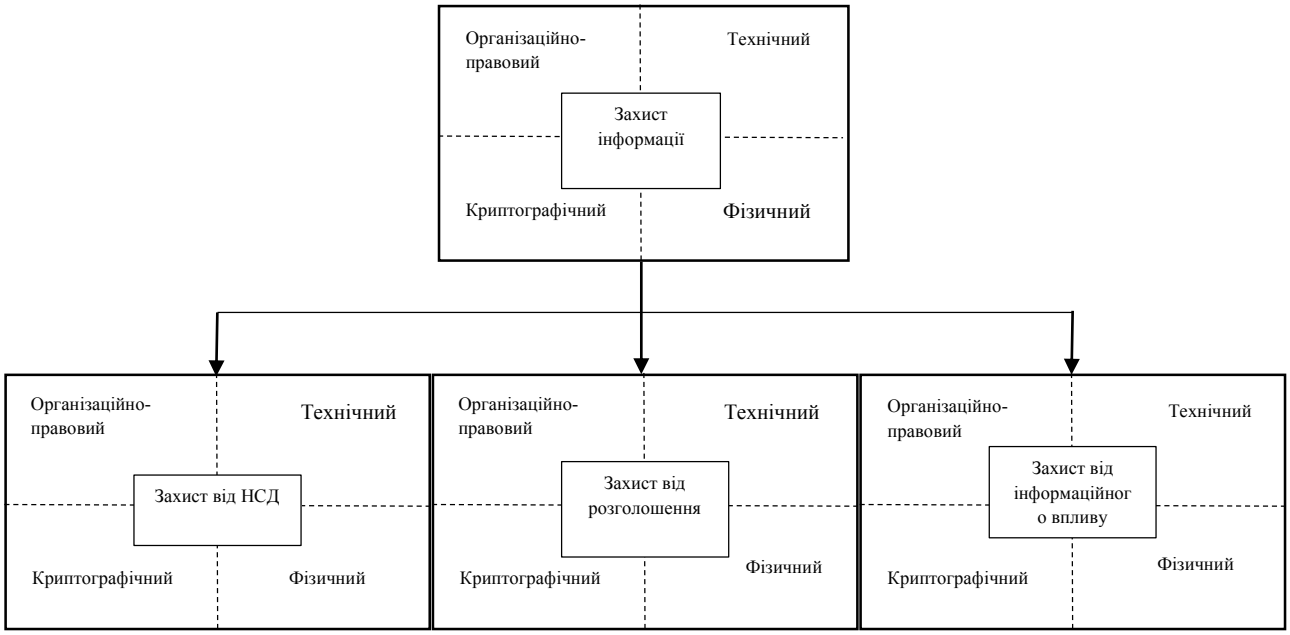

Рисунок 10 – Модель організування захисту інформації в організації (НСД – несанкціонований доступ) [18], [19]

Модель захисту інформації (табл. 1) – матриця $\|P(U_U/S_S)\|$, елементами якої є умовні ймовірності усунення загрози інформаційної безпеки U_U при застосуванні засобів захисту S_S Ці ймовірності визначаються проведенням експертного опитування.

Таблиця 1 – Представлення моделі захисту інформації

Засоби захисту інформації / Загрози інформаційної безпеки	S_1	S_2	…	S_i	…	S_s
U_1			…		…	
U_2			…		…	
…	…	…	…	…	…	…
U_i			…	$P(U_i / S_i)$	…	
…	…	…	…	…	…	…
U_U			…		…	

При застосуванні до елементів інформаційної інфраструктури декількох елементів захисту інформації $S_1, S_2, .., S_S$ ймовірність захисту від загрози U_U буде визначатись виразом

$$P\left(\frac{U_U}{S_S}\right) = 1 - \prod_{k=1}^{n,m}\left(1 - P\left(\frac{U_U}{S_K}\right)\right),$$

де $S_S = S_N^{OC} + S_M^{Д}$;

$(S_1^{OC}, S_2^{OC}, .., S_N^{OC})$ – основні засоби захисту інформації;

$(S_1^{Д}, S_2^{Д}, .., S_M^{Д})$ – додаткові засоби захисту інформації;

$(U_1, U_2, .., U_U)$ – загрози інформаційної безпеки.

Інтенсивність виникнення загроз інформаційної безпеки не може бути сталою величиною (рис. 11). Ось тому, модель захисту інформації орієнтована, перед усім, на ліквідацію/усунення та/чи зменшення ризиків, як вже виявлених, так і легко прогнозованих. Така система має бути спрямована на постійно оновлюваний набір і заздалегідь відомі сценарії їх реалізації.

Рисунок 11 – Взаємозв'язок між інтенсивністю потоку загроз інформаціиної безпеки та набором засобів захисту інформації

Висновки. Захист інформації, що циркулює в інформаційних системах і мережах ОКІІ, одна з найважливіших проблем сучасності. Окрім стандартизованих підходів до розроблення моделей захисту потрібно проєктувати і нетипові новітні моделі, що враховуватимуть нескінченну множину чинників, серед яких управління ризиками, прогнозування, когнітивний підхід до захисту інформації. Усі ці чинники має бути спрямовано на безперервне удосконалення процесів управління ОКІІ.

Описано традиційні структури концептуальних моделей, що можуть застосовуватись для сфери захисту інформації. Показано вибір компонентів для побудови моделі захисту. З'ясовано особливості застосування таких моделей. Встановлено, що їх можливості може бути розширено інтеграцією таких моделей. Зважаючи на перспективність даного напряму, потрібно провести подальші дослідження, зокрема, для перевірки та уточнення розробленої моделі, щоб досягнути узагальнення результатів.

Розгляд, дослідження та систематичний підхід до безпеки, заснований на застосуванні моделей різного ступеня формалізації, дозволяє розробникам таких моделей уникнути допущення помилок. Їм потрібно знати необхідні для успішної побудови системи захисту умови і чинники. До того ж, щоб досягнути мети дослідження, за допомогою абстрагування, відкинути зайві характеристики і параметри, які лише заважають бачити цілісну картину події інформаційної безпеки та прогнозувати стан інформаційної безпеки організації. Однак, при цьому важливо пам'ятати, що моделі потрібно на періодичній основі переглядати, щоб максимально наблизитися до розв'язання завдання у межах реального об'єкта дослідження. Водночас врахувати змінність завдань, обмежень, припущень з часом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] КПІ та ще два київських виші долучилися до проєкту USAID у галузі кібербезпеки. [Електронний ресурс]. Доступно: https://kpi.ua/2021-05-21. Дата звернення: Верес. 4, 2021.

[2] A. Wenger, V. Mauer and M. Cavelty, *International critical information infrastructure protection handbook 2008–2009*, Eds. Center for Security Studies, ETH Zurich, 2009.

[3] *National Institute of Standards and Technology*. (2018, Apr. 16). Framework for Improving Critical Infrastructure Cybersecurity. Ver. 1.1. [Online]. Available: https://doi.org/10.6028/NIST.CSWP.04162018. Accessed on: Sept. 4, 2021.

[4] *Стратегія національної безпеки України в контексті досвіду світової спільноти*. Зб. ст. за матер. міжн. конф. Київ: САТСАНГА, 2001.
[5] О. Довгань, "Критична інфраструктура як об'єкт захисту від кібернетичних атак", на *наук.-практ. конф. Інформаційна безпека: виклики і загрози сучасності,* Київ, 2013, с. 17-20.
[6] С. Гончар, Г. Леоненко, та О. Юдін, "Теоретико-методологічний аспект забезпечення інформаційної безпеки об'єктів критичної інфраструктури", *Вісник Національного університету "Львівська політехніка". Комп'ютерні системи та мережі,* № 806, 2014, с. 34-39.
[7] Е. Галкова, "Динамическая модель защиты информации при попытке рейдерского захвата кредитно-финансового учреждения", дис. канд. наук, СПб. нац. досл. ун-т інформ. техн. механіки і оптики, 2014.
[8] Д. Королев, и М. Королев, *Информационные системы в банковском деле*. Белгород: Изд-тво БелГУ, 2004.
[9] J.-S. Chang, Y.-H. Jeon, and S. Sim, "Information Security Modeling for the Operation of a Novel Highly Trusted Network in a Virtualization Environment". [Online]. Available: https://doi.org/10.1155/2015/359170. Accessed on: Sept. 4, 2021.
[10] Y. Lee, "Information Security Investment Model and Level in Incomplete Information", [Online]. Available: https://doi.org/10.13089/JKIISC.2017.27.4.855. Accessed on: Sept. 4, 2021.
[11] C. K. Wong, S. B. Maynard, A. Ahmad, and H. Naseer, "Information Security Governance: A Process Model and Pilot Case Study". [Online]. Available: https://aisel.aisnet.org/icis2020/cyber_security_privacy/cyber_security_privacy/3/. Accessed on: Sept. 4, 2021.
[12] Department of Homeland Security. (2002, Nov. 25). *The Critical Infrastructure Information Act of 2002*. [Online]. Available: https://www.dhs.gov/publication/critical-infrastructure-information-act/. Accessed on: Sept. 4, 2021.
[13] National Institute of Standards and Technology (NIST). Computer Security Resource Center (CSRC). (2008, July 25). *SP 800-123, Guide to General Server Security*. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-123/final. Accessed on: Sept. 4, 2021.
[14] T. Dalzell, *The Routledge Dictionary of Modern American Slang and Unconventional English*, 2009. [Online]. Available: https://BGoogle-5F. Accessed on: Sept. 4, 2021.
[15] E. Partridge, T. Dalzell, T. Victor, *The Concise New Partridge Dictionary of Slang*, Psychology Press, 2007.
[16] Е. Дербин, и С. Климов, *Организационные основы обеспечения информационной безопасности предприятия*. Москва: Финанс. ун-т, 2013.
[17] А. Носарев, "Модели в информационной безопасности". [Электронный ресурс]. Доступно: https://habr.com/ru/post/467269/. Дата обращения: Сент. 4, 2021.
[18] А. Вознюк, А. Кригер, и Г. Тумуров, "Модель организации защиты информации на предприятии". [Электронный ресурс]. Доступно: https://storage.tusur.ru/files/36680. Дата обращения: Сент. 4, 2021.
[19] А. Загородников, и С. Козлов, "Модель защиты информации", на *Конф. учас. ГПО ТУСУР*, 2014. [Електронний ресурс]. Доступно: https://gpoconference.tusur.ru/conference/2014/themes/99/projects/571/discourses/653. Дата звернення: Верес. 4, 2021.

Стаття надійшла до редакції 21.09.2021.

REFERENCES

[1] KPI and two other Kyiv universities have joined the USAID Cyber Security Project. [Online]. Available: https://kpi.ua/2021-05-21. Accessed on: Sept. 4, 2021.
[2] A. Wenger, V. Mauer and M. Cavelty, *International critical information infrastructure protection handbook 2008–2009*, Eds. Center for Security Studies, ETH Zurich, 2009.
[3] *National Institute of Standards and Technology*. (2018, Apr. 16). Framework for Improving Critical Infrastructure Cybersecurity. Ver. 1.1. [Online]. Available: https://doi.org/10.6028/NIST.CSWP.04162018. Accessed on: Sept. 4, 2021.

[4] *Ukraine's national security strategy in the context of the experience of the world community*. Coll. art. for mater. int. conf. Kyiv: SATSANGA, 2001.
[5] O. Dovhan, "Critical infrastructure as an object of protection against cyber-attacks", on *scientific-practical conf. Information security: challenges and threats of modernity*. Kyiv, 2013, pp. 17-20.
[6] S. Honchar, G. Leonenko, and O. Yudin, "Theoretical and methodological aspect of information security of critical infrastructure facilities", *Bulletin of Lviv Polytechnic National University. Computer Systems and Networks*, № 806, 2014, pp. 34-39.
[7] E. Galkova, "Dynamic model of information protection in an attempt to raid a credit and financial institution", dis. cand. sciences, St. Pet. nat. res. un. of inform. tech. mechanics and optics, 2014.
[8] D. Korolev, and M. Korolev, *Information systems in banking*. Belgorod: BelSU Publ. House, 2004.
[9] J.-S. Chang, Y.-H. Jeon, and S. Sim, "Information Security Modeling for the Operation of a Novel Highly Trusted Network in a Virtualization Environment". [Online]. Available: https://doi.org/10.1155/2015/359170. Accessed on: Sept. 4, 2021.
[10] Y. Lee, "Information Security Investment Model and Level in Incomplete Information", [Online]. Available: https://doi.org/10.13089/JKIISC.2017.27.4.855. Accessed on: Sept. 4, 2021.
[11] C. K. Wong, S. B. Maynard, A. Ahmad, and H. Naseer, "Information Security Governance: A Process Model and Pilot Case Study". [Online]. Available: https://aisel.aisnet.org/icis2020/cyber_security_privacy/cyber_security_privacy/3/. Accessed on: Sept. 4, 2021.
[12] Department of Homeland Security. (2002, Nov. 25). *The Critical Infrastructure Information Act of 2002*. [Online]. Available: https://www.dhs.gov/publication/critical-infrastructure-information-act/. Accessed on: Sept. 4, 2021.
[13] National Institute of Standards and Technology (NIST). Computer Security Resource Center (CSRC). (2008, July 25). *SP 800-123, Guide to General Server Security*. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-123/final. Accessed on: Sept. 4, 2021.
[14] T. Dalzell, *The Routledge Dictionary of Modern American Slang and Unconventional English*, 2009. [Online]. Available: https://BGoogle-5F. Accessed on: Sept. 4, 2021.
[15] E. Partridge, T. Dalzell, T. Victor, *The Concise New Partridge Dictionary of Slang*, Psychology Press, 2007.
[16] E. Derbin, and S. Klimov, *Organizational framework for information security of the enterprise*. Moscow: Fin. Un., 2013.
[17] A. Nosarev, "Models in Information Security" [Online]. Available: https://habr.com/ru/post/467269/. Accessed on: Sept. 4, 2021.
[18] A. Vozniuk, A. Krieger, and G. Tumurov, "Model of organization of information protection at the enterprise". [Online]. Available: https://storage.tusur.ru/files/36680. Accessed on: Sept. 4, 2021.
[19] A. Zagorodnikov, and S. Kozlov, "Information Protection Model", in *Proc. Conf. participation GPO TUSUR*, 2014. [Online]. Available: https://gpoconference.tusur.ru/conference/2014/themes/99/projects/571/discourses/653. Accessed on: Sept. 4, 2021.

YULIIA KOZHEDUB,
SERHII VASYLENKO,
ANDRII MAKSYMETS,
VIRA HYRDA

CONCEPTUAL MODEL OF INFORMATION PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE OBJECTS OF UKRAINE

The problem of the information protection sphere – the choice of the information protection model at the critical information infrastructure objects of Ukraine is investigated. An analysis of modern models for the protection of computer systems and networks that form the basis of critical

information infrastructure objects was carried out. These models consider the specific features of their operation. They make it possible to assess different scenarios of information security events, to analyze the state of computer systems and networks that are part of the critical information infrastructure objects. They are designed to simulate the actions of the attacker. The presented models of protection with reservations can be used during the development of the architecture for the protection system of critical information infrastructure objects. The schemes which can be used to design the information protection model architecture of critical information infrastructure objects have resulted. Particular attention is paid to issues related to the peculiarities of information security threats and shows the ways of their formation This analysis is appropriate for choosing the means of information protection circulating in computer systems and networks of critical information infrastructure objects. The reasons and conditions for the formation of information security threats are important, they are a source of valuable information for establishing a basic and additional set of information security tools. The main and additional means of protection are established unconditionally for the information protection models of critical information infrastructure objects. The basis for their implementation is the matrix of information security assessment for objects of critical information infrastructure, compiled with the help of expert assessment. The components of the objects of the critical information infrastructure information protection model are determined. It consists of three components: information security threats, information infrastructure elements, and protection measures, which in turn are divided into basic and additional. The relationship of the model components is formalized with the help of a matrix. The formulaic form of the model is presented, where its elements are the probabilities arising from the influential effect of information security threats on the elements of the information infrastructure. These probabilities are established by an expert method. Sets of conditions for the influence of (external and internal) factors, states (working and emergency) functioning, the structure of elements of critical information infrastructure objects are formulated. This important information is ultimately a linguistic description of the requirements for creating an information protection model of critical information infrastructure objects.

Keywords: information security model, object of critical information structure, information security threats, protection measures, information security status assessment matrix.

Кожедуб Юлія Василівна, кандидат технічних наук, старший науковий співробітник науково-організаційного відділу науково-дослідного центру, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0001-6181-5519, JuliaKozhedub@email.ua.

Василенко Сергій Вікторович, кандидат технічних наук, начальник науково-дослідної лабораторії науково-дослідного центру, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0001-6779-8246, vasylenko.phd@gmail.com.

Максимець Андрій Володимирович, старший інженер науково-дослідної лабораторії науково-дослідного центру, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0003-3551-0628, andy.west.corp@gmail.com.

Гирда Віра Анатоліївна, старший інженер науково-дослідної лабораторії науково-дослідного центру, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-3858-4086, gidraponka@ukr.net.

Kozhedub Yuliia, candidate of technical sciences, senior researcher of the scientific-organizational department of the scientific-research center, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Vasylenko Serhii, candidate of technical sciences, head of the scientific-research laboratory of the scientific-research center, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Maksymets Andrii, senior engineer of the scientific-research laboratory of the scientific-research center, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Hyrda Vira, senior engineer of the scientific-research laboratory of the scientific-research center, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.