DOI: 10.36910/6775-2524-0560-2020-39-22
УДК: [004.02/.032/.421] + 621.391 +004.031.42+007.2
Козубцова Леся Михайлівна
https://orcid.org/0000-0002-7866-8575
Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна

УДОСКОНАЛЕНА МЕТОДИКА ДІАГНОСТУВАННЯ КІБЕРНЕТИЧНОЇ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ З УРАХУВАННЯМ ДЕСТРУКТИВНИХ КІБЕРНЕТИЧНИХ ВПЛИВІВ

Козубцова Л.М. Удосконалена методика діагностування кібернетичної захищеності інформаційної системи з урахуванням деструктивних кібернетичних впливів. В статті проаналізовано відомі спроби рішень наукової задачі з розрахунку кібернетичної захищеності інформаційної системи спеціального призначення. Встановлено, що на даний час існуючі рішення не враховують при розрахунку деструктивний інформаційний вплив, а тому результат носить статичний характер. Запропонований математичний апарат методики забезпечує розрахунок кібернетичної захищеності інформаційної системи спеціального призначення для моделі найгіршого варіанту настання події загрози нульового дня.
Ключові слова: методика, оцінка, кібернетична захищеність, інформаційна система спеціального призначення, деструктивний кібернетичний вплив.

Козубцова Л.М. Усовершенствованная методика диагностирования кибернетической защищенности информационной системы с учетом деструктивных кибернетических воздействий. В статье проанализированы известные попытки решений научной задачи по расчету кибернетической защищенности информационной системы специального назначения. Установлено, что в настоящее время существующие решения не учитывают при расчете деструктивное информационное влияние, а потому результат носит статический характер. Предложенный математический аппарат методики обеспечивает расчет кибернетической защищенности информационной системы специального назначения для модели наихудшего варианта наступления события угрозы нулевого дня.
Ключевые слова: методика, оценка, кибернетическая защищенность, информационная система специального назначения, деструктивный кибернетический влияние.

Kozubtsova L. M. Improved method of diagnostics of cybernetic protection of the information system taking into account destructive cybernetic influences. The article analyzes well-known attempts to solve the scientific problem of calculating the cybernetic security of a special-purpose information system. It is established that currently existing solutions do not take into account destructive information influence in the calculation, and the result is static. The proposed mathematical apparatus of the method provides the calculation of cybernetic security of a special-purpose information system for the model of the worst-case scenario of a zero-day threat event.
Keywords: methodology, assessment, cybernetic security, special-purpose information system, destructive cybernetic influence.

Постановка завдання і зв'язок її з важливими науковими завданнями. Відповідно до мети, об'єкта, предмета та визначеного наукового завдання дисертаційного дослідження необхідно: визначити в умовах реальних деструктивних кібернетичних впливах числових значень кібернетичної захищеності кожного компонента (K_j) засобу (Z_i) інформаційної системи спеціального призначення (ІС СП) ($P_{КЗ(KjZi)}$) та кожного засобу (Z_i) ІС СП ($P_{КЗ(Zi)}$), а також ІС СП в цілому ($P_{КЗ(S)}$), див рис. 1 [1].

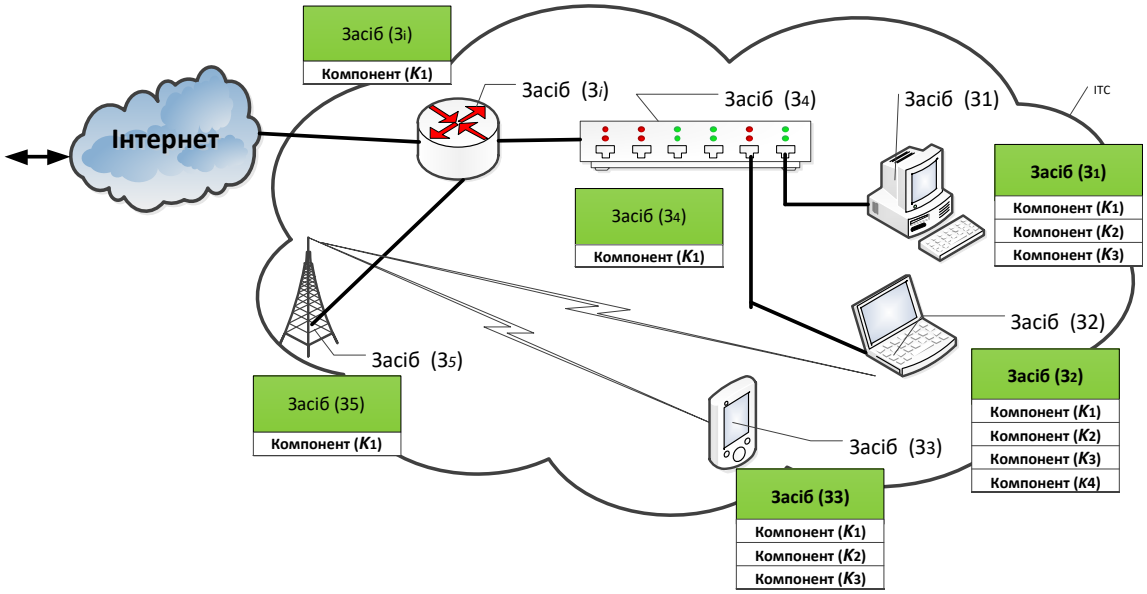

Рис. 1 Фрагмент умовної ІС СП

Аналіз останніх досліджень і публікацій. Аналіз останніх досліджень і публікацій за обраним напрямком досліджень представлено в наступних публікаціях.

В роботі [2] запропоновано, що посадовим особам, які відповідальні за кібернетичну безпеку ІТС (адміністративному персоналу) надається формальний апарат для кількісної оцінки поточного стану кібернетичної безпеки у будь-який момент на заданому часовому інтервалі, визначених кроків функціонування ІТС асоційованого з тривалістю періоду оновлення формалізованої бази шаблонів (правил, сигнатур) кібернетичних атак. Поряд з відносною простотою, наочністю, наявні особливості, а саме, що чисельні величини показників у складі приведених виразів мають сенс для визначення тільки у ході практичного моделювання, натурного експерименту чи практичної повсякденної роботи, як результат роботи відповідних автоматизованих функцій у складі програмного забезпечення діяльності адміністративного персоналу ІТС.

Запропонована методика [3], ґрунтується на методі анкетування, надає можливість одержати числову характеристику комплексного показника оцінки рівня кібербезпеки держави, значення якого дозволяє визначати необхідність розробки належних заходів щодо підвищення результативності власних систем кібернетичної безпеки. Однак не наводиться з допомогою якого математичного апарату досягається заданий результат.

Виходячи з суспільно важливої наукової задачі авторами у роботі [4] започатковано і обговорено єдиний підхід до побудови методики оцінки кібернетичної захищеності ІТС організації. Подальші наукові пошуки дозволили вибудувати методику оцінки кібернетичної захищеності системи зв'язку організації [5]. Вона також ґрунтувалася на методі експертного анкетування системних адміністраторів. Подальші вдосконалювання [6] дозволили розширити межі застосування методика, а саме для оцінки кібернетичної захищеності інформаційно-телекомунікаційного вузла зв'язку Збройних Сил України.

Слід зазначити що всі розглянуті методики [2 – 6] дозволяють здійснити розрахункову оцінку кібернетичної захищеності інформаційно-телекомунікаційного вузла зв'язку Збройних Сил України на деякий момент часу t_0, за якого активний деструктивний інформаційний вплив на ІС СП відсутній $F_{ДІВ} = 0$. Іншими словами методики дозволяють визначити рівень досягнення виконання політики безпеки на ІС СП, яка б гарантувала захист її від кібернетичних впливів з деякою ймовірністю, яка прямувала б до 1 за умови відсутності загрози нульового дня.

Таким чином, поза уваги вище перелічених методик лишається можливість обчислення (прогнозування) оцінки кібернетичної захищеності ІС СП на деякий момент часу $t_{ДІВ}$, за якого на ІС СП здійснюється активний кібернетичний ДІВ $F_{ДІВ} = 1$ в результаті чого втрачено деякий актив (Ак), або функціональність засобів (сервісів) W_{FZi}. Саме через відсутність в обігу понять актив організації, втрати цього активу та відсутності коефіцієнта функціональності засобів (сервісів) W_{FZi}, не можливо зрозуміти реальний зміст методики оцінки кібернетичної захищеності ІС СП, вибудувати математичний апарат її розрахунку, моделювати найгірші варіанти стану кібернетичної захищеності ІС СП в результаті настання загрози нульового дня.

Мета статті. Апробувати результат дисертаційного дослідження щодо удосконаленої методики діагностування кібернетичної захищеності ІС СП з урахуванням деструктивних кібернетичних впливів.

Виклад основного матеріалу.

Вихідні дані методики: $I_{Чкз}$ – часткові індикатори кібернетичної захищеності політики безпеки; Z_i – кількість засобів ІС СП; K_j – кількість компонентів у складі засобу (Z_i) ІС СП; W_{Zi} – ваговий коефіцієнт кожного засобу (Z_i) зі складу ІС СП; W_{KjZi} – ваговий коефіцієнт компонента (K_j) зі складу засобу (Z_i) ІС СП; W_{FZi} – коефіцієнти функціональності засобів (сервісів) (Z_i); W_{Fkj} – коефіцієнти функціональності компонентів (сервісів) засобу (K_j); W_{FS} – коефіцієнт функціональної працездатності всієї системи S, яка має виконувати цільову функцію за умов ДІВ; час (t_0, $t_{ДІВ1}$, …, $t_{ДІВn}$) контрольні часові точки вимірювань.

Необхідно знайти: $P_{КЗ(KjZi)}$ – показник (ймовірність) кібернетичної захищеності компонента (K_j) зі складу засобу (Z_i) ІС СП; $P_{КЗ(Zi)}$ – показники (ймовірність) кібернетичної захищеності засобу (Z_i) ІС СП; $P_{КЗ(S)}$ – показник (ймовірність) кібернетичної захищеності всієї ІС СП.

Прийняті обмеження:

Введемо наступні обмеження та припущення, що час t_0, - момент часу коли деструктивний інформаційний вплив відсутній ДІВ =0; час $t_{ДІВ1}$, …$t_{ДІВn}$ – момент часу фіксації дії деструктивного інформаційного впливу ДІВ ≠0.

В даній удосконаленій методиці використовується наступні методи випробувань: експериментально-розрахунковий, порівняльний.

Етап 1. Реалізація заходів з категоріювання та розкладання ІС СП на компоненти та елементи щодо вразливості кібернетичного впливу

1) складну ІС СП потрібно розкласти на: засоби (Z_i), а засоби на її компоненти (K_j);

2) експертна група уповноважених фахівців кібернетичної безпеки призначає наступні вагові коефіцієнти: для кожного засобу (Z_i) ІС СП складної системи (W_{Zi}); кожного компонента (K_j) кожного засобу (Z_i) ІС СП – W_{KjZi}; коефіцієнти функціональності засобів (сервісів) W_{FZi}. Коефіцієнт функціональності засобів (сервісів) W_{FZi} приймає значення [1, 0] (табл. 1).

Таблиця 1. Приклад підходу до формування коефіцієнта функціональності засобу

№ п/п	Індикатор реакції системи	Контрольний засіб фіксації функціональної роботи	Обсяг інформації	W_{FZi}
1.	відмова пристрою	Акт звірки конфігурації системи до і після кібернетичного впливу	вдала спроба (без компрометації)	0
			вдала спроба (з компрометацією)	0,5
			не вдала спроба (компрометація)	1

Перед початком розрахунку кібернетичної захищеності ІС СП визначається ваговий коефіцієнт кожного компонента (K_j) у кожному засобі (Z_i) ІС СП – W_{KjZi}.

Ваговий коефіцієнт – W_{KjZi} призначений врегулювати питання логічної важливості в порядку спадання компонентів у засобу (Z_i) ІС СП.

Вагові коефіцієнти розраховується згідно якісної шкали Сааті. Для цього необхідно здійснити експертну оцінку попарних порівнянь вагових значень компонентів (K_j).

Отримання коефіцієнтів важливості компонент W_{KjZi} здійснюється із використанням методу рангових оцінок [7; 8].

Чим більше ранг, тим більша вага компоненти W_{KjZi}, а сума всіх значень коефіцієнтів одного засобу (Z_i) ІС СП рівна 1, як наведено у виразі (4).

Для визначення коефіцієнтів експертами створюється матриця елементів W_{KjZi}, як відносна оцінка елемента за якісною шкалою Сааті [2].

Отримана матриця W_{KjZi} діагональна, симетрична, що дозволяє визначити елементи всіх рядків зі одним відомим. Важливість W_{KjZi} кожної компоненти оцінюється з позиції впливу на працездатність, кібернетичної захищеність та безпечний стан ІС СП.

Очевидно, що на абонентському терміналі, смартфоні найвищий W_{KjZi} присвоюється операційній системі (ОС) і найнижчий Bluetooth. Проте з точки функціональної важливості передача текстових або голосових повідомлень неможлива без працездатного радіотерміналу GSM, CDMA, Wi-Fi, Bluetooth. В той же час втрачається сенс при виході з ладу планшету або пошкодженні ОС (див. рис. 1).

Для врахування наслідків впливу активних кібернетичних впливів в розрахункові формули кібернетичної захищеності [5; 6] кожному засобу (Z_i) ІС СП в обов'язковому порядку вводиться коефіцієнт функціональності компонентів (сервісів) засобу W_{FKj}.

Етап 2. Розрахунок показників $P_{КЗ(KjZi)}$ – кібернетичної захищеності кожного компонента (K_j) зі складу засобу (Z_i) ІС СП.

1) визначаються найбільш критичні часткові індикатори кібернетичної захищеності ($I_{Чкз}$) з політики безпеки. Уточнений перелік часткових індикаторів ($I_{Чкз}$) для кожної кожного компонента (K_j) засобу (Z_i) ІС СП визначає експертна група уповноважених фахівців кібернетичної безпеки.

2) розподіляються часткові індикатори ($I_{Чкзі}$) за кожним компонентом (K_j) кожного засобу (Z_i) ІС СП;

3) перевіряються засоби (Z_i) ІС СП на відповідність налаштувань параметрів кібернетичної захищеності за частковими індикаторами.

Звірка здійснюється шляхом перевірки налаштувань кожного компонента (K_j) засобу (Z_i) ІС СП у відповідності з рекомендаціями об'єкта прийняття рішення (експертна група уповноважених фахівців кібернетичної безпеки) з переліком часткових індикаторів.

Частковий індикатор ($I_{Чкз}$) приймає вихідне значення "1" або "0" за наступних умов, якщо: налаштування компонента (K_j) засобу (Z_i) ІС СП відповідають політиці безпеці, тоді ($I_{Чкз}$) = "1", а в іншому випадку ($I_{Чкз}$) = "0" - налаштування компонента (K_j) засобу (Z_i) ІС СП не відповідають політиці безпеці. Кількість ($I_{Чкз}$) для різних компонентів засобів має різну кількість. Результати обчислювань заносяться до табл. 2.

Таблиця 2. Матриця показників часткових індикаторів $I_{\text{Чкз}i}$ для компонент (K_j) кожного засобу (Z_i) ІС СП

Компонента засобу	Значення показників часткових індикаторів ($I_{\text{Чкз}}$)					g_k
	1	2	3	…….	g_k	
Компонент №1 засобу №1	0	1	1	…….	0	g_1+g_0
Компонент №2 засобу №1	1	1	1		1	g_1+g_0
Компонент №3 засобу №1	1	0	0		0	g_1+g_0
Компонент №1 засобу №2	0	0	1		0	g_1+g_0
……	…..	……	….	……	……	g_1+g_0
Компонент №1 засобу №*N*	1	0	1	…….	0	g_1+g_0

Показник $P_{\text{КЗ}(KjZi)}$, обчислюємо за формулою (1):

$$P_{\text{КЗ}(KjZi)} = \frac{\sum_{i=1}^{k} g_1}{\sum_{i=1}^{k} (g_0 + g_1)} = \frac{\sum_{i=1}^{k} g_1}{g_k} \tag{1}$$

де g_k – кількість питання, що відповідають відповідній компоненті K_j; g_1– кількість індикаторів ($I_{\text{Чкз}}$), які приймає значення "1" для відповідної компоненти K_j; g_0– кількість індикаторів ($I_{\text{Чкз}}$), які приймає значення "0" для відповідної компоненти K_j.

Етап 3. Обчислення показника $P_{\text{КЗ}(Zi)}$ – кожного засобу (Z_i) зі складу ІС СП.

Показник кібернетичної захищеності $P_{\text{КЗ}(Zi)}$ обчислюється за формулою (2), як зважену та нормовану оцінку індикаторів стану кібернетичної захищеності всіх компонентів (j) кожного засобу (Z_i) ІС СП.

$$P_{\text{КЗ}(Zi)} = \frac{\sum_{j=1}^{m} \left(P_{\text{КЗ}(KjZi)} \times W_{Fkj} \times W_{KjZi} \right)}{\sum_{j=1}^{m} \left(W_{Fkj} \times W_{KjZi} \right)}, \tag{2}$$

де m – кількість компонентів (K_j) у кожному засобі (Z_i) ІС СП; W_{Fkj} – коефіцієнт функціональності компоненту (сервісу) (K_j) засобу (Z_i) ІС СП.

Результати обчислювань заносяться до табл. 3.

Таблиця 3. Результати обчислювань

№	Компоненти	K_1				K_j			$P_{\text{КЗ}(Zi)}$
		$P_{\text{КЗ}(K1Zi)}$	W_{FK1}	W_{K1Zi}	…	$P_{\text{КЗ}(K1Zi)}$	W_{FK1}	W_{K1Zi}	
1	Компонент №1 засобу №1				…				
2	Компонент №2 засобу №1								
..	……	…	…	…	…	….	…	…	..
К	Компонент №1 засобу №*N*								

Етап 4. Розрахунок $P_{\text{КЗ}(S)}$ – кібернетичної захищеності ІС СП в цілому.

Кількісним показником для оцінки кібернетичної захищеності складної системи є $P_{\text{КЗ}(S)}$ – ймовірність того, що в складній системі (ІС СП), всі її засоби та їх компоненти будуть захищені від кібернетичного втручання ДІВ та функціонуватимуть в штатному режимі.

Показник кібернетичної захищеності $P_{\text{КЗ}(S)}$ ІС СП загалом розраховується за формулою (3), як зважена та нормована оцінка показників стану кібернетичної захищеності всіх засобів складної системи:

$$P_{\text{КЗ}(S)} = \sum_{i=1}^{L} \left(P_{\text{КЗ}(Zi)} \times W_{FZi} \times W_{Zi} \right), \tag{3}$$

де L – кількість засобів (Z_i) у складі ІС СП;

Тоді, W_{FZi} коефіцієнт функціональності засобу (Z_i) ІС СП в цілому обчислюється за формулою (4):

$$W_{FZi} = \sum_{i=1}^{m} \left(W_{FKj} \right) \le 1, \tag{4}$$

де W_{Zi} – ваговий коефіцієнт засобу (Z_i) в складній системі ІС СП.

Результати обчислювань $P_{\text{КЗ}(S)}$ заносяться до табл. 4.

Таблиця 4. Результат розрахунку показників $P_{КЗ(S)}$ кібернетичної захищеності ІС СП в цілому

Засоби З *i*	$P_{КЗ(Zi)}$	W_{FZi}	W_{Zi}	$P_{КЗ(S)}$
Засіб №1				Формула (3)
Засіб №2				
Засіб №3				
……..	……..	…….	……	
Засіб №N				

Етап 5. Обробка, аналіз та оцінка результатів випробувань.

Методи контролю за дослідним зразком складної системи:

зовнішній огляд за системою оповіщення про інциденти (при її наявності);

проведення вимірювань швидкості передачі файлів (відео, графічних, текстових матеріалів);

проведення розбірливості голосових повідомлень;

зовнішній огляд стану зразку у випадку здійснення на нього кібернетичного впливу.

Критерії, при виконанні яких фрагмент випробувальної ІС СП вважається таким, що витримав випробування. Оцінка здійснюється на всіх етапах випробувань. ІС СП вважається такою, що пройшла перевірку випробування на кібернетичну захищеність, якщо за результатами розрахунку кібернетичної захищеності станом на час (t_0, $t_{ДІВ1}$, $t_{ДІВ2}$) задовольнило критерії табл. 5.

Таблиця 5. Критерії кібернетичної захищеності

№ п/п	$P_{КЗ(S)}$	Рівень кібернетичної захищеності	Кольорове трактування
1	$0,75 \le P_{КЗ(S)} \le 1$	високий	зелена
2	$0,4 \le P_{КЗ(S)} \le 0,75$	середній	жовта
3	$0 \le P_{КЗ(S)} \le 0,4$	низький	червона

Опис постановки експериментальної частини реалізації методики діагностування кібернетичної захищеності інформаційної системи з урахуванням деструктивних кібернетичних впливів

Етап 1. Реалізація заходів з категоріювання та розкладання ІС СП на компоненти та елементи щодо вразливості кібернетичного впливу.

1) Керівник комісії з перевірки кібернетичної захищеності формує наступні групи фахівців за напрямками та відповідальністю:

група №1 фіксації зміни стану функціонування ІС СП підчас діагностування;

група №2 створення ДІКВ – відпрацювання умовних дій в ролі «хакера»;

група №3 розрахунку – розраховують кібернетичну захищеність ІС СП на всіх етапах діагностування;

група №4 умовні користувачі (АРМ ІС СП), здійснюють фіксацію передачі голосових, текстових, графічних даних, відео потоку. Здійснюють інструментальне діагностування, вимірювання, оцінювання кількісних та якісних показників.

Порядок взаємодії учасників випробувань за даною методикою:

фахівці контролю та фіксації безпосередньо з групою розрахунку;

керівник випробувань через команду здійснення ДІКВ з – умовним хакером.

Забороняється: особам, що здійснюють кібернетичний вплив (№2) повідомляти початок настання події ДІКВ групі №1.

2) розкласти складну систему (ІС СП), яка визначена на тестування на наступні складові:

на засоби (Z_i) ІС СП;

на компоненти (K_j) засобу (Z_i) ІС СП;

3) розподілити і закріпити перелік часткових індикаторів ($I_{Чкз}$) за кожною компонентою (K_j) кожного засобу (Z_i) ІС СП;

4) призначити вагові коефіцієнти:

кожному засобу (Z_i) ІС СП (W_{Zi});

кожній компоненті (K_j) кожного засобу (Z_i) ІС СП – W_{KjZi};

функціональності W_{FZi}, W_{Fkj};

5) розрахувати станом на момент часу (t_0) «відсутні деструктивного інформаційного впливу» числове значення кібернетичної захищеності:

кожного компонента (K_j) зі складу засобу (Z_i) ІС СП – $P_{КЗ(KjZi)}$;

кожного засобу (Z_i) ІС СП $P_{КЗ(Zi)}$;

всієї складної ІС СП – $P_{КЗ(S)}$;

6) результат розрахунку комісія заноситься до таблиці порівнянь стану кібернетичної захищеності протоколу випробувань та здійснити оцінку відповідності стану кібернетичної захищеності ІС СП станом на момент часу (t_0).

7) оперативна нарада за результатами підготовчого етапу методики. Постановка завдання на відпрацювання першого етапу методики випробувань.

Етап 2. Розрахунок $P_{КЗ(S)}$ – кібернетичної захищеності ІС СП в цілому станом на (t_0) за етапами 2-5.

Етап 3. Розрахунок числового значення кібернетичної захищеності ІС СП станом на момент часу ($t_{ДІВ1}$) за результатами «активної фази ДІВ»:

1) за командою керівника випробувань група №2 здійснює «активну фазу ДІВ» на складну систему із зазначенням часу ($t_{ДІВ1}$).

2) група №1 переходить в посилений режим очікування;

3) група №3 працює в штатному режимі. З надходженням вихідних результатів від групи № 1 про зміни стану системи або реакції, приступають до обчислювань кібернетичної захищеності;

4) з настанням часу ($t_{ДІВ1}$), групи №2 за допомогою набору СПЗ здійснює:

рекогносцировку мережевого обладнання;

отримання IP-адресу для роботи в мережі;

аналіз вразливостей;

злом шляхом складання словників злому для підбору імен, облікових записів і паролів до них;

злом та проникнення до системи;

проводить Ddos-атаку.

За результатами сканування мережевого обладнання та отриманих вихідних даний здійснює санкціоновані (з позиції дозволених) кібернетичні втручання (впливи) для досягнення мети.

5) перевіряється (відслідковується):

групою №1 за допомогою функціонування штатної системи фіксації, контролю та оповіщення про зміни стану компоненти засобу(ів), зміни функціонування засобу(ів) або всієї складної ІС СП. Результати контролю надаються групі №3 у формі вихідних даних (час настання події ($t_{кв1ф}$), засіб, компонента засобу, загроза чи інше) та рекомендовані значення коефіцієнта функціональності – W_{FZi}, W_{Fkj};

групою №4 за допомогою інструментальних засобів оцінюють функціональні зміни стану компоненти засобу(ів), зміни функціонування засобу(ів) та надають пропозиції щодо W_{Fkj} відповідної компоненти засобу(ів), зміни функціонування засобу(ів) в залежності від реакції на кібернетичне втручання. Відбувається фіксація фактичного часу настання події зміни функціонування компоненти засобу(ів) або зміни функціонування всього засобу(ів) ($t_{ДІВ1фзф}$);

6) група №3 здійснює:

Розрахунок за методикою числового значення кібернетичної захищеності всієї ІС СП $P_{КЗ(S)}$ станом на час ($t_{ДІВ1ф}$);

результати обчислювань заносяться до таблиці порівнянь стану кібернетичної захищеності в протоколі випробувань із зазначенням часу ($t_{ДІВ1ф}$).

7) Здійснити оцінку:

відповідності стану кібернетичної захищеності ІС СП станом на момент ($t_{ДІВ1}$)

порівняти час реакції системи оповіщення про настання кібернетичних інцидентів ($t_{ДІВ1}$) з ($t_{ДІВ1ф}$), та ($t_{ДІВ1фзф}$). Він має бути ($t_{ДІВ1}$) ≈ ($t_{ДІВ1ф}$) ≈ ($t_{ДІВ1фзф}$) в межах прийнятної норми (згідно формуляру, техпаспорту);

часу затраченого на проведення проникнення і злому.

На всіх етапах перевірки групи №1-4 здійснюють фіксацію змін технічного стану та відхилення від нормального функціонування, як окремих складових (компонентів засобів) так і засобів в цілому та системи в цілому.

Таким чином: в запропонованій методиці на відміну від методик [2 – 6] можливо здійснити розрахункову оцінку кібернетичної захищеності ІТС на деякий момент часу $t_{ДІВ}$, за якого здійснено активний кібернетичний вплив на цю систему $F_{ДІВ} = 1$ в результаті чого, організація може втратити деякий актив (Ак); математичний апарат методики забезпечує розрахунок кібернетичної захищеності складної системи (ІС СП) для моделі найгіршого варіанту настання події загрози нульового дня.

Складання переліку часткових індикаторів діагностування кібернетичної захищеності компонентів ІС СП

Одним з відповідальних завдань, що покладається на експертну групу уповноважених фахівців кібернетичної безпеки є складання актуального та адекватного переліку часткових індикаторів.

Кількість ($I_{\text{чкз}}$) для різних компонентів засобів (З*і*) має різну кількість.

В дисертаційній роботі пропонується складати перелік часткових індикаторів кібернетичної захищеності компонентів для трьох рівнів захищеності, а в сукупності за допомогою всіх трьох констатувати максимальний рівень захищеності.

В роботі при розробці індикаторів діагностування кібернетичної захищеності інформаційної системи використано найкращі практики Nist, DoD та у відповідності до вимог Інструкції Міністерства оборони США "Cybersecurity Activities Support to DoD Information Network Operations" від 07.03.2016 № 8530.01, Cyber incident handling program. Chairman of the joint chiefs of staff manual CJCSM 6510.01B. 10 July 2012.

Загальні відомості про перелік групових індикаторів діагностування різного рівня стану кібернетичного захисту ІС СП подано у зведеній табл. 6.

Зазначені переліки часткових індикаторів діагностування кібернетичної захищеності компонентів розроблено і практично апробовано в рамках розробки програми та методики визначальних відомчих випробувань засобів широкосмугового мультисервісного радіодоступу мережі McWiLL на замовленні МО України.

Таблиця 6. Загальні відомості про перелік групових індикаторів діагностування різного рівня стану кібернетичного захисту ІС СП

Перелік питань / Часткові індикатори кібернетичної захищеності	Рівень кібернетичної захищеності		
	Низький	Середній	Високий
Перелік групових індикаторів діагностування початкового рівня стану кібернетичного захисту інформаційної	+	–	–
група питань №1 Вимоги з організаційного захисту інформаційної системи	+	–	–
група питань №2 Виконання вимог з технічного захисту інформаційної системи від витоків по акустичному каналу інформації про керування прав до доступу (адміністрування)	+	–	–
група питань №3 Виконання вимог з технічного захисту інформаційної системи від витоку візуальної інформації про керування прав до доступу (адміністрування)	+	–	–
група питань №4 Виконання вимог з технічного захисту від загроз викрадення носіїв матеріальних інформації	+	–	–
група питань №5 Виконання вимог з організації та спроможності забезпечення захищеності інформаційної системи шляхом розмежування прав доступу	+	–	–
група питань №6 Виконання вимог з захищеності інформаційної системи від заходів розвідки інфраструктури	+	–	–
група питань №7 Виконання вимог з захищеності інформаційної системи від заходів кібернетичного впливу на функціонування інфраструктури	+	–	–
група питань №8 Виконання вимог з захищеності інформаційної системи від заходів кібернетичного впливу на функціонування інфраструктури шляхом застосування системи захисту інфраструктуру	+	–	–
група питань №9 Виконання вимог з виконанню вимог з програмного захисту	+	–	–
група питань №10 Діагностування моделі внутрішнього і зовнішнього порушника.	+	–	–
Перелік групових індикаторів діагностування середнього рівня стану кібернетичного захисту інформаційної системи	–	+	–
група питань №1. Індикатор оцінки та аналізу вразливостей	–	+	–
група питань №2. Індикатор керування вразливостями	–	+	–
група питань №3. Індикатор захищеності від шкідливого програмного забезпечення	–	+	–

група питань №4. Індикатор моніторингу безпеки інформації	–	+	–
група питань №5. Індикатор обробки кіберінцидентів	–	+	–
група питань №6. Індикатор моніторингу інсайдерської діяльності користувачів	–	+	–
група питань №7. Індикатор попередження мережевої розвідки	–	+	
Перелік групових індикаторів діагностування високого рівня стану кібернетичного захисту інформаційної системи	–	–	+
група питань №1. «Авторизація неавторизованих та авторизованих мережевих пристроїв»	–	–	+
група питань №2. «Авторизація неавторизованого та авторизованого програмного забезпечення»	–	–	+
група питань №3. «Безпечна конфігурація для апаратного та програмного забезпечення»	–	–	+
група питань №4. «Безперервна оцінка вразливостей та їх виправлення»	–	–	+
група питань №5. «Контроль використання адміністративних привілеїв»	–	–	+
група питань №6. «Контроль документування подій в ІТС»	–	–	+
група питань №7. «Захист електронної пошти та веб-браузерів»	–	–	+
група питань №8. «Захист від шкідливого програмного забезпечення»	–	–	+
група питань №9. «Обмеження та контроль мережевих портів, протоколів та сервісів»	–	–	+
група питань №10. «Можливість відновлення даних»	–	–	+
група питань №11. «Безпечні конфігурації для мережевого обладнання»	–	–	+
група питань №12. «Захист мережевого периметру»	–	–	+
група питань №13. «Захист даних»	–	–	+
група питань №14. «Контрольований доступ»	–	–	+
група питань №15. «Контроль бездротового доступу»	–	–	+
група питань №16. «Моніторинг та управління обліковими записами»	–	–	+
група питань №17. «Відпрацювання навичок з інформаційної безпеки та проведення тренінгів для усунення недоліків»	–	–	+
група питань №18. «Захист прикладного програмного забезпечення»	–	–	+
група питань №19. «Настанова з реагування на інциденти»	–	–	+
група питань №20. «Тести на проникнення»	–	–	+

Загальні відомості щодо практичної реалізації методики розрахунок кібернетичної захищеності складної системи у формі спеціалізованого програмного забезпечення

Практична реалізація у вигляді спеціалізованого програмного забезпечення (СПЗ) методики забезпечує розрахунок кібернетичної захищеності складної системи, а саме для інформаційно-телекомунікаційної системи було виконано в контексті виконання доручення Начальника військ зв'язку Збройних Сил України – начальника Головного управління Зв'язку та інформаційних систем Генерального штабу Збройних Сил України Військовому інституту телекомунікацій та інформатизації на виконання оперативного завдання на проведення дослідження на тему «Комплексна методика оцінки ефективності функціонування системи зв'язку Збройних Сил України за основними характеристиками» в частині що стосується розробки «Методика оцінки показника кіберзахищеності, як складової стійкості системи зв'язку Збройних Сил України» від 25.11.2016. З метою покращення якості впровадження результатів теоретичних досліджень у практику та застосування військ (сил), зниження впливу негативних умов і факторів на організацію проведення досліджень на заходах оперативної та бойової підготовки, а також розвиток методичної бази, що застосовується під час досліджень на заходах оперативної та бойової підготовки Збройних Сил України тому методика експериментально перевірялася на дослідження на військових навчаннях під час стратегічного командно-штабному

навчанні з органами військового управління, військами (силами) Збройних Сил України "Непохитна стійкість – 2017" в період з 11.09.2017 по 26.09.1017 р. офіцерами-дослідниками Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації та підтвердили задовільний характер.

Висновки. Найважливішими науковими й практичними результатами дослідження стали:

1. Удосконалено методику діагностування кібернетичної захищеності інформаційної системи спеціального призначення. В запропонованій методиці на відміну від відомих забезпечено здійснити розрахункову оцінку кібернетичної захищеності інформаційної системи спеціального призначення на деякий момент часу $t_{\text{ДІВ}}$, за якого здійснено активний деструктивний інформаційно-кібернетичний вплив на цю систему $F_{\text{ДІВ}} = 1$ з метою прогнозування і запобігання втратити деяких актив (Ак). Математичний апарат методики забезпечує розрахунок кібернетичної захищеності інформаційної системи спеціального призначення для моделі найгіршого варіанту настання події загрози нульового дня.

2. Надано практичні рекомендації щодо підходу з визначення коефіцієнтів функціональності компонентів складної інформаційної системи спеціального призначення які вразливі деструктивним інформаційним та кібернетичним впливом.

Перспективи подальших досліджень доцільно зорієнтувати на обґрунтуванні методики діагностування кібернетичної стійкості функціонування інформаційної системи спеціального призначення в кібернетичному просторі.

Список бібліографічного опису

1. Козубцов І.М., Козубцова Л.М. Постановка завдання на розробку методики оцінки кібернетичної захищеності інформаційно-телекомунікаційної системи. *Міжнародна науково-практична конференція «Спільні дії військових формувань і правоохоронних органів держави: проблеми та перспективи»* (м. Одеса 12-13 вересня 2019 р.) Військова академія, 2019. С. 228 – 229.

2. Хусаінов П.В. Показник кібернетичної безпеки автоматизованої системи у часі. *Збірник наукових праць ВІТІ.* Київ, 2015. Вип. № 1. С. 101 – 111.

3. Кудінов В.А. Методика оцінки рівня кібербезпеки в Україні. *Матеріали всеукраїнської науково-практичної конференції „Кібербезпека в Україні: правові та організаційні питання"*(Одеса, 21 жовтня 2016). Одеса. С. 151 – 152.

4. Черноног О.О., Козубцов І.М., Куцаєв В.В., Козубцова Л.М., Терещенко Т.П. Обговорення єдиного підходу до побудови методики оцінки кібернетичної захищеності ІТС організації. *Міжнародна науково-практична конференція "Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку"* (14-15 березня 2018 року). – Харків. Національна академія Національної гвардії України, 2018. С. 15 – 16.

5. Козубцов І.М., Козубцова Л.М., Куцаєв В.В., Терещенко Т.П. Методика оцінки кібернетичної захищеності системи зв'язку організації. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2018. №1 (31). С. 43 – 46.

6. Куцаєв В.В., Радченко М.М., Козубцова Л.М., Терещенко Т.П. Методика оцінки кібернетичної захищеності інформаційно-телекомунікаційного вузла зв'язку. *Збірник наукових праць ВІТІ.* К.: ВІТІ, 2018. № 2. С. 67 – 76.

7. Ротштейн А.П. Интеллектуальные технологии идентификации: нечеткие множества, генетический алгоритм, нейронные сети. *Винница: УНИВЕРСУМ*, 1999. 320 с.

8. Хусаінов П.В. Методика визначення раціональної послідовності надання інформаційних повідомлень оператору системи захисту. *Збірник наукових праць ВІТІ НТУУ „КПІ"*. Київ, 2006. Вип. № 3. С. 148 – 155.

References

1. Kozubov I. M., Kozubova L. M. (2019) Statement of the problem to develop methods for the assessment of cyber security in information and telecommunication systems. International scientific and practical conference "Joint actions of military formations and law enforcement agencies of the state: problems and prospects" (Odessa, September 12-13, 2019) Military Academy, Pp. 228 – 229.

2.Khusainov P. V. (2015) Indicator of cybernetic security of an automated system in time. Collection of scientific works of VITI. Kiev. Vol. # 1. Pp. 101 – 111.

3. Kudinov V. A. (2016) Methodology for assessing the level of cybersecurity in Ukraine. Materials of the all-Ukrainian scientific and practical conference "Cybersecurity in Ukraine: legal and organizational issues"(Odessa, October 21, 2016). Odessa. Pp. 151 – 152.

4. Chernonog O. O., Kozubtsov I. M., Kutsaev V. V., Kozubtsova L. M., Tereshchenko T. P. (2018) Discussion of a unified approach to the construction of a methodology for evaluating the cybernetic security of an organization's its. International scientific and practical conference " application of information technologies in the training and activities of law enforcement forces" (March 14-15, 2018). – Kharkov. National Academy of the National guard of Ukraine. Pp. 15 – 16.

5. Kozubtsov I. M., Kozubtsova L. M., Kutsaev V. V., Tereshchenko T. P. (2018) Methods for evaluating the cybernetic security of the organization's communication system. Modern information technologies in the field of security and defense. No. 1 (31). Pp. 43 – 46.

6. Kutsaev V. V., Radchenko M. M., Kozubtsova L. M., Tereshchenko T. P. (2018) Methods for evaluating cybernetic security of an information and telecommunications node. Collection of scientific works of VITI. K: VITE. Vol. # 2. Pp. 67 – 76.

7. Rotshtein A. p. Intelligent identification technologies: fuzzy sets, genetic algorithm, neural networks. Vinnytsia: UNIVERSUM, 1999. 320 p.

8. Khusainov P. V. (2006) Method of determining the rational sequence of providing information messages to the operator of the protection system. Collection of scientific works of VITI NTUU "KPI". Kiev. Vol. # 3. Pp. 148 – 155.