НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА

КОМАРОВ Максим Юрійович

УДК 004.274:004.056

МЕТОД ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ВІД КІБЕРВПЛИВІВ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Спеціальність 05.13.05 – комп'ютерні системи та компоненти

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ-2021

Дисертацією є рукопис.

Робота виконана в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України

Науковий керівник доктор технічних наук, старший дослідник
Гончар Сергій Феодосійович,
Інститут проблем моделювання в енергетиці
ім. Г.Є. Пухова НАН України, учений секретар

Офіційні опоненти: доктор технічних наук, доцент
Гнатюк Сергій Олександрович,
Національний авіаційний університет
МОН України, заступник декана з наукової
роботи факультету кібербезпеки,
комп'ютерної та програмної інженерії;

доктор технічних наук, доцент
Гавриленко Світлана Юріївна,
Національний технічний університет
«Харківський політехнічний інститут»
МОН України, професор кафедри
обчислювальної техніки та програмування

Захист відбудеться «14» травня 2021 року о 14 годині на засіданні спеціалізованої вченої ради Д 26.185.01 Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України за адресою: 03164, м. Київ, вул. Генерала Наумова, 15.

З дисертацією можна ознайомитися в бібліотеці Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України за адресою: 03164, м. Київ, вул. Генерала Наумова, 15.

Автореферат розісланий « 14 » квітня 2021 р.

Вчений секретар
спеціалізованої вченої ради В.В. Душеба

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність. Події останніх років в Україні та світі показали нагальну потребу у забезпеченні інформаційної безпеки від кібервпливів комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури України в цілому та енергетичної галузі зокрема. Згідно з Законом України «Про основні засади забезпечення кібербезпеки України» (ст. 4) об'єктами кібербезпеки, серед іншого, є об'єкти критичної інфраструктури. Згідно зі статтею 6 цього ж закону Об'єктами критичної інфраструктури є підприємства, установи та організації незалежно від форми власності, які:

- провадять діяльність та надають послуги в галузі енергетики;
- надають послуги у сферах життєзабезпечення населення, зокрема у сфері постачання електричної енергії.

Згідно зі ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» функціонування національної системи кібербезпеки забезпечується, в тому числі, шляхом встановлення обов'язкових вимог інформаційної безпеки об'єктів критичної інформаційної інфраструктури, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об'єкти критичної інформаційної інфраструктури.

Постанова Кабінету Міністрів України від 19.06.2019 № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» визначає Перелік базових вимог із забезпечення кіберзахисту об'єктів критичної інфраструктури. Відповідно до п. 12 цієї Постанови організаційні та технічні заходи з кіберзахисту, які впроваджуються на об'єкті критичної інформаційної інфраструктури, серед іншого, повинні забезпечувати мережевий захист компонентів та інформаційних ресурсів об'єкта.

З огляду на вищезазначене тема роботи присвячена розробці методу та засобів захисту інформації від кібервпливів в комп'ютерних системах та мережах об'єктів критичної інфраструктури.

Дослідженню проблем, пов'язаних із процесом захисту інформації від кібервпливів в комп'ютерних системах та мережах об'єктів критичної інфраструктури, що являється об'єктом дисертаційного дослідження присвячується значна частина публікацій вітчизняних і зарубіжних вчених, таких як: О. Корченко, С. Казмірчук, О. Архіпов, С. Гнатюк, О. Богданов, L. Daniel, Attanasio C. R., Markstein P. W., Phillips R. J. та інші. Однак, незважаючи на значну кількість підходів до вирішення даної проблеми, вона залишається актуальною не тільки для України, але і для всієї світової спільноти.

Зв'язок роботи з науковими програмами, планами, темами. Тематика основних положень дослідження пов'язана з «Основними науковими напрямами та найважливішими проблемами фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук НАН України на 2014–2018 роки», «Планом проведення ДержНДІ Спецзв'язку науково-дослідних та дослідно-конструкторських робіт за основними напрямами науково-технічної діяльності Держспецзв'язку в 2018 році (Зведений тематичний план. Частина 2)» №01/02/02-96т від 02.03.2018,

«Планом проведення ДержНДІ Спецзв'язку науково-дослідних та дослідно-конструкторських робіт за основними напрямами науково-технічної діяльності Держспецзв'язку в 2019 році (Зведений тематичний план. Частина 2)» №01/02/02-117т від 27.03.2019, Стратегією національної безпеки України від 26.05.2015 № 287/2015, Стратегією кібербезпеки України від 15.03.2016 № 96/2016 та низкою науково-дослідних робіт. Результати досліджень відображені у звітах наступних науково-дослідних робіт: «Розробка методів оцінювання чутливості Об'єднаної енергосистеми України до кібернетичних впливів» (шифр «ВПЛИВ», державний реєстраційний номер 0118U005320), «Розроблення методів забезпечення кібербезпеки функціонування Об'єднаної енергетичної системи України в рамках впровадження концепції інтелектуальних мереж» (шифр «ІНТЕЛЕНЕРГО», державний реєстраційний номер 0119U101856), в яких здобувач був виконавцем окремих розділів.

Мета та задачі дослідження. Метою дисертаційного дослідження є підвищення рівня захисту інформації від кібервпливів в комп'ютерних мережах та системах об'єктів критичної інформаційної інфраструктури, шляхом розробки відповідного методу та засобів захисту інформації.

Для досягнення цієї мети в даній роботі необхідно було розв'язати такі основні задачі:

- проаналізувати сучасні методи та засоби захисту інформації в комп'ютерних мережах та системах;
- розробити таксономію інформаційних загроз комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури;
- скласти матрицю залежності інформаційних об'єктів захисту від типу потенційних загроз, що можуть на них впливати, та схильності до конкретних загроз;
- розробити модель бази даних загроз інформаційним об'єктам захисту комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури;
- розробити метод розпізнавання кіберзагроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури
- розробити методику оцінювання кіберстійкості комп'ютерних систем та мереж об'єктів критичної інформаційної інфраструктури;
- розробити структурну модель багаторівневої системи виявлення підозрілих впливів на комп'ютерні мережі та системи об'єктів критичної інформаційної інфраструктури;
- розробити алгоритм та програмний застосунок розрахунку кіберстійкості об'єктів критичної інформаційної інфраструктури.

Об'єктом дослідження є процеси захисту інформації від кібервпливів в комп'ютерних системах та мережах об'єктів критичної інфраструктури.

Предметом дослідження є методи та засоби захисту інформації від кібервпливів в комп'ютерних системах та мережах об'єктів критичної інфраструктури.

Методи дослідження. Методи дослідження, що використовуються в роботі, базуються на методологічному базисі теорії захисту інформації та системному аналізі. При складанні матриці залежності інформаційних об'єктів захисту від типу потенційних загроз використовувались елементи теорії ймовірності і випадкових процесів. При розробці моделі бази даних кіберзагроз інформаційним об'єктам захисту інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури використовувались засоби об'єктно-орієнтовного програмування та система керування базами даних SQL Server.

Наукова новизна одержаних результатів полягає в тому, що:

– *вперше* розроблено таксономію кіберзагроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури, яка за рахунок використання ієрархічної структури відносин з деревовидним розкриттям категорій, дозволяє описувати багатоетапні атаки, які на сьогоднішній день отримали дуже широку розповсюдженість;

– *вперше* розроблено модель бази даних кіберзагроз інформаційним об'єктам захисту комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури, яка за рахунок використання параметрів загроз, визначених та класифікованих з використанням розробленої таксономії кіберзагроз, їх характеристик, параметрів заходів протидії та параметрів властивостей інформації, що підлягає захисту, дозволяє розробити базу даних кіберзагроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури;

– *вперше* розроблено комбінований метод розпізнавання кіберзагроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури, який за рахунок поєднання сигнатурного методу та методу виявлення аномалій, дозволяє розширити спектр виявлених кіберзагроз;

Практичне значення одержаних результатів. Практична цінність роботи полягає у наступному:

– розроблено алгоритмічне забезпечення на основі запропонованого комбінованого методу розпізнавання кіберзагроз для реалізації відповідного програмного засобу, що дозволяє здійснювати автоматизоване розпізнавання кіберзагроз та здійснювати захист від них;

– розроблено алгоритмічне забезпечення на основі запропонованої методики оцінювання кіберстійкості для реалізації відповідного програмного засобу, що дозволяє здійснювати автоматизований розрахунок кіберстійкості з урахуванням таких показників як кібернадійність, кіберзахищеність та кіберстійкість;

– на основі запропонованих алгоритмів розроблений програмний застосунок, що використовує запропоновану методику для захисту інформації в комп'ютерних мережах та системах об'єктів критичної інфраструктури.

Результати теоретичних та практичних досліджень знайшли застосування у таких науково-дослідних роботах:

– «Розробка методів оцінювання чутливості Об'єднаної енергосистеми України до кібернетичних впливів» (шифр «ВПЛИВ», державний реєстраційний номер 0118U005320);

– «Розроблення методів забезпечення кібербезпеки функціонування Об'єднаної енергетичної системи України в рамках впровадження концепції інтелектуальних мереж» (шифр «ІНТЕЛЕНЕРГО», державний реєстраційний номер 0119U101856).

Результати дисертаційної роботи впроваджено у діяльність Адміністрації Державної служби спеціального зв'язку та захисту інформації України, Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, Державного підприємства «Український державний центр радіочастот», Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, ПрАТ «Фарлеп-Інвест», ТОВ "ІНТЕСИС".

Особистий внесок здобувача. Основні положення та результати дисертаційної роботи, що виносяться до захисту, отримані автором самостійно. У роботах, написаних як у співавторстві, так і самостійно, автору належать: [1] – аналіз можливості інтеграції систем управління інформаційної безпеки до існуючих комплексних систем захисту інформації; [2] – аналіз стандартів з питань побудови та впровадження систем управляння інформаційною безпекою; [3] – розробка моделі загроз для захищеного вузлу Інтернет доступу; [4] – розробка моделі порушника для захищеного вузлу Інтернет доступу; [6] – аналіз існуючих механізмів безпеки системи управління базами даних; [9] – розробка таксономії кіберзагроз об'єктів критичної інфраструктури; [11] – розгляд практичних аспектів побудови комплексної системи захисту інформації в інформаційно-телекомунікаційних системах об'єктів критичної інфраструктури; [12] – дослідження нормативної бази та практичних аспектів побудови системи управління інформаційною безпекою на об'єктах критичної інфраструктури; [13] – розробка моделі загроз та моделі порушника на об'єктах критичної інфраструктури; [14] – аналіз загроз для захищеного вузлу Інтернет доступу; [15] – аналіз та розробка підходів оцінювання ризиків інформаційної безпеки; [16] – запропонована методика оцінки кіберстійкості об'єктів критичної інфраструктури; [18] – запропоновані підходи до розробки бази даних кіберзагроз об'єктів критичної інформаційної інфраструктури; [19] – огляд загальних характеристик об'єктів критичної інфраструктури та кібератак на об'єкти критичної інфраструктури; [20] – основні підходи до оцінки кібербезпеки та дослідження актуальних проблем забезпечення кібербезпеки; [21] – розроблено метод виявлення кібернетичних атак на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури; [22] – розроблена база даних кіберзагроз об'єктів критичної інформаційної інфраструктури Об'єднаної енергосистеми України. З робіт, опублікованих самостійно та у співавторстві, для вирішення задач, поставлених у дисертаційному дослідженні, використовуються результати, отримані особисто здобувачем наукового ступеня.

Апробація результатів дисертації. Основні положення дисертаційної роботи доповідались і обговорювались на таких наукових конференціях: XVII Міжнародна науково-практична конференція «Безпека інформації у інформаційно-телекомунікаційних системах» (Київ, 2015 р., 2018 р.); VI Міжнародна наукова конференція «Моделювання-2018» (Київ, 2018 р.); Всеукраїнська науково-практична конференція «Безпека соціально-економічних процесів в кіберпросторі» (Київ, 2019 р.); науково-практична конференція «Кібербезпека енергетики» (Одеса, 2018 р., 2019 р.); науково-технічна конференція «Інформаційна безпека України» (Київ, 2018р.); XII Міжнародна науково-технічна конференція «Комп'ютерні системи та мережні технології» (Київ, 2019 р.); всеукраїнська науково-практична конференція «Безпека соціально-економічних процесів в кіберпросторі» (Київ, 2019); науково-практична конференція «Проблеми теорії та практики інформаційного протиборства в умовах ведення гібридних війн» (Житомир, 2019р.), науково-практична конференція «Безпека енергетики в епоху цифрової трансформації» (Київ, 2020 р.).

Публікації. Основні положення дисертаційного дослідження опубліковано у 22 наукових працях, у тому числі: 9 наукових статей у фахових наукових журналах та збірниках наукових праць [1-9], з яких 5 – у наукових журналах, що індексуються міжнародними наукометричними базами даних [3, 4, 7, 8, 9], 1 патент України на корисну модель [21], 1 свідоцтво про реєстрацію авторського права на твір [22], а також 11 матеріалів та тез доповідей конференцій [10-20].

Структура та обсяг роботи. Дисертаційна робота складається з анотації, вступу, чотирьох розділів, висновків, 2 додатків, списку використаних джерел, та містить 152 сторінки основного тексту, 22 рисунка, 17 таблиць, 18 сторінок додатків. Список використаних джерел налічує 102 найменування на 11 сторінках. Загальний обсяг дисертаційної роботи складає 171 сторінку.

ОСНОВНА ЧАСТИНА

У анотації та вступі представлена загальна характеристика дисертації, висвітлено актуальність теми дисертаційної роботи, сформульовано мету і задачі дослідження, визначено наукову новизну отриманих результатів та їх практичне значення, наведено інформацію про впровадження результатів роботи, їх апробацію та наукові публікації, структуру, об'єм та ключові слова.

У першому розділі проведено аналіз сучасних методів та засобів захисту інформації від кібервпливів за темою дисертаційної роботи. Досліджено національне нормативно-правове забезпечення кібербезпеки та захисту інформації в комп'ютерних системах та мережах об'єктів критичної інфраструктури. Проведено аналіз існуючих робіт та можливі підходи щодо таксономії загроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інфраструктури. Описані основні підходи до створення таксономій кіберзагроз.

Порівняльна таблиця підходів до розробки таксономій кіберзагроз наведена у табл. 1.

Таблиця 1 – Порівняльна таблиця підходів до розробки таксономій кіберзагроз

Властивості / підходи до класифікації	Застосовуваність (інформативність)	Повнота	Детермінованість	Взаємне виключення	Чіткість термінів	Об'єктивність	Зрозумілість	Однозначність	Узгодженість	Повторюваність результатів
За ефектом впливу на властивості інформації	-	+	+	-	-	+	-	-	+	-
Вразливості апаратного та програмного забезпечення	+	-	+	+	+	+	+	+	-	-
Загальний список атак	+	-	-	-	+	+	-	-	+	-
Комбінований підхід	+	+	+	+	+	+	+/-	+	+	+

Таким чином, у першому розділі, на основі проведеного аналізу, обґрунтовано основні задачі дослідження, розв'язання яких необхідне для досягнення мети, що поставлена в дисертаційній роботі.

У другому розділі розроблено таксономію кіберзагроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури, складено матрицю залежності інформаційних об'єктів захисту від типу потенційних загроз, що можуть на них впливати, та схильності до конкретних загроз, а також розроблено модель бази даних кіберзагроз інформаційним об'єктам захисту комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури.

Запропонована власна таксономія кіберзагроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інфраструктури.

Кількість комп'ютерних атак, що постійно збільшується, призводить до необхідності створення організованих (або таких, що здатні самоорганізовуватись) структур, які призначені для забезпечення та надання актуальної інформації про виявлені кібервразливості, їх оперативне усунення, створення систем виявлення та запобігання вторгнень (систем активного та пасивного аудиту - Intrusion Detection System (IDS), Intrusion Prevention System (IPS)) та інші заходи. З цієї причини існують дуже великі масиви інформації щодо актуальних комп'ютерних атак та вразливостей інформаційно-телекомунікаційних систем. Однак часто ця інформація (особливо, що стосується атак) є дуже різнорідною, неструктурованою та мало придатною для подальшого аналізу. Як наслідок, в даному випадку виникає необхідність в розробці моделі та інструментарію, які за своїм призначенням направлені на можливість упорядкування та систематизації накопичених знань. Іншими словами – створення таксономії.

У запропонованій таксономії розвивається комбінований підхід до вирішення задачі класифікації. Однак, на відміну від попередніх робіт, вводиться ієрархічна структура відносин з деревовидним розкриттям категорій. Як самостійний окремий об'єкт вводиться важливе поняття «етап атаки», рис. 1, що дозволяє, на відміну від попередніх підходів, досить природним чином описувати багатоетапні атаки, які отримали високу розповсюдженість на сьогоднішній день.

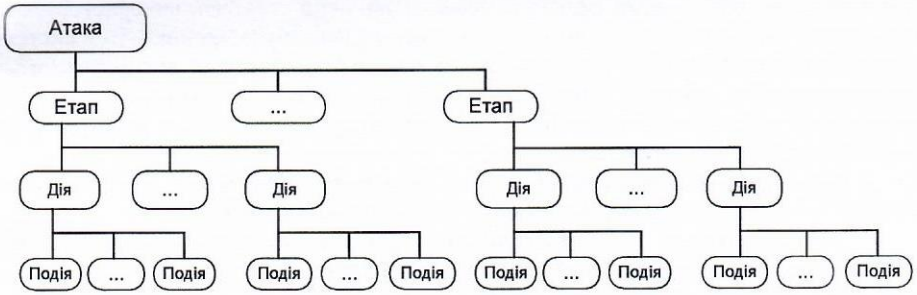

Рисунок 1 – Загальна структура атаки

Атака може складатися з декількох етапів, етап, в свою чергу, з декількох дій, дія – з декількох подій. Наприклад, злом через pro-ftpd може бути частиною одного з етапів атаки і складається з чотирьох подій, які можуть відбуватися в різному порядку.

Крім вкладеності в поняття більш високого рівня, кожне з цих чотирьох понять розкривається за допомогою дерева підкатегорій, тобто має свій власний набір атрибутів. Поняття атаки має такі атрибути, як глобальна мета / результат, властивості атаки, об'єкт атаки і атакуючий. Кожен з перерахованих атрибутів теж має свої атрибути і є піддеревом дерева атрибутів атаки.

Важливим атрибутом є об'єкт атаки, так як атаки на об'єкти різної функціональності і категорійності мають, як правило, різний характер. Тут виділяються такі властивості об'єкта атаки, як тип системи, яку атакують, її фізичний носій (обладнання, яке формує інформаційно-обчислювальну середу системи), тип засобів захисту, які використовуються в системі, і ступінь захищеності (рівень жорсткості правил безпеки), а також зовнішні комунікації системи.

Ще одним атрибутом атаки є атакуючий. Основними властивостями, які його характеризують, є розташування щодо системи, початкові привілеї і права доступу. Якщо атакуючих декілька, то в цьому випадку виникає ворожа багатоагентна система, тому стає вкрай важливим їх кількість, наявність і характер координації між атакуючими.

Останнім атрибутом, представленим на діаграмі, є атрибут «властивості атаки». Для зменшення ризику бути виявленими атаки іноді тривають по кілька місяців, а інших випадках, кілька секунд (щоб, наприклад, виключити можливість втручання адміністратора системи, яку атакують). В силу цих обставин темп

розвитку атаки являє собою важливу для класифікації властивість атаки. Інші дві властивості – видимість і можливість простежити джерело атаки (відстеженість). Видимість означає, що сценарій атаки роблений таким чином, що передбачається, що під час проведення атака не буде виявлена засобами виявлення. Відстеженість означає, що після проведення атаки при проведенні розслідування існує можливість простежити джерело атаки. Слід зазначити, що ці дві властивості сильно пов'язані одна з одною. Значення кожного з неї залежить, в першу чергу, від поставленої зловмисником мети, і вони сильно впливають на вибір стратегії, використовуваної при атаці. Наприклад, якщо завдання зловмисника непомітно проникнути в систему і викрасти конфіденційну інформацію, то при виборі стратегії він цілком може використовувати сценарії, які невидимі, проте відслідковуються (наприклад, редагування або стирання лог-файлів робить атаку істотно більш помітною, але менш відслідковуваною).

Атака складається з етапів, які, в свою чергу, теж мають свої атрибути. Поняття етап відображає окрему частину атаки та має свою локальну мету.

Етап складається з дій. Дія являє собою, в деякому сенсі, «атомарну» атаку (наприклад, сканування портів або використання програмних вразливостей). Дія теж має атрибути: тип дії, суб'єкт, об'єкт, наслідки дії, результат. Фактично, вона є мінімальним смисловим кроком атаки.

Атрибут «тип дії» описує безпосередньо саму дію, що відбувається на даному етапі атаки. Цей атрибут є найбільш важливим і інформативним. Список можливих дій схожий на перелік типових атак. З цієї причини йому теж властива відсутність повноти і, можливо, при застосуванні таксономії на практиці, представлений на рисунку список буде потребувати розширення (в залежності від специфіки області застосування). Параметр «наслідки» характеризує наслідки дії, а саме, отримані атакуючим права і привілеї в об'єкті атаки, інформацію, до якої він отримав доступ в результаті цієї дії тощо. Цей параметр містить також інформацію про рівень тривожності даної дії (безумовно, рівень тривожності є вельми суб'єктивною величиною і сильно залежить від передісторії і від оточення, в якому відбувається дія, тому тут мається на увазі деяке апріорне мірило оцінок тривожності).

Подією є мінімальний (на заданому рівні деталізації) крок з точки зору системи. Подія має наступні атрибути: тип, результат, час, суб'єкт та об'єкт.

Проведений аналіз існуючих систем захисту інформації та таксономії кіберзагроз дають змогу побудувати первинну матрицю кіберзагроз для програмних та апаратних засобів об'єктів критичної інформаційної інфраструктури. Матриця наведена у вигляді таблиці та включає загрози програмного та апаратного забезпечення, кіберзагрози прикладного ПЗ та кіберзагрози операційної системи, табл. 2.

Таблиця 2 – Матриця кіберзагроз для програмних та апаратних засобів об'єктів критичної інформаційної інфраструктури

Об'єкти / загрози	Кабельна система	Мережеве обладнання	Засоби мережевого захисту	Технологічна інформація захисту АМО	Технологічна інформація захисту хостів	Дані, що передаються мережею	ПЗ	Файли	Записи баз даних	Обчислювальні ресурси
Мережеві загрози										
Відсутність фізичного з'єднання	+	+								
Помилки, непрацездатність АМО		+	+							
Розголошення даних про мережу				+	+					
Перехоплення (сніффінг) пакетів				+	+	+				
Підміна отримувача (спуфінг пакетів)				+	+					
Відмова в обслуговуванні (DoS)				+	+		+			
Дзеркалювання трафіку					+	+				
Непрацездатність мережевих застосувань							+	+	+	
Несанкціоновані точки доступу до мережі (бекдор)		+	+	+			+	+		+
Віддалене захоплення (боти, ботнети)				+	+		+			+
Сканування системи		+	+	+						
З'єднання від імені довіреного користувача				+	+		+	+	+	+
Соціальна інженерія	+	+	+	+	+	+	+	+	+	+
Цільова кібератака (advanced persistent threat, APT)		+	+	+	+	+				
Загрози прикладного ПЗ										
Помилка, збій та відмова прикладного ПЗ							+	+	+	+
Виконання недоку-ментованих функцій					+			+	+	
Розповсюдження вірусів та хробаків					+		+	+	+	+
Несумісність версій ПЗ							+			
Перехоплення інформації					+					
Підміна або дезорганізація							+			
Злам					+		+			
Використання вразливостей та слабких місць (експлоіт)					+		+	+	+	+
Фіксація дій на пристроях вводу інформації (кейлогер)					+			+	+	
Атака під час реєстрації (login attack)					+		+	+	+	
Захоплення облікового запису (account takeover, ATO)					+		+	+	+	
Загрози операційних систем										
Помилка, збій та відмова системного ПЗ							+	+		+
Перехоплення технологічної інформації захисту					+					
Пошкодження файлів ОС					+		+			
Збирання «сміття»					+			+		
Втручання в роботу ОС з мережі					+		+	+		
Руткіт (rootkit)					+		+	+	+	+
Атака нульового дня							+	+		+

База даних «Кіберзагроз об'єктів критичної інформаційної інфраструктури Об'єднаної енергосистеми України в рамках впровадження концепції інтелектуальних мереж» (далі – БД) призначена для використання в автоматизованій системі розпізнавання несанкціонованого впливу на режими роботи об'єктів критичної інфраструктури. Кластерна структура бази даних орієнтована на зберігання параметрів елементів та об'єктів Об'єднаної енергосистеми, розрахункових параметрів режиму і інформації, отриманої від SCADA (існуючі системи управління і збору інформації) і EMS (Energy Management System) в реальному часі.

Система управління базою даних (далі - СУБД) повинна надавати системний каталог, в якому міститься:

- опис даних, які зберігаються в БД;
- опис зв'язків між даними;
- обмеження цілісності даних;
- реєстраційні дані користувачів;
- інша службова інформація.

Завдяки метаданим БД стає доступною для зовнішніх додатків, спрощується розуміння сенсу даних, посилюються заходи безпеки, виконуються передумови для аудиту інформації.

БД даних завжди повинна знаходитись у непротирічному стані в незалежності від будь-яких збоїв при проведенні операцій оновлення даних. Для цього операції з даними (в першу чергу вставки, редагування, видалення) об'єднуються у єдиний блок, який називається транзакцією. Всі оператори транзакції повинні бути виконані коректно та повністю, тільки в такому випадку в БД будуть зафіксовані зміни. В іншому випадку здійснюється автоматичний відкат транзакції, тобто стан БД буде відновлений на момент часу, який передував виклику транзакції.

Всі дані, які містяться в БД, мають бути коректними та непротирічними. Це означає, що дані в таблицях можуть модифікуватися тільки у відповідності з затвердженими правилами. В загальному випадку мається на увазі три правила підтримки цілісності даних:

- цілісність доменів;
- цілісність відношень;
- цілісність зв'язків між відношеннями.

У випадку непередбачуваних помилок та збоїв, які призвели до пошкодження або руйнуванню даних, СУБД повинна мати можливість відновлювати постраждалі дані. В першу чергу ця функція реалізована за допомогою процедур резервного копіювання.

СУБД повинна підтримувати сучасні технології та надавати доступ до БД віддаленим персональним комп'ютерам.

Доступ до даних можуть здійснювати тільки зареєстровані користувачі у відповідності із призначеними адміністратором СУБД їм правами.

Для того щоб СУБД виявилась в змозі надавати послуги, перелічені вище, вона повинна складатися із набору компонентів, наведених на рис. 2.

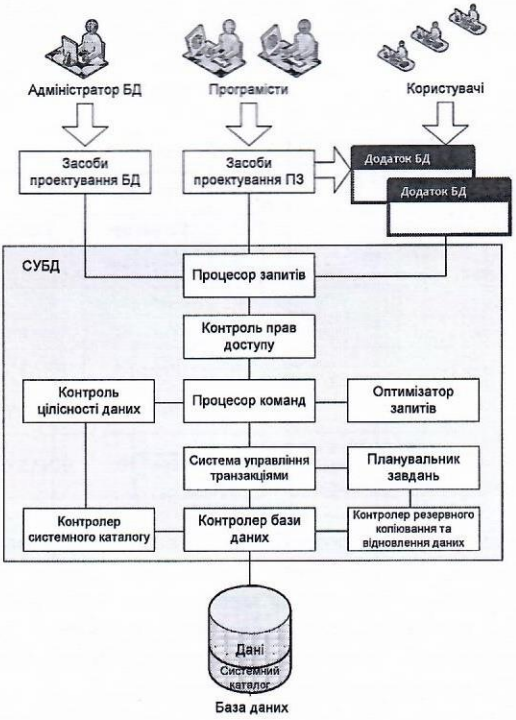

Рисунок 2 – Узагальнена структура моделі бази даних

Структура бази даних кіберзагроз об'єктів критичної інформаційної інфраструктури приведена на рис. 3.

Рисунок 3 – Структура бази даних кіберзагроз об'єктів критичної інформаційної інфраструктури

Нижче наведені приклади сутностей таблиць бази даних та фізичні характеристики логічних атрибутів приведені у табл. 3 і 4 відповідно.

Таблиця 3

Тип	Кіберзагроза
Threat	Spoofing
Specifications	Кількість виявлених IP-адрес у спам-базах
Specifications	Кількість спам-слів у темі
Specifications	Кількість спам-слів в повідомленні
Properties	Цілісність
Properties	Доступність
Properties	Спостережність
Protection	Налаштування управління доступом
Protection	Додаткова автентифікація (одноразовий пароль, криптографічна автентифікація)

Таблиця 4

№	Назва атрибуту	Фіз. формат	Переклад назви атрибуту
1	**Threats**	TXT	Назва загрози
2	**Properties**	TXT	Властивості інформації
3	**Protection**	TXT	Заходи протидії
4	**Specifications**	TXT	Назва типу документу
5	**Thre_ID**	BINARY	Ідентифікатор загрози
6	**Prop_ID**	BINARY	Ідентифікатор властивості інформації
7	**Prot_ID**	BINARY	Ідентифікатор заходу протидії
8	**Spec_ID**	BINARY	Ідентифікатор характеристики загрози

У третьому розділі розроблено метод розпізнавання кіберзагроз інформаційній безпеці комп'ютерних систем та мереж об'єктів критичної інфраструктури, розроблена структурна модель багаторівневої системи виявлення підозрілих впливів на комп'ютерні системи та мережі об'єктів критичної інфраструктури, розроблена методика оцінювання кіберстійкості комп'ютерних систем та мереж об'єктів критичної інфраструктури.

Метод ґрунтується на способі моніторингу трафіку, що надходить до відомчої інформаційно-телекомунікаційної системи з глобальної мережі Інтернет. Метод призначений для застосування у багаторівневій системі виявлення підозрілих впливів, яка здійснює моніторинг, аналіз та обробку покажчиків вхідного трафіку. Метод реалізує три рівня аналізу впливів:

1) автоматичне сканування трафіку, визначення типу протоколу мережевої взаємодії;
2) аналіз та виявлення таких підозрілих факторів, як відмова в обслуговуванні, підміна IP-адрес, вразливості (слабкі місця) протоколів мережевої взаємодії, вразливості (слабкі місця) додатків;
3) атака (спроба підбору) на пароль, захоплення (привласнення) привілей, спроби впровадження шкідливого програмного забезпечення типу «троянські коні», аудит (моніторинг) мережі, скриті дії.

На підставі даного методу розроблено структурну модель (рішення) багаторівневої системи виявлення підозрілих впливів на комп'ютерні системи та мережі об'єктів критичної інфраструктури, що реалізує запропонований у даній дисертаційній роботі метод, рис. 4.

З використанням запропонованих у дисертаційній роботі таксономії кіберзагроз та моделі бази даних кіберзагроз розроблена методика оцінювання кіберстійкості комп'ютерних систем та мереж об'єктів критичної інфраструктури.

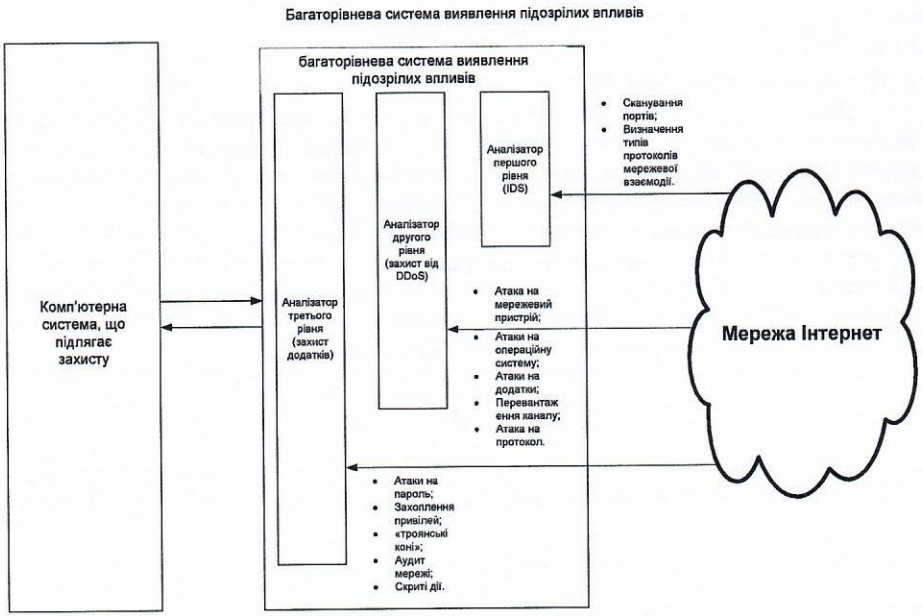

Рисунок 4 – Структурна модель (рішення) багаторівневої системи виявлення підозрілих впливів

Запропонована методика полягає в оцінці складних технічних систем, що мають високий ступінь критичності. Дану методику можливо її застосовувати для підвищення ефективності управління критичною інфраструктурою.

Узагальнений показник кіберстійкості одноланкового об'єкта КІІ має вигляд:

$$К_{ОКІІ}^{уп} = К_{ОКІІ}^{жив} * К_{ОКІІ}^{зах} * К_{ОКІІ}^{над}, \quad (1)$$

де: $К_{ОКІІ}^{уп}$ – узагальнений показник кіберстійкості; $К_{ОКІІ}^{жив}$ – кіберживучість об'єкта КІІ, яка трактується як здатність збереження його працездатності (виживання) в умовах виходу з ладу технічних засобів обробки інформації внаслідок кібервпливів (КВ), тобто, по суті – внесок кожного базового елемента одноланкового об'єкта КІІ у виконання ним цільової функції; $К_{ОКІІ}^{зах} = (1 - Р_{ЗКА})*(1 - Р_{ЦКА})$ – кіберзахищеність одноланкового об'єкта КІІ, що трактується як ймовірність забезпечення виконання цільової функції об'єкта КІІ із заданою якістю в умовах застосування «загальних» і цілеспрямованих КВ; $Р_{ЗКА}$ і $Р_{ЦКА}$ – ймовірності ураження технічних засобів обробки інформації, що входять до об'єкта КІІ, загальними ($Р_{ЗКА}$) та цілеспрямованими ($Р_{ЦКА}$) КВ; $К_{ОКІІ}^{над}$ – кібернадійність одноланкового об'єкта КІІ, під якою розуміється ймовірність забезпечення виконання цільової функції об'єкта КІІ протягом визначеного часового інтервалу в умовах виникнення різних подій (i = 1,…., N) – програмних та технічних відмов засобів об'єкта КІІ внаслідок КВ, де

$$K_{ОКІІ}^{над} = \prod_{i=1}^{N} K_{ОКІІНАДі} (1 - P_i), \quad (2)$$

де P_i – імовірність *i*-ої події ($i = 1,\ldots, N$).

До об'єктів КІІ вже на етапах проєктування висуваються досить жорсткі вимоги з технічної надійності і передбачається низка спеціальних заходів щодо запобігання технічним і програмним відмовам технічних засобів обробки інформації (наприклад, завдяки кластеризації серверів, через резервування окремих компонентів). Відповідно до цього в завданнях оцінки кіберстійкості КІІ цілком допустимо вважати ймовірність програмних та технічних відмов за умови своєчасного і якісного проведення технічного обслуговування зневажливо малою, тобто $P_{ТН}=0$, де $P_{ТН}$ – імовірність технічного неспрацювання. У цьому разі кібернадійність одноланкового об'єкта КІІ буде визначатися як:

$$K_{ОКІІ}^{о} = K_{ОКІІ}^{жив} * K_{ОКІІ}^{зах}. \quad (3)$$

Якщо вважати виходи з ладу ланок КІІ в умовах КВ незалежними подіями, кіберстійкість багатоланкового об'єкта КІІ ($K_{ОКІІстб}$) може бути знайдена із виразу:

$$K_{ОКІІстб}(N) = \prod_{i=1}^{N} K_{ОКІІоі}, \quad (4)$$

де N – кількість різних шкідливих подій, зумовлених КВ;

$K_{ОКІІоі}$ – кіберстійкість *i*-го одноланкового об'єкта КІІ.

Кібернадійність багатоланкового об'єкта КІІ трактується як ймовірність забезпечення виконання цільової функції об'єкта КІІ протягом визначеного часового інтервалу в умовах виникнення програмних помилок і технічних збоїв одноланкових об'єктів КІІ, з яких складається багатоланковий.

Тобто кіберстійкість багатоланкового об'єкта КІІ має розраховуватися як спільна N-мірна функція розподілу ймовірності збереження працездатності одночасно N ланок, які складають цей багатоланковий об'єкт КІІ:

$$K_{ОКІІсб}\left(K_{ОКІІсо1,\ldots,K_{ОКІІсоN}}\right) = P\left\{K_{ОКІІсо1} \geq K_{ОКІІсопотр}, \ldots, K_{ОКІІсоN} \geq K_{ОКІІоспотр}\right\} \quad (5)$$

де: $K_{ОКІІсб}(N)$ – кіберстійкість багатоланкового об'єкта КІІ;

$K_{ОКІІсо1}$ – кіберстійкість першого одноланкового об'єкта КІІ;

$K_{ОКІІсопотр}$ – потрібна кіберстійкість першого одноланкового об'єкта КІІ;

$K_{ОКІІсоN}$ – кіберстійкість N-го одноланкового об'єкта КІІ;

$K_{ОКІІоспотр}$ – потрібна кіберстійкість N-го одноланкового об'єкта КІІ.

Основою розрахунку кіберстійкості багатоланкових об'єктів КІІ є розрахунок показників кіберзахищеності і кіберживучості окремих ланок об'єкта КІІ.

Зважаючи на те, що властивості, які характеризують кіберживучість об'єкта КІІ в умовах здійснення КВ – Ω, починають проявлятися тільки після того, як об'єкт зазнав впливу, то міра живучості має визначатися умовною імовірністю збереження працездатності, за умови, що система отримала локальне пошкодження.

Під показником кіберживучості одноланкового об'єкта КІІ, $К_{ОКІІ\ ЖИВ}$, будемо розуміти умовну ймовірність невиходу кінцевого стану об'єкта КІІ за межі заданої області безпечних станів S^I простору безпечних станів S у разі проведення КВ S_0.

$$К_{ОКІІЖИВ} = P[(\|S - s_0\| < S^I)/\Omega]. \quad (6)$$

З огляду на розуміння функціональної вразливості системи V_S, під якою будемо розуміти ймовірність виходу кінцевого стану системи із заданої безпечної області S^I, справедливо:

$$К_{ОКІІ\ ЖИВ} = 1 - V_S, \quad (7)$$

а в конкретній точці часового інтервалу, що досліджується:

$$К_{ОКІІ\ ЖИВ}(t) = 1 - V_S(t). \quad (8)$$

Критерієм оцінки кіберживучості одноланкового об'єкта КІІ будемо розглядати вираз:

$$К^{пот}_{ОКІІЖИВ}(t) \geq К^{пр}_{ОКІІЖИВ}(t), \quad (9)$$

де $К^{пот}_{ОКІІЖИВ}(t)$ – поточний рівень кіберживучості одноланкового об'єкта КІІ, а $К^{пр}_{ОКІІЖИВ}(t)$ – потрібний рівень його кіберживучості в умовах здійснення КВ.

Визначимо наступний критерій здатності об'єкта КІІ виконувати цільову функцію в умовах КВ W_6:

$$W_6 = \begin{cases} К^{пот}_{ОКІІЖИВ}(t) > 0{,}9 - \text{об'єкт КІІ повністю дієздатний} \\ 0{,}7 \leq К^{пот}_{ОКІІЖИВ}(t) < 0{,}9 - \text{об'єкт КІІ загалом дієздатний} \\ 0{,}5 \leq К^{пот}_{ОКІІЖИВ}(t) < 0{,}7 - \text{об'єкт КІІ обмежений} \\ 0{,}3 \leq К^{пот}_{ОКІІЖИВ}(t) < 0{,}5 - \text{об'єкт КІІ недієздатний (підлягає відновленню)} \\ К^{пот}_{ОКІІЖИВ}(t) \leq 0{,}3 - \text{об'єкт КІІ недієздатний (не підлягає відновленню)} \end{cases} \quad (10)$$

Схематичне відображення методики оцінки кіберстійкості КІІ зображено на рис. 5.

Методика оцінки кіберстійкості охоплює такі етапи:

1. Оцінка кіберживучості кожного об'єкта КІІ окремо.

1.1. Оцінка кіберживучості одноланкового об'єкта КІІ.

Рівень кіберзахищеності – ймовірність збереження працездатності *i*-го елемента в умовах КВ.

Оцінити коефіцієнт пов'язаності *i*-го елемента і його внесок в цільову функцію об'єкта КІІ.

1.2. Оцінка кіберживучості багатоланкового об'єкта КІІ.

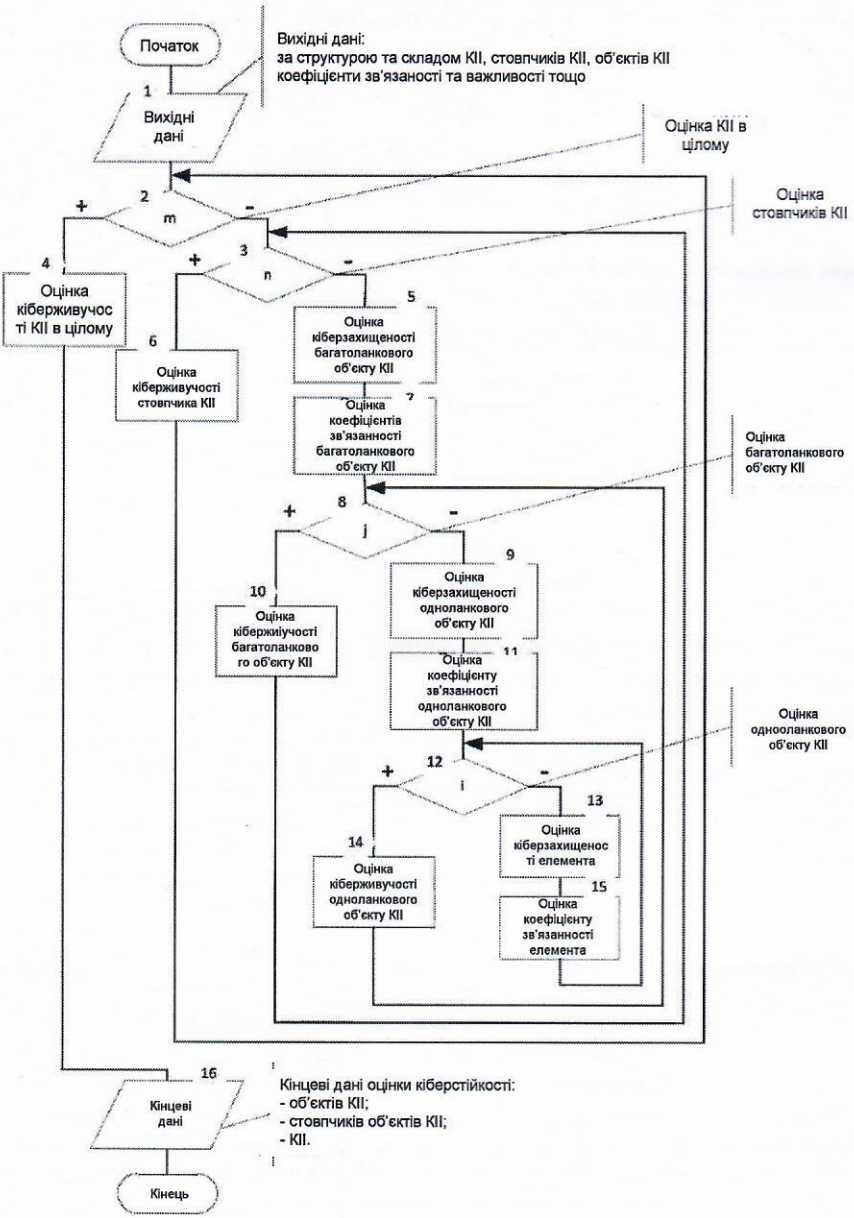

Рисунок 5 – Схематичне відображення методики оцінки кіберстійкості КІІ

Рівень кіберзахищеності – ймовірність збереження працездатності *j*-го одноланкового об'єкта КІІ в умовах реалізації КВ.

Оцінити коефіцієнт пов'язаності *j*-го одноланкового об'єкта КІІ та його внесок у цільову функцію багатоланкового об'єкта КІІ.

2. Оцінка кіберживучості взаємодіючих об'єктів КІІ (стовпчиків об'єктів КІІ).

Рівень кіберзахищеності – ймовірність збереження працездатності *n*-го багатоланкового об'єкта КІІ в умовах реалізації КВ.

3. Оцінка кіберживучості КІІ через суму стійкості її елементів з урахуванням їх коефіцієнта пов'язаності.

Оцінка кіберживучості КІІ загалом, відповідно до поточного стану КІІ і ступеня важливості, в певний момент часу, виконання ними функцій.

Під час розробки методики оцінки стійкості об'єктів КІ, що функціонують у кіберпросторі, було запропоновано введення такої властивості, як кіберстійкість. Необхідність введення такої властивості викликана специфічним середовищем функціонування мережевої інфраструктури об'єктів КІІ (кіберпростір) та появою нових вразливостей і загроз для КІІ і об'єктів КІІ Об'єднаної енергосистеми України.

Запропонована методика завдяки декомпозиції КІІ на окремі об'єкти КІІ з урахуванням коефіцієнтів зв'язаності і ступеня важливості функцій, які виконуються в цей момент, дозволяє здійснити оцінку кіберстійкості КІІ відповідно до заданого рівня. Отриманий результат, відповідно до розробленої схеми відповідності стану об'єкта КІІ рівню захищеності, дозволяє однозначно оцінити стан кіберзахищеності КІІ від кібератак.

У четвертому розділі розроблено алгоритм функціонування багаторівневої системи виявлення підозрілих впливів та програмний за стосунок, який реалізує даний алгоритм, проведено експериментальні дослідження систем захисту інформації комп'ютерних систем та мереж об'єктів критичної інфраструктури.

З використанням методу та засобів, розроблених у даній дисертаційній роботі, проводилися роботи по створенню КСЗІ захищеного вузла Інтернет доступу «Фарлеп-Інвест» та здійсненні державної експертизи КСЗІ в автоматизованій інформаційній системі «Централізована база даних перенесених номерів» державного підприємства «Український державний центр радіочастот».

Отримані результати підтверджують функціонування системи захисту інформації комп'ютерних систем та мереж об'єктів критичної інфраструктури, створеної на основі розроблених у дисертації методу та методики, та успішне практичне застосування даної системи.

У додатках наведено документи, що підтверджують впровадження результатів дисертації, та лістинги (коди) програмних засобів.

ВИСНОВКИ

У дисертаційній роботі вирішено актуальну науково-прикладну задачу, пов'язану з підвищенням рівня захисту інформації від кібервпливів в комп'ютерних мережах та системах об'єктів критичної інформаційної інфраструктури, шляхом розробки відповідного методу та засобів захисту інформації.

При вирішенні цієї задачі отримані такі основні результати:

1. Проаналізовано сучасні методи та засоби захисту інформації в комп'ютерних мережах та системах. Встановлено, що дослідженню проблем, пов'язаних із процесом захисту інформації від кібервпливів в комп'ютерних системах та мережах об'єктів критичної інфраструктури, що являється об'єктом дисертаційного дослідження, присвячується значна частина публікацій вітчизняних і зарубіжних вчених. Однак, незважаючи на значну кількість підходів до вирішення даної проблеми, вона залишається актуальною не тільки для України, але і для всієї світової спільноти.

2. Розроблено таксономію кіберзагроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури, яка за рахунок використання параметрів системи, властивостей порушника та визначеної структури загрози дозволяє розробити модель загроз та модель порушника інформації в комп'ютерних мережах та системах об'єктів критичної інформаційної інфраструктури.

3. Складено матрицю залежності інформаційних об'єктів захисту від типу потенційних загроз, що можуть на них впливати, та схильності до конкретних загроз.

4. Розроблено модель бази даних кіберзагроз інформаційним об'єктам захисту комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури, яка за рахунок використання параметрів загроз, визначених та класифікованих з використанням розробленої таксономії кіберзагроз, їх характеристик, параметрів заходів протидії, параметрів властивостей інформації, що підлягає захисту, дозволяє розробити базу даних кіберзагроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури.

5. Розроблено комбінований метод розпізнавання кіберзагроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури, який за рахунок поєднання сигнатурного методу та методу виявлення аномалій, дозволяє розширити спектр виявлених кіберзагроз.

6. Розроблено методику оцінювання кіберстійкості комп'ютерних систем та мереж об'єктів критичної інформаційної інфраструктури, яка за рахунок використання розробленої таксономії кіберзагроз та моделі бази даних кіберзагроз дозволяє забезпечити підтримку створення систем захисту інформації комп'ютерних систем та мереж об'єктів критичної інформаційної інфраструктури.

8. Розроблено структурну модель багаторівневої системи виявлення кібервпливів на комп'ютерні мережі та системи об'єктів критичної інфраструктури на основі запропонованого комбінованого методу розпізнавання кіберзагроз, що дозволяє здійснювати автоматизоване розпізнавання кіберзагроз та здійснювати захист від них.

9. Розроблено алгоритмічне забезпечення та програмний застосунок захисту інформації, яка циркулює в комп'ютерних мережах та системах об'єктів критичної інфраструктури, що дозволяє здійснювати автоматизований розрахунок кіберстійкості з урахуванням таких показників як кібернадійність, кіберзахищеність та кіберстійкість з використанням розробленої методики. Зазначений програмний

застосунок використано при побудові комплексних систем захисту інформації інформаційних систем об'єктів критичної інфраструктури.

10. Експериментальні дослідження програмного застосунку обчислювальних систем для розрахунку суми ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури, а також впровадження та успішне практичне використання зазначених розробок підтвердили достовірність теоретичних гіпотез та практичних розробок і висновків дисертаційної роботи.

Результати дисертаційної роботи впроваджено у діяльність Адміністрації Державної служби спеціального зв'язку та захисту інформації України (відгук від 20.03.2019р. № 05/02-295), Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації (акт від 11.03.2021р.), Державного підприємства «Український державний центр радіочастот» (відгук від 10.10.2019р. №80/14.2-55/847/13063), Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (акт від 12.01.2021р.), ПрАТ «Фарлеп-Інвест» (відгук від 09.07.2018р. №65/04-10), ТОВ "ІНТЕСИС" (відгук від 01.10.2019р. №011019/01).

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Комаров М.Ю. Методика побудови системи управління інформаційною безпекою на об'єктах критичної інфраструктури / Комаров М.Ю., Гончар С.Ф. // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ ім. Г.Є. Пухова НАН України. – Київ, 2017. – №81. – С. 12-19.
2. Комаров М.Ю. Нормативний аспект побудови та впровадження системи управління інформаційною безпекою на об'єктах критичної інфраструктури / Комаров М.Ю., Гончар С.Ф., Ониськова А.В. // Моделювання та інформаційні технології. – 2018. – №82, С. 40-48.
3. Комаров М.Ю. Аналіз та дослідження загроз для захищеного вузлу Інтернет доступу / Комаров М.Ю., Гончар С.Ф. // Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки. – 2018. – Том 29 (68). № 4. Ч1, С. 165-168.
4. Комаров М.Ю. Аналіз та дослідження моделі порушника безпеки інформації для захищеного вузла інтернет доступу / Комаров М.Ю., Ониськова А.В., Гончар С.Ф. // Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Технічні науки. – 2018. – Том 29 (68), №5, Ч.1, С. 138-142.
5. Комаров М.Ю. Підсистема управління доступом системи управління базами даних ORACLE DATABASE 12C ENTERPRISE EDITION / Комаров М.Ю. // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ ім. Г.Є. Пухова НАН України. – 2018. №84. С. 87-96.
6. Комаров М.Ю. Аналіз механізмів безпеки системи управління базами даних Oracle Database 12C enterprise Edition / Комаров М.Ю., Гончар С.Ф. // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ ім. Г.Є. Пухова НАН України. – 2018. №85. С. 107-116.
7. Комаров М.Ю. Загальні характеристики підприємства електроенергетики і елементи їх вразливості технологічного походження / Комаров М.Ю. // Електронне моделювання. – 2019. Том 41, №1. С. 93-104.

8. Комаров М.Ю. Огляд кібератак на об'єкти критичної інфраструктури / Комаров М.Ю. // Електронне моделювання. – 2019. Том 41, № 6. С. 91-106.
9. Комаров М.Ю. Вимоги до таксономії кіберзагроз об'єктів критичної інфраструктури та аналіз існуючих підходів / Комаров М.Ю. // Електронне моделювання. – 2020. Том 42, № 3. С. 111-124.
10. Комаров М.Ю. Особливості оцінки рівня гарантій Г-3 коректності реалізації функціональних послуг безпеки у засобах захисту інформації від несанкціонованого доступу / Комаров М.Ю. // Безпека інформації в інформаційно-телекомунікаційних системах: Міжнар. наук.-практ. конф., 2015, Київ, 2015, С. 52-53.
11. Комаров М.Ю. Система управління інформаційною безпекою. Аналіз нормативної бази / Комаров М.Ю., Гончар С.Ф., Леоненко Г.П. // Безпека інформації в інформаційно-телекомунікаційних системах: XX Ювілейна Міжнар. наук.-практ. конф., 2018, Київ, 2018, С. 250-251.
12. Комаров М.Ю. Практичні аспекти побудови комплексної системи захисту інформації / Комаров М.Ю., Гончар С.Ф. // Кібербезпека енергетики: Наук.-практ. конф., 2018, м. Одеса.
13. Комаров М.Ю. Застосування систем управління інформаційною безпекою на об'єктах критичної інфраструктури / Комаров М.Ю., Гончар С.Ф. // Інформаційна безпека України: Наук.-практ. конф. 2018, м. Київ.
14. S. Honchar, M. Komarov, A. Onyskova. Model of Threats for a Secured Internet Access Node / S. Honchar, M. Komarov, A. Onyskova // Моделювання-2018: Міжнар. наук.-практ. конф., Київ, 2018, С. 123-126.
15. Ткаченко В.В. Основні підходи оцінювання ризиків інформаційної безпеки / Ткаченко В.В., Комаров М.Ю. // Комп'ютерні системи та мережні технології: конф., Київ, 2019.
16. Гончар С.Ф. Методика оцінки кіберстійкості об'єктів критичної інфраструктури / Гончар С.Ф., Комаров М.Ю. // Безпека соціально-економічних процесів в кіберпросторі: Всеук. наук.-практ. конф., 2019, Київ, 2019, С. 49-50.
17. Комаров М.Ю. Аналіз шкідливого програмного забезпечення, як кіберзброї, та методи протидії кібератакам / Комаров М.Ю. // Проблеми теорії та практики інформаційного протиборства в умовах ведення гібридних війн: конф., Житомир, 2019, С. 235-238.
18. Комаров М.Ю. Розробка бази даних кіберзагроз об'єктів критичної інформаційної інфраструктури, М.Ю. Комаров, А.В. Ониськова, С.Ф. Гончар, В.В. Ткаченко, С.М. Сергєєв // Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України: XXXVIII наук-техн. конф. молодих вчених, Київ, 2020, С. 30-32.
19. Ткаченко В.В. Основні підходи до оцінки кібербезпеки SMART GRID систем» В.В. Ткаченко, М.Ю. Комаров, С.М. Сергєєв // Європейський університет, Національний авіаційний університет: Актуальні питання забезпечення кібербезпеки та захисту інформації: VI Міжнародна наук-практ. конф., Київ 2020, С. 99-104.

20. Комаров М.Ю. Дослідження актуальних проблем забезпечення кібербезпеки Об'єднаної енергосистеми України в рамках впровадження концепції інтелектуальних мереж / Комаров М.Ю., Гончар С.Ф., Ониськова А.В. // Матеріали Другої науково-практичної конференції «Безпека енергетики в епоху цифрової трансформації», Київ, 2020, С. 11.
21. Комаров М.Ю., Мохор В.В., Гончар С.Ф. Спосіб виявлення кібернетичних атак на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури. Патент на корисну модель №132581. Патент опубліковано 25.02.2019, бюл. №4.
22. Мохор В.В., Гончар С.Ф., Комаров М.Ю., Чьочь В.В. База даних «Кіберзагрози об'єктів критичної інформаційної інфраструктури Об'єднаної енергосистеми України». Свідоцтво про реєстрацію авторського права на твір № 95314 від 14.01.2020.

АНОТАЦІЯ

Комаров М.Ю. Метод та засоби захисту інформації від кібервпливів в комп'ютерних системах та мережах об'єктів критичної інфраструктури. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти. – Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, 2021.

У дисертаційній роботі вирішено актуальну науково-прикладну задачу, пов'язану з підвищенням рівня захисту інформації від кібервпливів в комп'ютерних мережах та системах об'єктів критичної інформаційної інфраструктури, шляхом розробки відповідного методу та засобів захисту інформації. Розроблено таксономію кіберзагроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури. Складено матрицю залежності інформаційних об'єктів захисту від типу потенційних загроз, що можуть на них впливати, та схильності до конкретних загроз. Розроблено модель бази даних кіберзагроз інформаційним об'єктам захисту комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури. Розроблено комбінований метод розпізнавання кіберзагроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури. Розроблено методику оцінювання кіберстійкості комп'ютерних систем та мереж об'єктів критичної інформаційної інфраструктури. Розроблено структурну модель багаторівневої системи виявлення кібервпливів на комп'ютерні мережі та системи об'єктів критичної інфраструктури на основі запропонованого комбінованого методу розпізнавання кіберзагроз. Розроблено алгоритмічне забезпечення та програмний застосунок захисту інформації, яка циркулює в комп'ютерних мережах та системах об'єктів критичної інфраструктури. Проведено експериментальні дослідження з метою підтвердження теоретичних положень та практичних розробок дисертаційного дослідження.

Ключові слова: захист інформації, кібервплив, комп'ютерна система, мережа, кібербезпека, інформаційна система, об'єкт критичної інфраструктури.

АННОТАЦИЯ

Комаров М.Ю. Метод и средства защиты информации от кибервлияний в компьютерных системах и сетях объектов критической инфраструктуры. – На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.05 – компьютерные системы и компоненты. – Институт проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины, Киев, 2021.

Диссертационная работа посвящена повышению уровня защиты информации от кибервлияний в компьютерных сетях и системах объектов критической информационной инфраструктуры, путем разработки соответствующего метода и средств защиты информации. Проанализированы современные методы и средства мониторинга, выявления и противодействия киберугрозами информационно-телекоммуникационных систем. Показано, что обеспечение киберзащиты информационных сетей предприятия электроэнергетики при реализации мер противодействия современным киберугрозами является неотъемлемой частью политики безопасности информации предприятий энергетической отрасли. Анализируя общие угрозы безопасности информации при разработке политики безопасности на предприятии энергетического сектора, необходимо учитывать специфику его функционирования, а также принимать во внимание технологическую и функциональную специфику обработки информации, циркулирующей на соответствующих объектах информационной деятельности. Проанализированы основные уязвимости информационно-телекоммуникационных систем объектов критической инфраструктуры, усовершенствованы основные подходы к защите от киберугроз информационно-телекоммуникационных сетей объектов критической инфраструктуры, а также разработана классификация киберугроз информационно-телекоммуникационным сетям объектов критической инфраструктуры. Разработан таксономии киберугроз информационно-телекоммуникационным сетям объектов критической инфраструктуры. В предлагаемой таксономии развивается комбинированный подход к решению задачи классификации. Однако в отличие от предыдущих работ вводится иерархическая структура отношений с древовидным раскрытием категорий. Как самостоятельный отдельный объект вводится важное понятие «этап атаки», что позволяет, в отличие от предыдущих подходов, достаточно естественным образом описывать многоэтапные атаки, которые на сегодняшний день получили очень широкую распространенность. Составлен матрицу зависимости информационных объектов защиты от типа потенциальных угроз, которые могут на них влиять, и склонности к конкретным угроз. Разработана модель базы данных киберугроз информационным объектам защиты информационно-телекоммуникационных систем объектов критической инфраструктуры. Разработан универсальный инструментарий, включающий в себя набор методов и средств обеспечения устойчивой кибербезопасности информационных объектов защиты информационно-телекоммуникационных систем объектов критической инфраструктуры от, как можно, широкого круга угроз информации. Научные положения, выводы и рекомендации, сформулированные в диссертации, основаны на достаточном уровне.

Методы исследования, используемые в работе, базируются на методологическом базисе теории защиты информации и системном анализе новейших теоретических и практических разработок, применяемых в области информационной безопасности для эффективного решения соответствующих проблем кибербезопасности. При составлении матрицы зависимости информационных объектов защиты от типа потенциальных угроз, которые могут на них влиять, и склонности к конкретным угроз, использовались элементы теории вероятности и случайных процессов. При разработке модели базы данных киберугроз информационным объектам защиты информационно-телекоммуникационных систем объектов критической инфраструктуры, использовались средства объектно-ориентированного программирования и система управления базами данных SQL Server. При разработке универсального инструментария, включающего в себя набор методов и средств обеспечения устойчивой кибербезопасности информационных объектов защиты информационно-телекоммуникационных систем объектов критической инфраструктуры от как можно широкого круга угроз информации, применялись элементы теории алгоритмов, эксперимента, объектно-ориентированное программирование, а также имитационное моделирование информационных процессов и структур. Методы исследования применены корректно. Достоверность теоретических результатов проверена экспериментально. Результаты моделирования хорошо согласуются с полученными экспериментальным путем. Результаты диссертационной работы внедрены в деятельность Администрации Государственной службы специальной связи и защиты информации Украины, Государственного научно-исследовательского института технологий кибербезопасности и защиты информации, Государственного предприятия «Украинский государственный центр радиочастот», Института проблем моделирования в энергетике им. Е. Пухова НАН Украины, ЧАО «Фарлеп-Инвест», ООО «ІНТЕСИС".

Ключевые слова: защита информации, кибервлияние, компьютерная система, сеть, кибербезопасность, информационная система, объект критической инфраструктуры.

ABSTRACT

Komarov M. Method and means of protecting information from cyber influences in computer systems and networks of critical infrastructure objects. – As the manuscript.

Thesis for a Candidate of Technical Sciences degree in specialty 05.13.05 – computer systems and components. – Pukhov Institute for Modeling in Energy Engineering, National Academy of Sciences of Ukraine, Kyiv, 2021.

The dissertation solves a topical scientific and applied problem related to increasing the level of protection of information from cyber influences in computer networks and systems of critical information infrastructure, by developing an appropriate method and means of information protection. A taxonomy of cyber threats to information security of computer networks and systems of critical information infrastructure objects has been developed. A matrix of dependence of information objects of protection on the type of

potential threats that may affect them and susceptibility to specific threats has been compiled. A model of a database of cyber threats to information objects of protection of computer networks and systems of objects of critical information infrastructure has been developed. A combined method for recognizing cyber threats to information security of computer networks and systems of critical information infrastructure has been developed. A method for assessing the cyber resilience of computer systems and networks of critical information infrastructure has been developed. A structural model of a multilevel system for detecting cyber impacts on computer networks and systems of critical infrastructure objects has been developed on the basis of the proposed combined method of cyber threat recognition. Algorithmic software and software application for protection of information circulating in computer networks and systems of critical infrastructure objects have been developed. Experimental researches are carried out for the purpose of confirmation of theoretical positions and practical developments of dissertation research.

Keywords: information protection, cyber influence, computer system, network, cybersecurity, information system, critical infrastructure object.

Підписано до друку 12.04.2021 р. Формат 60х90 1/16.
Папір офсетний. Друк лазерний.
Набір комп'ютерний. Умовн. др. арк. 0,9.
Наклад 100 прим. Зам. № 1304/03.

Надруковано ФОП Гузік О.М.
Реєстраційний номер №2705814113
м. Київ, вул. Б. Гаврилишина, 16
Тел.: 338-16-61.