УДК 004.7.056 **doi: 10.32620/reks.2020.1.02**

С. М. ЛИСЕНКО[1], В. С. ХАРЧЕНКО[2], К. Ю. БОБРОВНІКОВА[1], Р. В. ЩУКА[1]

[1] ***Хмельницький національний університет, Україна***
[2] ***Національний аерокосмічний університет ім. М. Є. Жуковського "Харківський авіаційний інститут", Україна***

РЕЗИЛЬЄНТНІСТЬ КОМП'ЮТЕРНИХ СИСТЕМ В УМОВАХ КІБЕРЗАГРОЗ: ТАКСОНОМІЯ ТА ОНТОЛОГІЯ

Стрімкий розвиток інформаційних технологій призвів до розширення можливостей кіберзагроз щодо комп'ютерних систем (КС). Кіберзлочинці розробляють нові способи уникнення виявлення атак, тому існуючі підходи не в змозі протистояти зростаючій загрозі атак. Тим часом наслідки кібератак стають більш небезпечними та руйнівними. Одним із підходів до вирішення проблеми є побудова резильєнтних систем, які здатні швидко відновлюватися та продовжувати функціонувати в умовах здійснення атак. ***Предметом*** *дослідження є процес побудови резильєнтних комп'ютерних систем в умовах кіберзагроз.* ***Метою*** *є розроблення таксономії та онтології резильєнтних комп'ютерних систем в умовах кіберзагроз.* ***Результати.*** *У статті представлені визначення поняття резильєнтності з точки зору кібкрбезпеки, представлено зв'язок понять резильєнтності з гарантоздатністю. В роботі представлено основні елементи таксономічної схеми резильєнтності КС, до яких належать загрози (зміни середовища та вимог, мережні атаки, атаки на ПЗ, вразливості програмного та апаратного забезпечення, помилки, відмови, впливи), інформаційно-технічні стани, які КС проходить протягом свого операційного циклу, принципи, на яких базується резильєнтність (проактивність, адаптивність, стійкість до втручань, диверсність, еластичність, керована деградація, захист в глибину, здатність до еволюції), а також первинні та вторинні властивості. На основі вищевказаних елементів розроблено узагальнену таксономічну схему резильєнтності, пов'язану з інформаційною безпекою. В роботі подано операційний цикл резильєнтної КС як множину інформаційно-технічних станів, які проходить система (підготовка, захист системи, виявлення загроз, поглинання загроз, відповідь на загрозу, відновлення системи після здійснення кібератаки, адаптація). Розроблено схему онтології резильєнтності з точки зору інформаційної безпеки комп'ютерних систем в умовах кіберзагроз.* ***Висновки****. Розроблено таксономію та онтологію резильєнтних комп'ютерних систем в умовах кіберзагроз.*

Ключові слова: *резильєнтність; кіберзагроза; кібератака; виявлення бот-мереж; захист мережі; самоадаптивні системи; сценарій безпеки; зловмисне програмне забезпечення; DDoS-атака.*

Вступ. Проблема побудови резильєнтних комп'ютерних систем в умовах кіберзагроз

Сьогодні кіберзлочинці знаходять нові способи отримання прибутку від підприємств, які є об'єктом вимагання та прибутковим джерелом доходу для організованих злочинних груп через приватну інформацію, що зберігається та обробляється цими установами. Різні види кіберзагроз є потужним інструментом, який використовується кіберзлочинцями для вчинення зловмисних дій [1].

Стрімкий розвиток інформаційних технологій призвів до значного розширення можливостей кіберзагроз при запуску атак на відмову в обслуговуванні, інфікування мільйонів комп'ютерних систем (КС) шкідливим кодом, викраденні конфіденційних даних, розсилання масштабного спаму, шантажу і вимагання. Кіберзагрози можуть використовувати комбінації декількох атак, що використовують відомі та невідомі вразливості кінцевих пристроїв [2].

Кіберзлочинці розробляють нові способи уникнення сучасних методів виявлення атак, тому існуючі підходи не в змозі протистояти зростаючій загрозі атак. Тим часом наслідки кібератак стають все більш небезпечними та руйнівними.

Описана ситуація активізує розробку нових підходів, здатних виявляти, запобігати та пом'якшувати кібератаки на мережі. Крім того, дуже важливо забезпечити стабільне функціонування КС в умовах атак. Одним із способів вирішення цієї проблеми є побудова резильєнтних систем, які здатні швидко відновлюватися та продовжувати функціонувати в умовах здійснення атак [3].

Мета роботи. Відповідно до цього метою даної роботи є побудова таксономічних схем та онтології резильєнтності комп'ютерних систем в умовах здійснення кібератак. Структурно вона складається з

© С. М. Лисенко, В. С. Харченко, К. Ю. Бобровнікова, Р. В. Щука, 2020

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

трьох розділів: у першому розділі подано суть поняття резильєнтності, походження та сфери використання; у другому розділі пропонується таксономія резильєнтності КС в умовах кіберзагроз; у третьому розділі представлено онтологічну схему резильєнтності з точки зору інформаційної безпеки. У висновках сформульовано напрями подальших досліджень у розробленні резильєнтних комп'ютерних систем в умовах здійснення кібератак.

1. Поняття резильєнтності

Поняття резильєнтності було широко досліджено в багатьох контекстах, і деякі з цих досліджень вже застосовуються до критичних інфраструктур. Наприклад, в екологічному контексті [4] резильєнтність – це властивість популяції, яку можна розглядати з точки зору властивостей рівноваги та коливань, обумовлених збуреннями системи. Аналогічне трактування застосовано в економіці [5]. Конструкція будівель включає властивість резильєнтності протистояти катастрофам [6]. В контексті захисту критичної інфраструктури резильєнтність систем представлено в [7].

Слово «резильєнтність» походить від латинського слова «resiliere», що означає «відскочити назад». Загальне вживання слова резильєнтність передбачає здатність суб'єкта чи системи повернутися до нормального стану після настання події, яка порушує її нормальний стан. Таке широке визначення стосується різноманітних галузей, таких як екологія, матеріалознавство, психологія, економіка та інженерія. Запропоновано деякі загальні визначення резильєнтності, які охоплюють різні дисципліни. Наприклад, у [8] резильєнтність визначено як «здатність системи підтримувати своє функціювання та структуру в ситуації внутрішніх і зовнішніх змін і знижувати продуктивність системи, коли це необхідно». В [9] резильєнтність визначено як «міру здатності системи поглинати постійні та непередбачувані зміни і все ще підтримувати свої життєво важливі функції». В [10] резильєнтність визначено як «здатність системи витримувати великі порушення в межах прийнятних параметрів деградації та відновлення з відповідним часом та розумними витратами та ризиками». Резильєнтність до стихійних лих характеризується безпекою інфраструктури [11] як здатність запобігати чи захищати від значних загроз та інцидентів, пов'язаних з різними небезпеками, включаючи терористичні напади, та відновлювати критичні служби з мінімальними руйнуваннями для безпеки та здоров'я населення. В [12] резильєнтність системи визначається наступним чином: «З огляду на виникнення певної руйнівної події (або набору подій), резильєнтність системи щодо цієї події (або подій) – це здатність системи ефективно знижувати величину і тривалість відхилення від цільових рівнів продуктивності системи».

Необхідно відзначити два важливих елементи цього визначення:

- негативний вплив на систему (зміна в системі), що призводить до дестабілізації у функціонуванні системи і вимірюється різницею між цільовим та поточним рівнем продуктивності системи в умовах здійснення негативного впливу;
- загальні зусилля відновлення та ресурси, витрачені на відновлення системи, що зазнала такого впливу чи зміни.

Хоча існують різні інтерпретації поняття, в роботі резильєнтність розглядається з точки зору визначення, що ґрунтується на основі поняття гарантоздатності комп'ютерних систем, яке була запропоноване в [13] і описане в [14]: резильєнтність системи використовується для визначення здатності системи стабільно надавати свої послуги в надійний спосіб навіть при зовнішніх та внутрішніх змінах системи.

З точки зору кібербезпеки резильєнтність – це здатність передбачати, протистояти, відновлюватись та пристосовуватися до несприятливих умов, зовнішніх впливів, атак чи порушення нормального функціонування системи [15-18].

2. Таксономія резильєнтності комп'ютерних систем в умовах кіберзагроз

2.1. Зв'язок поняття резильєтності з гарантоздатністю

Резильєнтність – це еволюція концепції гарантоздатності, яка фокусується на вивченні впливу змін на надійність системи [19]. Зміна є широким терміном, який може розглядатися по-різному в різних сферах. Зміни можуть бути систематизовані відповідно до їх характеру, перспективи і часу [20]:

- природа: функціональна, інфраструктурна або технологічна;
- перспектива: передбачені, передбачувані, непередбачені зміни;
- час: короткострокові (наприклад, від секунди до годин), середньострокові (наприклад, від години до місяців) і довгострокові зміни (наприклад, від місяця до років).

Резильєнтність розширює концепцію гарантоздатності, акцентуючи необхідність створення систем, які є гнучкими і адаптивними. Вона вимагає впровадження передових механізмів реконфігурації та гнучких стратегій для ефективного використання

компонентів системи, щоб впоратися зі змінами та допускати несправності [21].

Оскільки резильєнтність є еволюцією поняття гарантоздатності, то більшість її понять та принципів ґрунтуються на класичних визначеннях, пропонованих для гарантоздатності, які розглядаються далі. Гарантоздатність є однією з основних вимог, яка застосовується до комп'ютерних систем. Вона може бути визначена як здатність системи надавати послуги, яким можна довіряти [22, 23]. Гарантоздатність є інтегрованою концепцією, яка включає такі ключові атрибути, як:

- готовність (availability): можливість системи надавати послугу в будь-який момент часу;
- безвідмовність (reliability): здатність системи надавати послугу протягом визначеного проміжку часу;
- функційна безпека (safety): можливість системи до надання послуг у заданих умовах без катастрофічних наслідків для користувачів і зовнішнього середовища;
- цілісність (integrity): відсутність неналежної зміни системи;
- обслуговуваність (maintainability): здатність системи бути відновленою до стану, в якому вона може правильно надавати послуги;
- конфіденційність (confidentiality): відсутність несанкціонованого розголошення інформації.

Різні загрози можуть спричинити небажані відхилення у функціонуванні системи і таким чином знижувати її гарантоздатність, а, значить, і резильєнтність. Традиційно загрози класифікують за наступними категоріями: *відмови*, *помилки* і *дефекти*, а розроблення гарантоздатних систем ґрунтується на чотирьох основних підходах: *запобігання несправностей* (fault prevention), *видалення несправностей* (fault removal), *прогнозування несправності* (fault forecasting) та відмовостійкості (fault tolerance).

2.2. Узагальнена таксономічна схема резильєнтності

Основними елементами таксономічної схеми резильєнтності КС є загрози T (зміни середовища та вимог, мережні атаки, атаки на ПЗ, вразливості програмного та апаратного забезпечення, помилки, відмови, впливи), інформаційно-технічні стани S, які КС проходить протягом свого операційного циклу; принципи T, на яких базується резильєнтність; а також первинні P_1 та вторинні P_2 властивості.

Атаки A (мережного типу $A_{net} \in A$ або атаки на програмне забезпечення $A_{soft} \in A$) призводять до порушень та помилок E функціонування комп'ютерних систем, які спричиняють відмову F та при яких КС переходять у непрацездатний або частково непрацездатний (деградований) стан. Таким чином, маємо ланцюги:

$$\begin{aligned} A_{net} &\rightarrow E \rightarrow F; \\ A_{soft} &\rightarrow E \rightarrow F. \end{aligned} \qquad (1)$$

Внаслідок впливу загроз змінюється інформаційно-технічний стан S комп'ютерної системи, коли або порушується цілісність інформації, або зовнішнє середовище (інша система) несанкціановано отримує доступ до неї.

Поняття резильєнтності КС в умовах здійснення кібератак таксономічно розширюється такими принципами, на яких вона базується [24-30]:

- проактивність (proactivity);
- адаптивність (adaptability);
- стійкість до втручань (resistance);
- диверсність (diversity);
- еластичність (plasticity);
- керована деградація (controlled degradation);
- захист в глибину (defense in depth);
- здатність до еволюції (evaluability).

Значна частина інформаційної безпеки базується на *проактивності*, *адаптивності* та *стійкості до втручань* системи при атаках. Якщо система захищена належним чином, то рівень ризику зменшується, і, таким чином, ймовірність події збитку також знижується. Якщо відбудеться невідома атака, то належним чином загартована система буде більш стійкою до дій атаки (зловмисника), який проник у систему або її скомпрометував.

Аналогічно можна *протистояти* діям зловмисника, ускладнивши завдання здійснення атаки на систему. *Диверсність* (*diversity*) компонентів системи та їх побудови (наприклад, операційна система, мова програмування, канал доступу) вимагає від зловмисника сформулювати декілька стратегій атаки. Модульність в системі дозволяє здійснювати конфігурацію та заміну компонентів, не вимагаючи змін в інтерфейсі між ними, тим самим забезпечуючи більшу диверсність. *Диверсність*, як правило, створює рівень накладних витрат для адміністраторів і може не підходити для всіх ситуацій, однак у складних сучасних системах є здійсненною та виправданою.

Еластичність і *керована деградація* дозволяють системі зменшувати продуктивність без повного руйнування. Такі поняття, як надлишкові компоненти, надлишок обробної або комунікаційної спроможності та уникнення одиночних точок відмови є загальними способами, що дозволяють системі *поглинати* несподівані події, продовжуючи надавати принаймні мінімально прийнятний рівень обслуговування. *Керована деградація* – це концепція того,

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

що система може бути попередньо налаштована з набором послідовно менш функціональних станів, які представляють прийнятні компроміси між продовженням функціональності та забезпеченням параметрів безпеки.

Захист в глибину (defense in depth) – це підхід до забезпечення резильєнтності КС в умовах атак, в якому ряд захисних механізмів шаруються для захисту цінних даних та інформації. Якщо один механізм не забезпечує захист, то залучається інший, щоб запобігти атаці. Цей багатошаровий підхід підвищує безпеку системи в цілому і стосується багатьох різних векторів атак.

Розроблення резильєнтних систем обов'язково повинне включати здатність до їх *еволюції* таким чином, щоб врахувати досвід попередніх атак і мати можливість внесення необхідних структурних, архітектурних чи інших змін в систему, що дозволить зменшити вразливість та підвищити стійкість до потенційних майбутніх атак.

Узагальнена таксономічна схема резильєнтності, пов'язана з інформаційною безпекою, подана на рис. 1.

2.3. Операційний цикл резильєнтної комп'ютерної системи

Для забезпечення резильєнтного функціонування КС в умовах атак система повинна [31-34]:

- бути підготовленою до можливих атак (be prepared);
- бути захищеною (be protected);
- мати здатність до виявлення атак (able to detect attacks);
- мати здатність протистояння атакам (able to respond / adsorb attacks);
- бути адаптивною (be adaptable);
- бути відновлюваною (be recoverable).

Приймемо кібератаку A множиною деструктивних дій a_m щодо системи C_i, $A = \{a_m\}_{m=1}^{N_m}$, тоді операційний цикл резильєнтної КС в умовах кібератак подамо множиною інформаційно-технічних станів, які проходить система (рис. 2):

$$S = \{s_{prep}, s_{prot}, s_{detect}, s_{absorb}, s_{respond}, s_{recovery}, s_{adapt}\}, \quad (2)$$

де s_{prep} – підготовка (прогнозування, попередження) до функціонування системи в умовах кібератак; s_{prot} – захист системи; s_{detect} – виявлення атаки; s_{absorb} – поглинання атаки; $s_{respond}$ – відповідь на атаку; $s_{recovery}$ – відновлення системи після здійснення атаки; s_{adapt} – адаптація на основі знань про попередні атаки.

Приймемо початковий момент функціонування системи C як t_0, в якому система функціонує нормально, t_a – момент, коли почала виконуватися атака A, t_{deg} – момент, коли система зазнає деградації під впливом дії атаки A, t_{rec} – момент, коли система починає відновлення, t_{norm} – момент, коли система досягла нормального стану після відновлення.

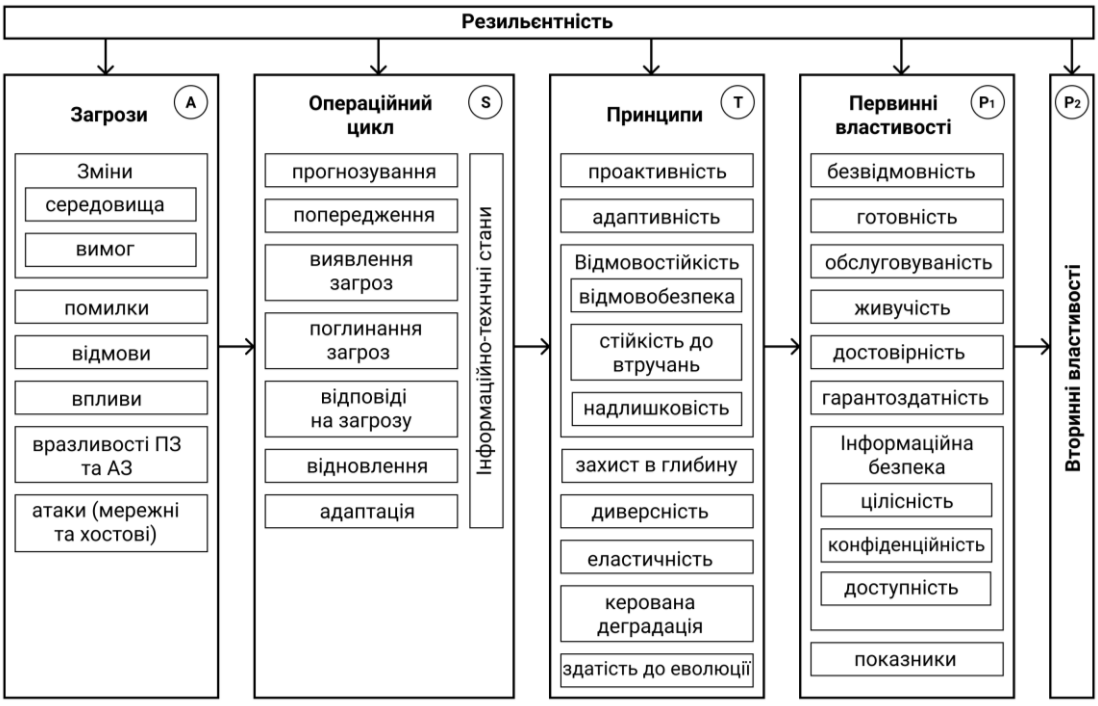

Рис. 1. Узагальнена таксономічна схема резильєнтності КС

Тоді визначимо множину інтервалів часу, що характеризують резильєнтність системи С в умовах здійснення атак:

$$\tau = \{\tau_0, \tau_{att}, \tau_{inf}, \tau_{rec}\}, \quad (3)$$

де τ_0 – інтервал нормального функціонування системи, $\tau_0(C, A) = [t_0, t_a)$; τ_{att} – інтервал вразливого функціонування системи, коли здійснюється атака, але система деградації ще не зазнає, $\tau_{att}(C, A) = [t_a, t_{deg})$; τ_{inf} – інтервал деградації системи під впливом деструктивних дій атаки, $\tau_{inf}(C, A) = [t_{deg}, t_{rec})$; τ_{rec} – інтервал відновлення системи від атаки, $\tau_{rec}(C, A) = [t_{rec}, t_{norm})$.

Рис. 2. Операційний цикл резильєнтної КС в умовах кіберзагроз

Кожен стан КС характеризується множиною значень параметрів

$$\forall s_j \in S : s_j = \{X_j, Z_j, F_j\}, \quad (4)$$

де $X_j = \{X_{sys}, X_{env}, X_{req}, X_{fail}\}$; X_{sys} – параметри системи, $X_{sys} = \{x_j\}_{j=1}^{N_{X_{sys}}}$, $N_{X_{sys}}$ – кількість параметрів системи; X_{req} – вимоги до системи, $X_{req} = \{x_j\}_{j=1}^{N_{X_{req}}}$, $N_{X_{req}}$ – кількість вимог до системи; X_{env} – параметри середовища, $X_{env} = \{x_j\}_{j=1}^{N_{X_{env}}}$, $N_{X_{env}}$ – кількість параметрів середовища; X_{fail} – параметри відмов, $X_{fail} = \{x_j\}_{j=1}^{N_{X_{fail}}}$, $N_{X_{fail}}$ – кількість параметрів відмов;

$$F_j = \{F_{prep}, F_{prot}, F_{detect}, F_{absorb}, F_{respond}, F_{recovery}, F_{adapt}\}$$

– множина механізмів F_j, які необхідно застосувати в залежності від стану системи C_i в умовах атаки A_k, $C_i \times A_k \to F_j$;

$$Z_j = \{Z_{prep}, Z_{prot}, Z_{detect}, Z_{absorb}, Z_{respond}, Z_{recovery}, Z_{adapt}\}$$

– множина параметрів системи, одержаних в результаті застосування механізмів F_j.

Розглянемо операційний цикл КС на прикладі smurf атаки [35], якій характерна велика кількість пакетів ICMP з підробленою IP-адресою жертви в мережі, що змушує КС в мережі реагувати, надсилаючи відповідь на IP-адресу джерела. Даний тип DDoS відомий, тому такий вплив атаки переводить систему С в момент t_a зі стану підготовки у стан виявлення $A_{smurf} : s_{prep} \to s_{detect}$, $C \times A_{smurf} \to F_{smurf}$, $\tau_{att}(C, A_{smurf}) = [t_a, t_{deg})$.

Послаблення наслідків smurf атаки покладається на надмірне резервування каналів, застосування служб фільтрації для виявлення та блокування небажаних відповідей ICMP, а також на застосування BGP маршрутизації з метою перенаправлення усього вхідного трафіку через зовнішню мережу. За допомогою перевірки вхідного трафіку всі небажані відповіді ICMP виявляються та блокуються.

Застосування механізмів послаблення (mitigation) F_{smurf} в момент t_{deg} $\tau_{inf}(C, A_{smurf}) = [t_{deg}, t_{rec})$ переведе систему у стани відповіді на атаку та відновлення системи: $s_{detect} \to s_{resp} \to s_{req}$. В залежності від інтенсивності атаки та ефективності заходів мітіґації в момент часу t_{req} система переходить в стан відновлення $s_{req} \to s_{norm}$, $\tau_{rec}(C, A_{smurf}) = [t_{rec}, t_{norm})$.

З точки зору операційного циклу на резильєнтність КС С впливатиме множина показників w, які відображають різні аспекти невизначеності станів S. Тоді представимо міру резильєнтності вектором $W = (w_1; w_2; \ldots)$, де $w_i (i = 1, 2, \ldots)$ – окремі показники міри резильєнтності КС.

Оскільки інформаційно-технічні стани S є незалежними, то ймовірність P успішної реалізації

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

операційного циклу функціонування комп'ютерної системи С представимо як добуток ймовірностей:

$$P(W) = P(W_{prep}) \cup P(W_{detect}) \cup P(W_{absorb}) \cup \cup P(W_{respond}) \cup P(W_{recovery}) \cup P(W_{adapt}),$$

$$P(W) = \sum_{w_i \in W} P_i, \quad (5)$$

де $P(w_{prep})$ – ймовірність того, що система вчасно підготовлена та захищена; $P(w_{detect})$ – ймовірність того, що система здатна до виявлення загроз; $P(w_{absorb})$ – ймовірність того, що система здатна до поглинання загроз; $P(w_{respond})$ – ймовірність того, що система здатна давати відповідь на загрозу; $P(w_{recovery})$ – ймовірність того, що система здатна до відновлення після здійснення кіберзагрози; $P(w_{adapt})$ – ймовірність того, що система здатна до адаптації.

1.3. Етапи резильєнтного функціонування системи в умовах кіберзагроз

Розглянемо етапи резильєнтного функціонування системи в умовах кіберзагроз.

Планування/підготовка (preparation). Для побудови резильєнтної системи C_i в умовах здійснення кібератаки А потрібно застосувати множину підготовчих заходів G_{prep} щодо прогнозування попередження можливих атак:

$$G_{prep} = \{Ar, Com, Seg, Mon, SS, Res\}, \quad (6)$$

де Ar – множина заходів для налаштування архітектурних компонентів системи, $Ar = \{ar_j\}_{j=1}^{N_{Ar}}$, N_{Ar} – кількість заходів; Com – множина заходів для налаштування зв'язків системи, $Com = \{com_j\}_{j=1}^{N_{Com}}$, N_{Com} – кількість заходів; Seg – множина заходів для налаштування сегментації системи, $Seg = \{seg_j\}_{j=1}^{N_{Seg}}$, N_{Seg} – кількість заходів сегментації; Mon – множина заходів для забезпечення моніторингу системи, $Mon = \{mon_j\}_{j=1}^{N_{Mon}}$, N_{Mon} – кількість заходів моніторингу; SS – множина сценаріїв безпеки системи, $SS = \{ss_j\}_{j=1}^{N_{SS}}$, N_{SS} – кількість сценаріїв; Res – множина заходів для забезпечення резервування критичних даних та інформації системи, $Res = \{res_j\}_{j=1}^{N_{Res}}$, N_{Res} – кількість заходів резервування.

Іншими аспектами *підготовленості* резильєнтної системи до функціонування КС є виконання дій:

- розуміння та оцінювання кіберризиків шляхом здійснення аналізу та симуляції атак;
- виявлення та усунення відомих вразливостей комп'ютерних систем, за допомогою яких кіберзлочинці здійснюють атаки;
- підвищення обізнаності про ознаки відомих кіберзагроз та розуміння того, як їх розпізнати;
- забезпечення відповідних стратегій резервного копіювання та відновлення.

Захист (protection). Етап *захисту* полягає в розробці та впровадженні множини методів та заходів G_{prot} безпеки системи С з метою обмеження чи стримування наслідків кібератак.

Метою є захист інфраструктури та мінімізація ймовірності того, що атака може бути успішною, і, якщо це станеться, можливість швидко реагувати, щоб зменшити шкоду. Проведена оцінка захищеності системи повинна виявити будь-які вразливості в існуючих методах захисту.

Виявлення (detection). Метою виявлення є розробка та здійснення множини методів та засобів G_{Detect}, $G_{Detect} = \{G_{Detect}^{host}, G_{Detect}^{lan}\}$ щодо швидкого виявлення атаки А, оцінки системи, яка може зазнати впливу, та забезпечення своєчасного реагування, де G_{Detect}^{host} – множина методів виявлення атак хостового типу, G_{Detect}^{lan} – множина методів виявлення атак мережного типу. Крім того, цей етап пов'язаний з продовженням моніторингу системи за іншими ознаками, пов'язаними з цією атакою, та впевненістю, що методи захисту були ефективними.

Поглинання (absorption). Продовження функціонування в умовах здійснення атак може вимагати непередбачуваних змін базової архітектури системи, залежно від того, що саме зазнає деградації засобами кібератаки.

Для опису процесу деградації системи в умовах здійснення атак введемо функцію ξ, що відображатиме поточну продуктивність системи. Будь-яка деструктивна дія a_m атаки А впливатиме на систему, тоді $\xi(t \mid a_m)$ визначатиме значення показника продуктивності в момент *t* при виконанні дії a_m.

Враховуючи вплив деструктивних дій атаки А на систему С, яка функціонувала в інтервалі від t_0 до t_{norm}, визначимо множину дій атаки А як $A = \{a_m : \xi(t \mid a_m) \neq \xi(t_0)\}$, $t \in [t_0, t_{norm})$.

Відповідь (respond). Етап забезпечення резильєнтності системи *Відповідь* повинен містити множину методів G_{resp} щодо видів діяльності, які можуть пришвидшити час до виправлення та стримувати вплив атаки після її виявлення. Щоб процес виявлення мав будь-яке значення, повинна бути своєчасна реакція.

Відновлення (recovery). Остаточний і надважливий етап забезпечення резильєнтності системи в умовах здійснення атаки – це *відновлення*. Цей етап передбачає розробку та впровадження відповідної множини методів G_{rec} для відновлення даних, служб, сервісів, які могли зазнати впливу під час кібератаки. Очевидно, що неможливо уникнути певних типів атак. Навіть якщо система швидко реагує на кібератаку, то система зазнає наслідків. Ефективне відновлення залежить від чіткого і ретельного застосування сценаріїв безпеки в залежності від типу виявленої атаки.

Адаптація (adaptation). Для підвищення резильєнтності системи *адаптація* полягає в залученні множини методів

$$G_{adapt},\ G_{adapt} = \{R_{str}, R_{cnf}\},$$

де R_{str} – множина методів реструктуризації, R_{cnf} – множина методів реконфігурування компонентів системи на основі попередніх атак.

Виходячи з вищеописаної концепції резильєнтності та її атрибутів, розглянемо відображення кожного етапу та дій для забезпечення резильєнтності системи в умовах здійснення атак (таблиця 2).

3. Онтологія резильєнтності комп'ютерних систем

На рис. 3 показана схема онтології резильєнтності з точки зору інформаційної безпеки комп'ютерних систем в умовах кіберзагроз.

Таблиця 2

Етапи резильєнтного функціонування системи в умовах кіберзагроз

Цілі для забезпечення резильєнтності	Дії з боку системи	Дії зловмисника
Планування / підготовка (мета: передбачити атаку)	Впровадження методів захисту та моніторингу для своєчасного виявлення можливої атаки, забезпечення альтернативних можливостей обробки даних та комунікації	Підготовка до атаки, вивчення об'єкта атаки
Захист (мета: запобігати атаці)	Застосування методів безпеки системи з метою обмеження наслідків атак, мінімізації ймовірності того, що атака може бути успішною. Оцінка захищеності системи	Здійснення атаки, спроба виявлення вразливостей для проникнення в КС
Виявлення (мета: ідентифікувати атаку)	Розробка та здійснення заходів щодо швидкого виявлення атаки, оцінки системи, яка може зазнати впливу, та забезпечення своєчасного реагування. Продовження моніторингу системи за іншими ознаками, пов'язаними з цією атакою, та впевненістю, що методи захисту є ефективні	Здійснення атаки. Атака частково або повністю успішна
Поглинання / відповідь (мета: протистояти атаці)	Застосування методів та механізмів сповіщення/координації для протистояння атакам (реконфігурування, оновлення, перерозподіл ресурсів, ізоляція, відмова), а також забезпечення модульності КС, відокремлення критичних даних від некритичних. Застосування принципу керованої деградації та методів мітігації. Підтримка мінімально необхідної продуктивності для надання послуг та сервісів системою. Визначення дій для підтримки контролю над системою та ізоляції її важливих ресурсів	Проникнення в систему. Підтримка зловмисником присутності в атакованій системі. Повний або частковий контроль над системою або її компонентом
Відновлення (мета: відновити систему)	Застосування дій щодо відновлення системи після атаки шляхом повернення системи до початкового стану. Визначення альтернативних комунікацій та методів обробки даних та моніторингу. Визначення критеріїв та компромісів для перерозподілу ресурсів та функціональності системи. Аналіз щодо надмірності, диверсності та витрат	Втрата часткового або повного контролю над атакованою системою
Адаптація (мета: розвивати систему)	Зміна структури системи, розробка та застосування нових сценаріїв безпеки, повторне перепроектування компонентів системи, розробка модульності системи	Підготовка нової атаки

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

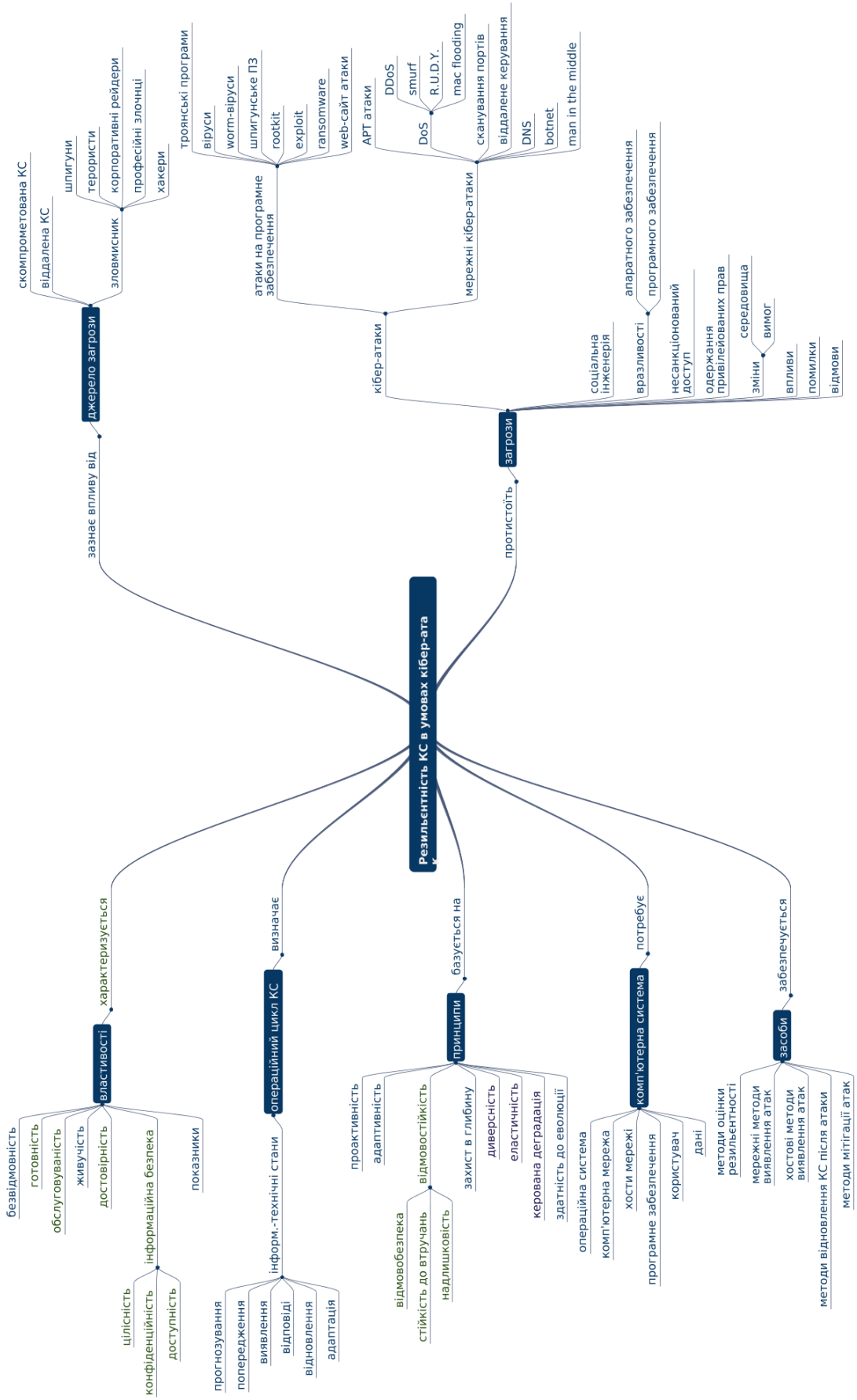

Рис. 3. Онтологічна схема резильєнтності комп'ютерних систем в умовах кібератак

Резильєнтність є основним класом, розташованим в центрі онтології, та має зв'язки з класами: *Властивості; Принципи, Операційний Цикл КС, Комп'ютерна система, Засоби, Джерело загрози, Загрози, Кіберзагрози.*

Висновки

У роботі визначено та проаналізовано концепцію резильєнтності. Представлено визначення поняття резильєнтності з точки зору кібербезпеки, а також основні елементи таксономічної схеми резильєнтності КС. Розроблено узагальнену таксономічну схему резильєнтності, пов'язану з інформаційною безпекою. Також подано операційний цикл резильєнтної КС як множину інформаційно-технічних станів, які проходить система. Розроблено схему онтології резильєнтності з точки зору інформаційної безпеки комп'ютерних систем в умовах кіберзагроз.

Подальша робота передбачає аналіз та розширення існуючих методів безпеки для вирішення аспектів резильєнтності.

Література

1. *SearchDataCenter. Data center resiliency [Electronic resource]. – Access mode: http://searchdatacenter.techtarget.com/definition/resiliency. – 13.12.2019.*
2. *NEXUSGUARD. DDoS Threat Report 2019 Q3 [Electronic resource]. – Access mode: https://www.nexusguard.com/threat-report-q3-2017. – 9.12.2019 p.*
3. *Zuzcak, M. Behavioral analysis of bot activity in infected systems using honeypots [Text] / M. Zuzcak, T. Sochor // Communications in Computer and Information Science. – Springer, Cham, 2017. – Vol. 718. – P. 118-133.*
4. *Holling, C. S. Resilience and stability of ecological systems [Text] / C. S. Holling // Annual Rev Ecology and Systematics. – 1973. – No. 4. – P. 1-23.*
5. *Economic vulnerability and resilience: concepts and measurements [Text] / L. Briguglio, G. Cordina, N. Farrugia, S. Vella // Oxford Devel Studies. – 2009. – No. 37(3). – P. 229-247.*

   DOI: 10.1080/13600810903089893.
6. *Cimellaro, G. P. Introduction to special issue on resilience-based analysis and design of structures and infrastructure systems [Text] / G. P. Cimellaro, L. Dueñas-Osorio, A. M. Reinhorn // Structural Engineering. – 2016. – No. 142(8). – P. 1-5.*
7. *Conceptual framework for developing resilience metrics for the electricity oil and gas sectors in the United States [Text] / J-P. Watson, R. Guttromson, C. Silva-Monroy, R. Jeffers, K. Jones, J. Ellison, C. Rath, J. Gearhart, D. Jones, T. Corbet, C. Hanley, L. T. Walker. – Sandia National Laboratories, Albuquerque, NM (United States), Tech. Rep., 2015. – 104 p.*
8. *Allenby, B. Toward inherently secure and resilient societies [Text] / B. Allenby, J. Fink // Science. – 2005. – Vol. 309, No. 5737. – P. 1034-1036.*
9. *Pregenzer, A. L. Systems resilience: A new analytical framework for nuclear nonproliferation [Text] / A. L. Pregenzer. – Albuquerque, NM : Sandia National Laboratories, Tech. Rep., 2011. – 27 p.*
10. *Haimes, Y. Y. On the definition of resilience in systems [Text] / Y. Y. Haimes // Risk Analysis. – 2009. – No. 29(4). – P. 498-501.*
11. *The infrastructure Security Partnership (TISP). Regional disaster resilience: a guide for developing on action plan [Text]. – American Society of Civil Engineers, 2006. – 36 p.*
12. *A framework for assessing the resilience of infrastructure and economic systems [Text] / E. D. Vugrin, D. E. Warren, M. A. Ehlen, R. C. Camphouse // Sustainable Infrastructure Systems: simulation, modeling, and intelligent engineering. – Berlin : Springer-Verlag, Inc., 2010. – P. 77-116.*
13. *Laprie, J.-C. Resilience for the Scalability of Dependability [Text] / J.-C. Laprie // Fourth IEEE International Symposium on Network Computing and Applications. – 2005. – P. 5-6.*
14. *Харченко, В. С. Гарантоздатні системи та багатоверсійні обчислення: аспекти еволюції [Текст] / В. С. Харченко // Радіоелектронні і комп'ютерні системи. – 2009. – № 7(41). – С. 46–59.*
15. *Bodeau, D. Structured Cyber Resiliency Analysis Methodology (SCRAM) [Text] / D. Bodeau, R. Graubart // The MITRE Corporation, PR Case No. 16-0777. – 2016. – 13 p.*
16. *Resilience metrics for cyber systems [Text] / I. Linkov, D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen, A. Kott // Environment Systems and Decisions. – 2013. – No. 33(4). – P. 471-476.*
17. *Bodeau, D. J. Cyber resiliency design principles: selective use throughout the lifecycle and in conjunction with related disciplines [Text] / D. J. Bodeau, R. D. Graubart. – The MITRE Corporation, Tech. Rep., 2017. – 98 p.*
18. *Development of Models in Resilient Computing [Text] / O. Drozd, V. Kharchenko, A. Rucinski, T. Kochanski, R. Garbos, D. Maevsky // 10th International Conference on Dependable Systems, Services and Technologies (DESSERT). – 2019. – P. 1-6.*
19. *Guelfi, N. A formal framework for dependability and resilience from a software engineering perspective [Text] / Nicolas Guelfi // Central European Journal of Computer Science. – 2011. – No. 1. – P. 294-328.*
20. *Laprie, J.-C. From Dependability to Resilience [Text] / J.-C. Laprie // IEEE Computer Society. – 2008. – P. 1-3.*
21. *Strigini, L. Resilience: What is it, and how much do we want? [Text] / L. Strigini // IEEE Security & Privacy. – 2012. – No. 10(3). – P. 72-75.*
22. *Basic Concepts and Taxonomy of Dependable and Secure Computing [Text] / A. Avizienis, J.-C. Laprie, B. Randell, C. E. Landwehr // IEEE Trans.*

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Dependable Sec. Comput. – 2004. – No. 1(1). – P. 11-33.

23. Avizienis, A. Dependability and its Threats – A taxonomy [Text] / A. Avizienis, J.-C. Laprie, B. Randell // IFIP Congress Topical Sessions. – 2004. – P. 91-120.

24. Cyber resilience – fundamentals for a definition [Text] / F. Björck, M. Henkel, J. Stirna, J. Zdravkovic // New contributions in information systems and technologies. – Springer, Cham, 2015. – P. 311-316.

25. Basel Committee on Banking Supervision. Cyber-resilience: Range of practices [Text]. – Bank for International Settlements, Tech. Rep., 2018. – 10 p.

26. Ontology and taxonomies of resilience [Text] / P. T. Vlacheas, V. Stavroulaki, P. Demestichas, S. Cadzowm, S. Gorniak, D. Ikonomou. – ENISA report, 2011. – 59 p.

27. Approaches to Enhancing Cyber Resilience: Report of the North Atlantic Treaty Organization (NATO) Workshop IST-153 [Text] / A. Kott, B. Blakely, D. Henshel, G. Wehner, J. Rowell, N. Evans, K. Krutilla // arXiv preprint. – Report number: ARL-SR-0396. – 2018. – 44 p. arXiv: 1804.07651.

28. The Cyber Resilience Blueprint: A New Perspective on Security [Text]. – Symantec, Tech. Rep., 2014. – 14 p.

29. A new resilience taxonomy [Text] / M. A. Thompson, M. J. Ryan, J. Slay, A. C. McLucas // INCOSE International Symposium. – 2016. – Vol. 26. – No. 1. – P. 1318-1330.

30. Validating resilience and vulnerability indices in the context of natural disasters [Text] / L. A. Bakkensen, C. Fox-Lent, L. K. Read, I. Linkov // Risk analysis. – 2017. – Vol. 37, No. 5. – P. 982-1004. DOI: 10.1111/risa.12677.

31. Deliverable D34: Resilience ontology: final [Text]. – ReSIST : Resilience for Survivability in IST., Tech. Rep., 2008. – 28 p.

32. Constructing a science of cyber-resilience for military systems [Text] / A. Alexeev, D. S. Henshel, K. Levitt, P. McDaniel, B. Rivera, S. Templeton, M. Weisman. – NATO IST-153 Workshop on Cyber Resilience, 2017. – 13 p.

33. Lang, C. Understanding the mission impact of a cyberattack in a system of systems environment [Text] / C. Lang, B. Madahar. – NATO IST-156 Workshop on Modelling and Simulation S&T: Critical Enabler for Cyber Defense, 2017. – 36 p.

34. Statistical models for the number of successful cyber intrusions [Text] / N. O. Leslie, R. E. Harang, L. P. Knachel, A. Kott // Defense Modeling and Simulation. – 2017. – No. 15(1). – P. 49-63. DOI: 10.1177/1548512917715342.

35. IMPERVA. Smurf DDoS attack [Electronic resource]. – Access mode: https://www.imperva.com /learn/application-security/smurf-attack-ddos. – 9.12.2019.

References

1. *SearchDataCenter*. Data center resiliency. Available at: http://searchdatacenter.techtarget.com/ definition/resiliency (accessed 13.12.2019).

2. *NEXUSGUARD. DDoS Threat Report 2019 Q3*. Available at: https://www.nexusguard.com/threat-report-q3-2019 (accessed 9.12.2019).

3. Zuzcak, M., Sochor, T. Behavioral analysis of bot activity in infected systems using honeypots. *Communications in Computer and Information Science*, Springer, Cham, 2017, vol. 718, pp. 118-133.

4. Holling, C. S. Resilience and stability of ecological systems. *Annual Rev Ecology and Systematics*, 1973, no. 4, pp. 1-23.

5. Briguglio, L., Cordina, G., Farrugia, N., Vella, S. Economic vulnerability and resilience: concepts and measurements. *Oxford Devel Studies*, 2009, no. 37(3), pp. 229-247. DOI:10.1080/13600810903089893.

6. Cimellaro, G. P. et al. Introduction to special issue on resilience-based analysis and design of structures and infrastructure systems. *Structural Engineering*, 2016, no. 142(8), pp.1-5.

7. Watson, J-P., Guttromson, R., Silva-Monroy, C., Jeffers, R., Jones, K., Ellison, J., Rath, C., Gearhart, J., Jones, D., Corbet, T., Hanley, C., Walker, L.T. *Conceptual framework for developing resilience metrics for the electricity oil and gas sectors in the United States*. Sandia National Laboratories, Albuquerque, NM (United States), Tech. Rep, 2015. 104 p.

8. Allenby, B., Fink, J. Toward inherently secure and resilient societies. *Science*, 2005, vol. 309, no. 5737, pp. 1034-1036.

9. Pregenzer, A. L. *Systems resilience: A new analytical framework for nuclear nonproliferation*. Albuquerque, NM, Sandia National Laboratories, Tech. Rep., 2011. 27 p.

10. Haimes, Y.Y. On the definition of resilience in systems. *Risk Analysis*, 2009, no. 29(4), pp. 498-501.

11. *The infrastructure Security Partnership (TISP). Regional disaster resilience: a guide for developing on action plan.* American Society of Civil Engineers, 2006. 36 p.

12. Vugrin, E. D., Warren, D. E., Ehlen, M. A., Camphouse, R. C. A framework for assessing the resilience of infrastructure and economic systems. *Sustainable Infrastructure Systems: simulation, modeling, and intelligent engineering*, Berlin, Springer-Verlag, Inc., 2010, pp. 77-116.

13. Laprie, J.-C. Resilience for the Scalability of Dependability. *Fourth IEEE International Symposium on Network Computing and Applications*, 2005, pp. 5-6.

14. Kharchenko, V. S. Harantozdatni systemy ta bahatoversiyni obchyslennya: aspekty evolyutsiyi [Dependable systems and multi-version computing: aspects of evolution]. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2009, no. 7 (41), pp. 46–59.

15. Bodeau, D., Graubart, R. Structured Cyber Resiliency Analysis Methodology (SCRAM). *The MITRE Corporation*, PR Case No. 16-0777, 2016. 13 p.

16. Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., Kott, A. Resilience metrics for cyber systems. *Environment Systems and Decisions*, 2013, no. 33(4), pp. 471-476.

17. Bodeau, D. J., Graubart, R. D. *Cyber resiliency design principles: selective use throughout the lifecycle and in conjunction with related disciplines*. The MITRE Corporation, Tech. Rep., 2017. 98 p.

18. Drozd, O., Kharchenko, V. et al. Development of Models in Resilient Computing. *10th International Conference on Dependable Systems, Services and Technologies (DESSERT),* 2019, pp. 1-6.

19. Guelfi, Nicolas. A formal framework for dependability and resilience from a software engineering perspective. *Central European Journal of Computer Science*, 2011, no. 1, pp. 294-328.

20. Laprie, J.-C. From Dependability to Resilience. *IEEE Computer Society*, 2008, pp. 1-3.

21. Strigini, L. Resilience: What is it, and how much do we want? *IEEE Security & Privacy*, 2012, no. 10(3), pp. 72-75.

22. Avizienis, A., Laprie, J.-C., Randell, B., Landwehr, C. E. Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Trans. Dependable Sec. Comput.*, 2004, no. 1(1), pp. 11-33.

23. Avizienis, A., Laprie, J.-C., Randell, B. Dependability and its Threats – A taxonomy. *IFIP Congress Topical Sessions*, 2004, pp. 91-120.

24. Björck, F., Henkel, M., Stirna, J., Zdravkovic, J. Cyber resilience – fundamentals for a definition. *New contributions in information systems and technologies.* Springer, Cham, 2015, pp. 311-316.

25. *Basel Committee on Banking Supervision. Cyber-resilience: Range of practices*. Bank for International Settlements, Tech. Rep., 2018. 10 p.

26. Vlacheas, P. T., Stavroulaki, V., Demestichas, P., Cadzowm, S., Gorniak, S., Ikonomou, D. *Ontology and taxonomies of resilience*. ENISA report, 2011. 59 p.

27. Kott, A., Blakely, B., Henshel, D., Wehner, G., Rowell, J., Evans, N., Krutilla, K. *Approaches to Enhancing Cyber Resilience: Report of the North Atlantic Treaty Organization (NATO) Workshop IST-153.* arXiv preprint, Report number: *ARL-SR-0396*, 2018. 44 p. arXiv:1804.07651.

28. *The Cyber Resilience Blueprint: A New Perspective on Security.* Symantec, Tech. Rep, 2014. 14 p.

29. Thompson, M. A., Ryan, M. J., Slay, J., McLucas, A. C. A new resilience taxonomy. *INCOSE International Symposium,* 2016, vol. 26, no. 1, pp. 1318-1330.

30. Bakkensen, L. A., Fox-Lent, C., Read, L. K., Linkov, I. Validating resilience and vulnerability indices in the context of natural disasters. *Risk analysis*, 2017, vol. 37, no. 5, pp. 982-1004. DOI: 10.1111/risa.12677.

31. *Deliverable D34: Resilience ontology: final.* ReSIST: Resilience for Survivability in IST., Tech. Rep., 2008. 28 p.

32. Alexeev, A. et al. *Constructing a science of cyber-resilience for military systems*. NATO IST-153 Workshop on Cyber Resilience, 2017. 13 p.

33. Lang, C., Madahar, B. Understanding the mission impact of a cyberattack in a system of systems environment. *NATO IST-156 Workshop on Modelling and Simulation S&T: Critical Enabler for Cyber Defense*, 2017. 36 p.

34. Leslie, N. O., Harang, R. E., Knachel, L. P., Kott, A. Statistical models for the number of successful cyber intrusions. *Defense Modeling and Simulation*, 2017, no. 15(1), pp. 49-63. DOI: 10.1177/1548512917715342.

35. *IMPERVA. Smurf DDoS attack.* Available at: https://www.imperva.com/learn/application-security/smurf-attack-ddos (accessed 9.12.2019).

Надійшла до редакції 12.12.2019, розглянута на редколегії 20.01.2020

РЕЗИЛЬЕНТНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ В УСЛОВИЯХ КИБЕРУГРОЗ: ТАКСОНОМИЯ И ОНТОЛОГИЯ

С. Н. Лысенко, В. С. Харченко, К.Ю. Бобровникова, Р. В. Щука

Стремительное развитие информационных технологий привело к расширению возможностей киберугроз относительно компьютерных систем (КС). Киберпреступники разрабатывают новые способы для избежания обнаружения атак, поэтому существующие подходы не в состоянии противостоять растущей угрозе атак. Между тем последствия кибератак становятся более опасными и разрушительными. Одним из подходов к решению проблемы является построение резильентных систем, которые способны быстро восстанавливаться и продолжать функционировать в условиях осуществления атак. **Предметом** исследования является процесс построения резильентных компьютерных систем в условиях киберугроз. **Целью** является разработка таксономии и онтологии резильентных компьютерных систем в условиях киберугроз. **Результаты**. В статье представлены определения понятия резильентности с точки зрения кибербезопасности, представлена связь понятий резильентности и гарантоспособности. В работе представлены основные элементы таксономической схемы резильентности КС, к которым относятся угрозы (изменения среды и требований, сетевые атаки, атаки на ПО, уязвимости программного и аппаратного обеспечения, ошибки, отказы, воздействия), информационно-технические состояния, которые КС проходит в течение своего операционного цикла, принципы, на которых базируется резильентность (проактивность, адаптивность, устойчивость к вмешательствам, диверсность, эластичность, управляемая деградация, защита в глубину, способность к эволюции), а также первичные и вторичные свойства. На основе вышеуказанных элементов разработана обоб-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

щенная таксономическая схема резильентности, связанная с информационной безопасностью. В работе представлен операционный цикл резильентной КС как множество информационно-технических состояний, которые проходит система (подготовка, защита системы, обнаружение угроз, поглощение угроз, ответ на угрозу, восстановление системы после кибератаки, адаптация). Разработана схема онтологии резильентности с точки зрения информационной безопасности компьютерных систем в условиях киберугроз. **Выводы**. Разработаны таксономия и онтология резильентных компьютерных систем в условиях киберугроз.

Ключевые слова: резильентность; киберугроза; кибератака; адаптивность; диверсность; онтология; таксономия; защита в глубину; проактивность; стойкость к вмешательствам; эластичность; управляемая деградация; способность к эволюции.

COMPUTER SYSTEMS RESILIENCE IN THE PRESENCE OF CYBER THREATS: TAXONOMY AND ONTOLOGY

S. Lysenko, V. Kharchenko, K. Bobrovnikova, R. Shchuka

The rapid development of information technology has expanded the capabilities of cyberthreads regarding computer systems. Cybercriminals are developing new ways to avoid attack detection, so existing approaches are not able to withstand the growing threat of attacks. Meanwhile, the consequences of cyberattacks are becoming more dangerous and destructive. One of the approaches to solve the problem is the construction of resilient systems that are able to quickly recover and continue to function under attack conditions. **The subject** of research is the construction process of the resilient computer systems in the face of cyber threats. **The goal** is to develop a taxonomy and ontology of resilient computer systems under cyberthreats. **Results**. The article presents the definitions of the resilience from the point of view of cybersecurity, presents the gap between the concepts of resilience and dependability. The paper presents the main elements of the taxonomic scheme of computer system resilience, which include threats (changes in the environment and requirements, network attacks, attacks on software, software and hardware vulnerabilities, errors, failures), information and technical conditions that computer system passes during its operating cycle, the principles on which resilience is based (proactivity, adaptability, resistance, diversity, elasticity, controlled degradation, defense in depth, ability to evolvability), as well as primary and secondary properties. Based on the above elements, a generalized taxonomic scheme of resilience related to information security has been developed. The work presents the operational cycle of a resilient CS as a set of information and technical states that the system goes through (preparation, system protection, threat detection, threat absorption, response to a threat, system recovery after a cyberattack, adaptation.) An ontology scheme of the resilience from the point of view of information security of computer systems in the presence of cyberthreats is developed. **Conclusions** A taxonomy and ontology of resilient computer systems in the presence of cyberthreats has been developed.

Keywords: resilience; cyberthreat; cyberattack; adaptability; diversity; ontology; taxonomy; defense in depth; proactivity; resistance; elasticity; controlled degradation; evolvability.

Лисенко Сергій Миколайович – канд. техн. наук, доцент кафедри комп'ютерної інженерії та системного програмування, Хмельницький національний університет, Хмельницький, Україна.

Харченко Вячеслав Сергійович – д-р техн. наук, проф., зав. кафедри комп'ютерних систем, мереж та кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Бобровнікова Кіра Юліївна – канд. техн. наук, доцент кафедри комп'ютерної інженерії та системного програмування, Хмельницький національний університет, Хмельницький, Україна.

Щука Роман Володимирович – аспірант кафедри комп'ютерної інженерії та системного програмування, Хмельницький національний університет, Хмельницький, Україна.

Lysenko Sergii – PhD, Associate Professor of Computer Engineering & System Programming Department, Khmelnytskyi National University, Khmelnytskyi, Ukraine, e-mail: sirogyk@ukr.net,
ORCID Author ID: 0000-0001-7243-8747, Scopus Author ID: 54420643500, ResearcherID: I-1728-2018
https://scholar.google.com.ua/citations?hl=uk&user=TuAfytwAAAAJ&view_op=list_works

Kharchenko Vyacheslav – DrS on Engineering, Professor, Head of the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: v.kharchenko@csn.khai.edu, ORCID Author ID: 0000-0001-5352-077X, Scopus Author ID: 22034616000, ResearcherID: A-7719-2017, https://scholar.google.com/citations?hl=ru&user=FQ4dH4EAAAAJ.

Bobrovnikova Kira – PhD, Associate Professor of Computer Engineering & System Programming Department, Khmelnytskyi National University, Khmelnytskyi, Ukraine, e-mail: bobrovnikova.kira@gmail.com,
ORCID Author ID: 0000-0002-1046-893X, Scopus Author ID: 56946906000, ResearcherID: I-1504-2018,
https://scholar.google.com.ua/citations?hl=uk&user=NZaNO5AAAAAJ&view_op=list_works.

Shchuka Roman – PhD student of Computer Engineering & System Programming Department, Khmelnytskyi National University, Khmelnytskyi, Ukraine, e-mail: roman@gmail.com.