Куцаєв В.В. (ВІТІ НЦЗІ)
Радченко М.М. (ВІТІ НЦЗІ)
Терещенко Т.П. (ВІТІ НЦЗІ)

МОДЕЛЬ ОЦІНКИ ГОТОВНОСТІ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОГО ВУЗЛА ЗВ'ЯЗКУ В УМОВАХ КІБЕРНЕТИЧНИХ АТАК

Розглядається модель оцінки готовності інформаційно-телекомунікаційного вузла зв'язку інформаційно-телекомунікаційної системи спеціального призначення в умовах кібернетичних атак. Обґрунтовано оцінку потоку кібернетичних атак, як простішого потоку. Запропонована модель функціонування вузла зв'язку, як відновлювальної системи з обмеженою надійністю елементів. Модель дозволяє оцінити стан кібернетичної захищеності головних компонентів вузла зв'язку, якими є: система кібернетичної безпеки, кореневий маршрутизатор та сервіси, які надає вузол зв'язку. Розглянуто простий потік кібернетичних атак λ на вході та виході системи кібернетичної безпеки, на вході та виході кореневого маршрутизатора та на вході основних сервісів. Запропоновані оцінки коефіцієнтів готовності сервісів, кореневого маршрутизатора та вузла зв'язку у цілому. Запропонована оцінка коефіцієнтів вразливості та захищеності вузла зв'язку від кібернетичних атак.

Ключові слова: *модель, процес, кібепростір, сервіс, простий потік, актив, інтенсивність атак, кібернетична вразливість, кібернетична захищеність, коефіцієнт готовності, час відновлення, час нормального функціонування, інформаційно-телекомунікаційний вузол зв'язку, система кібернетичної безпеки.*

Куцаєв В.В., Радченко Н.Н., Терещенко Т.П. Модель процеса функционирования информационно-телекоммуникационного узла связи в условиях кибернетических атак. *Рассматривается модель оценки готовности информационно-телекоммуникационного узла связи информационно-телекоммуникационной системы специального назначения в условиях кибернетических атак. Предложена модель функционирования узла, как восстанавливаемой системы с ограниченной надежностью элементов. Модель позволяет оценить состояние кибернетической защищенности главных компонентов узла, которыми являются: система кибернетической безопасности, корневой маршрутизатор и сервисы, которые предоставляет узел. Рассмотрен простой поток кибернетических атак λ на входе и выходе системи кибернетической безопасности, на входе и выходе корневого маршрутизатора и на входе основных сервисов. Предложены оценки коэфициентов готовности сервисов, корневого маршрутизатора и узла связи в целом. Предложена оценка коэффициентов уязвимости и защищенности узла связи от кибернетических атак.*

Ключевые слова: *модель, процесс, кибепростир, сервис, простой поток, актив, интенсивность атак, кибернетическая уязвимость, кибернетическая защищенность, коэффициент готовности, время восстановления, время нормального функционирования, информационно-телекоммуникационный узел связи, система кибернетической безопасности.*

V. Kytsayev, N. Radchenko, T. Terestchenko The model of the functioning of the information and telecommunication communications center in the context of cyber attacks. *There are a model of the process of functioning of the information and telecommunication communication center of the information and telecommunication system for special purposes in the context of cyber attacks is considered. The model of process of functioning of the communication center is offered, as a refurbishable system with a limitreliability of the components. The model allows to estimate the state of cybernetic security of main components of the communication center, that it is been: system of cybernetic safety, root router and services that is given by the communication center. The flow of cyber attacks λ at the input and output of the communication center, at the input and output of the root router, and at the entrance to the main services is considered. The estimation of coefficients of vulnerability and security of the communication center is offered from cybernetic attacks. Pre-conditions are created for the estimation of possibletime on renewal of the communication center and his main components after influence of cybernetic attacks.*

Key words: *model, process, kiberbostir, service, simple flow, asset, attack intensity, cyber vulnerability, cyber security, availability, recovery time, normal functioning time, information and telecommunication communication center, cyber security system.*

Постановка завдання в загальному вигляді. У щорічній доповіді експертів Всесвітнього економічного форуму про глобальні ризики у світі під назвою „World Economic Forum Global Risks Report 2019", яка опублікована в 15 січня 2019 року [1], на друге місце після природних катаклізмів за негативним впливом, для світової спільноти, виносяться кібератаки. Ризики кібербезпеки постійно зростають, як у їх поширеності, так і руйнівному потенціалі. Наприклад, кількість кібератак на підприємства у світі подвоїлася протягом п'яти останніх років, а інциденти, які колись розглядалися як надзвичайні, сьогодні стають все

більш розповсюдженими. Об'єкти критичної інфраструктури України стають мішенями, на яких випробовуються все нові технології кібератак [2, 3] внутрішніх та зовнішніх кібернетичних злочинців, діяльність яких активно зросла особливо під час гібридної війни з РФ. Інформаційно-телекомунікаційні вузли Збройних сил України також розміщені у зоні постійного кібернетичного впливу.

Виходячи з цього, автори вважають за доцільне зосередити зусилля на розробці моделі процесу функціонування інформаційно-телекомунікаційного вузла зв'язку (далі – ІТВ*)* в умовах кібернетичних атак та розробки рекомендацій для реалізації ефективної кібернетичної безпеки, як будь-якого окремого ІТВ так і всієї ІТС у цілому.

Аналіз останніх публікацій і напрямки вирішення завдання

Питання створення моделей кібернетичного захисту в інформаційно телекомунікаційній системі та її складових знайшли своє відображення у розробці наукових підходів та математичного апарата в роботах багатьох дослідників, для прикладу взяті джерела [4 – 7], а нижче коротко наведені їх особливості.

В запропонованій авторами статті [4] зазначається, що в ході вирішення завдання отримання основних ймовірно-часових характеристик системи захисту від кібератак, характеристики ставляться у залежність від варіантів побудови системи захисту від того, як підключені компоненти захисту кожного агрегату автоматизації управління (далі – ААУ) в обстановці впливу широкого класу кібератак. Наведені три способи включення елементів системи захисту в компоненти ААУ автоматизованої системи управління (далі – АСУ), що захищається:

– послідовне включення, коли всі елементи *і*-го агрегатного компонента системи захисту включені послідовно з компонентами ААУ;

– паралельне включення, коли всі елементи *і*-го агрегатного компонента системи захисту включені паралельно компонентам ААУ і не впливають на їх функціонування;

– змішане включення, що є комбінацією з двох перших способів включення елементів *і*-го агрегатного компонента системи.

В роботі приведені сильні сторони та недоліки різних моделей підключення елементів системи захисту в компоненти ААУ АСУ.

В роботі [4] не вирішене завдання створення моделі, яка б максимально точніше відображала процеси, які відбуваються у внутрішній роботі ІТВ під час впливу атак та у відновлювальний період. Запропоновані моделі побудови систем захисту більше стосуються реакції структури захисту на гіпотетичний вплив атак ніж на відображення процесів, які відбуваються при функціонуванні ІТВ. Моделі, згідно якої була б можливість оцінити готовність ІТВ до впливу кібернетичної атаки та визначити величину збитку від порушення критичних властивостей інформаційних активів у роботі не приводилось.

У статті [5] отримано аналітичні вирази для оціночних значень ймовірностей виявлення атак в наступних моделях подій: без повтору атак і без усунення наслідків; з повтором атак і без усунення наслідків; без повтору атак і з усуненням наслідків; з повтором атак і з усуненням наслідків. На думку авторів це дає можливість обґрунтовано здійснювати вибір значень доцільних періодів опитування (середніх значень періодів опитування). Авторами пропонується використовувати факти виявлених нелегітимних значень параметрів MIB (Management Information Base) агентів управління телекомунікаційного обладнання вузлів телекомунікаційної мережі спеціального призначення. Зміна вважається не санкціонованою і фіксується, якщо вона не була викликана керуючим впливом через уповноважений підрозділ технологічного управління. При цьому атака вважається не виявленою або пропущеною засобами захисту інформації, наявними на вузлах телекомунікаційної мережі спеціального призначення, тому що в іншому випадку зміни не приведуть до дозволених змін параметра MIB.

В статті [5] використовувався математичний апарат теорії потоків і масового обслуговування, але не отримана максимально наближена до реалій модель процесу, яка описує надійність компонентів телекомунікаційного вузла в умовах кібернетичних атак.

В роботі [6] розроблена математична GERT-модель початкової генерації коду кібератаки несанкціонованого доступу (далі – НСД) до ресурсів компютерної системи, але вона відрізняється від відомих моделей урахуванням основних етапів генерації в процесі математичної формалізації GERT-мережі. В ході моделювання автори отримали аналітичний вираз (функції, щільності розподілу) для розрахунку часу генерації коду кібератаки НСД, що дає можливість використовувати результати для проведення порівняльного аналізу та досліджень, більш складних комплексних етапів кібератаки НСД.

Недоліком такого підходу в роботі [6] можна вважати те, що сама модель може бути використана для дослідження тільки одного типу кібератаки, а саме – НСД і не дає цілісної уяви щодо процесів, які відбуваються в об'єкті під час повноцінного потоку кібератак різного типу з інтенсивністю **λ.**

У статті [7] на думку авторів запропоновано новий підхід до аналітичного моделювання кібератак, заснований на методі перетворення стохастичних мереж. Сутність даного підходу полягає в заміні безлічі елементарних гілок стохастичної мережі однією еквівалентною гілкою і у подальшому визначенні еквівалентної функції мережі, а також початкових моментів і функції розподілу випадкового часу реалізації кібератаки. Перевірка запропонованого підходу проведена, для моделювання кібератак типу «Сканування мережі та виявлення її вразливостей» і «Відмова в обслуговуванні», які є одними з найбільш поширених і небезпечних для компютерних мереж.

Недоліком такого підходу [7] можна вважати те, що до оцінки кіберстійкості було прийнято обмеження, згідно з яким нова кібератака починається через деякий час після того, як була виявлена попередня, і були усунені наслідки її реалізації. В реальності одночасно діючих зловмисників може бути досить багато і кібератаки, що активуються ними, можуть накладатися одна на одну. Інше обмеження розглянутого підходу повязано з тим, що сценарії можливих атак заздалегідь вважаються відомими, а сценарії реалізації заходів протидії атак не розглядаються. У той же час безліч можливих сценаріїв протидії кібератакам є кінцевими, що не дає аналітичної моделі поведінки компютерної мережі в умовах кібервпливу і не дозволяє оцінювати і вибирати найбільш ефективні заходи протидії.

Таким чином визначимо, що публікації в даній предметній області не дають повної відповіді на завдання, пов'язані з функціонуванням ІТВ в умовах впливу кібернетичних атак. Відсутні обґрунтовані рекомендації щодо покращення ефективності функціонування ІТВ ІТС після впливу кібернетичних атак. Відсутні відповіді на наступні актуальні питання:

яким законом визначається розподіл кібернетичних атак націлених на ІТВ;

яку модель оцінки функціонування ІТВ доцільно використати для оцінки готовності, вразливості та захищеності ІТВ в умовах впливу на неї кібернетичних атак;

які аналітичні моделі доцільні для розрахунку коефіцієнтів готовності, вразливості та захищеності ІТВ в умовах впливу на неї кібернетичних атак.

***Мета статті*:** розробка моделі оцінки готовності функціонування ІТВ з системою кібернетичної безпеки (далі – СКБ) в умовах впливу на неї потоку кібернетичних атак для оцінки ймовірності знаходження ІТВ або його компонентів у стані нормального функціонування та розрахунків коефіцієнтів готовності, вразливості та захищеності.

Виклад основного матеріалу

Розглянемо процес функціонування ІТВ, який має у своєму складі розгорнуту СКБ, кореневий маршрутизатор та підсистему сервісів *s*, де $s = 1, 2, \ldots, S$, де S – загальна кількість сервісів ІТВ (рис. 1). Кожний сервіс ІТВ виконує окрему інформаційну послугу та складається з технічних засобів і особового складу, який забезпечує його функціонування. На вхід ІТВ, а саме на СКБ, надходить вхідний потік кібернетичних атак.

Введемо обмеження для запропонованої моделі функціонування ІТВ в умовах сучасних кібернетичних атак:

на вхід ІТВ надходить сумарний потік випадкових потоків кібернетичних атак з кібернетичного простору, який в сумі наближається до простішого [8];

після СКБ виходить простий потік, який наближається до простішого;

простіший потік кібернетичних атак є найбільш складним для обробки, тому таке припущення призведе до отримання найгірших коефіцієнтів готовності, вразливості та захищеності;

під час кібернетичних атак інтервали функціонування ІТВ розподілені за експоненціальним законом [9] (рис 2, 3);

кібернетичні загрози, які надходять в потоці кібернетичних атак співпадають з вразливостями ІТВ з інтервалами часу розподіленими за експоненціальним законом;

Спрощена структурна схема такого інформаційно-телекомунікаційного вузла зв'язку наведена на рис. 1, де прийняті наступні позначення:

λ – інтенсивність загального потоку кібернетичних атак на вході ІТВ,

де $\lambda = \lambda_M + \sum_{s=1}^{S} \lambda_s,\ \lambda_z = \lambda_{zM} + \sum_{s=1}^{S} \lambda_{zs}.$;

λ_M – інтенсивність потоку кібернетичних атак на вході ІТВ націлених на кореневий маршрутизатор;

λ_s – інтенсивність потоку кібернетичних атак на вході ІТВ націлених на сервіс s, де $s = 1, \ldots, S$;

λ_z – інтенсивність потоку кібернетичних атак після виявлення та заблокування атак СКБ;

λ_o – інтенсивність потоку кібернетичних атак, який заблокувала СКБ ІТВ;

λ_{zM} – інтенсивність потоку кібернетичних атак націлених на кореневий маршрутизатор після впливу на потік атак СКБ;

λ_{zs} – інтенсивність потоку кібернетичних атак на вході сервісів s, де $s = 1, \ldots, S$ після впливу на потік атак СКБ;

A_s – актив АПК сервісу s, де $s = 1, \ldots, S$.

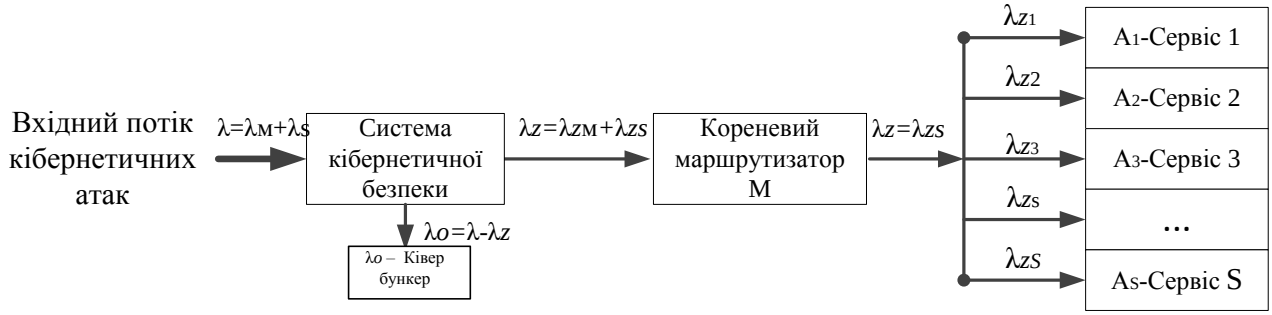

Рис.1. Спрощена структурна схема інформаційно-телекомунікаційного вузла зв'язку, функціонуючого в умовах кібернетичних атак

З рис. 1 видно, що система кібернетичної безпеки здійснює розрідження вхідного потоку кібернетичних атак, частина з яких з інтенсивністю λ_{zM} спрямована на маршрутизатор, а частина з інтенсивністю λ_{zs} на сервіси s. Будемо вважати, що вдала кібернетична атака на кореневий маршрутизатор призведе до повного блокування ІТВ в цілому, а кібернетична атака на s-й сервіс до втрати активів сервісу A_s, $s = 1, 2, \ldots, S$.

Розглянемо процес функціонування кореневого маршрутизатора після впливу на нього кібернетичної атаки. Будемо вважати, що в момент виявлення впливу атаки, обслуговуючий персонал ІТВ одразу приступає до відновлення працездатності обладнання маршрутизатора та сервісів s. Тривалість відновлення маршрутизатора – випадкова величина $t_{вмi}$, $i = 1, 2, \ldots$, з функцією розподілення $F_{вм}(t) = P\{t_{вм} < t\}$ та кінцевим математичним очікуванням середнього часу відновлення $T_{вм} < \infty$. В момент завершення відновлення маршрутизатора, ІТВ відновляє нормальне функціонування до моменту впливу наступної кібернетичної атаки. Тривалість нормального функціонування маршрутизатора випадкова величина $t_{мi}$, $i = 1, 2$, з функцією розподілення $F_{нфм}(t)=P\{t_{нфм}<t\}$, $F_м(t)=P\{t_м<t\}$ та кінцевим математичним

очікуванням Tнфм < ∞.

Графічне зображення цього процесу зображено на рис. 2, де прийняті наступні позначення:

ti – моменти початку впливу кібернетичних атак на маршрутизатор не виявлених СКБ де i = 1, 2, …;

*t*вм*i* – тривалість відновлення маршрутизатора після впливу кібернетичної атаки i = 1, 2, …;

*t*м*i* – тривалість нормального функціонування маршрутизатора i = 1, 2, … .

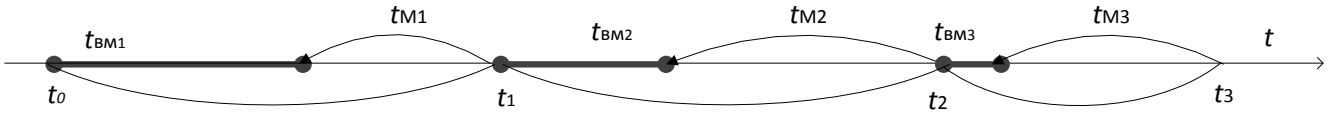

Рис. 2. Графічне зображення процесу функціонування кореневого маршрутизатора в умовах впливу кібернетичних атак з інтенсивністю λ*z*М

Аналогічно функціонує кожний сервіс *s* при впливі кібернетичних атак з інтенсивністю λ*z*s, які не заблоковані СКБ, де *s,* де *s* = 1, …, *S.* Це зображено на (рис. 3) де прийняті наступні позначення:

*T*в*si* – реалізація випадкових величин часу відновлення працездатності сервісу *s* після впливу кібернетичної атаки де i = 1, 2, …;

Tsi – тривалість нормального функціонування сервісу *s* після чергового відновлення працездатності ІТВ де i = 1, 2, … .

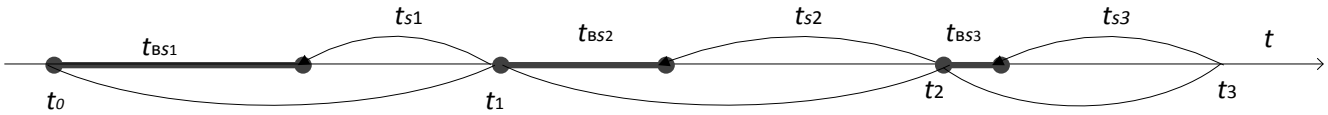

Рис. 3. Графічне зображення процесу функціонування сервісу *s* в умовах впливу кібернетичних атак з інтенсивністю λ*zs*

Таким чином бачимо, що модель процесу функціонування ІТВ в умовах впливу кібернетичних атак аналогічна моделі процесу функціонування *відновлюваної системи з обмеженою надійністю елементів*. Тому для кількісної оцінки ефективності захищеності ІТВ від кібернетичних атак доцільно використати комплексний показник надійності функціонування відновлюваної системи *K*г – коефіцієнт готовності [9], коефіцієнти вразливості – *Kvr* та захищеності – *K*з від кібернетичних атак [10].

Під коефіцієнтом готовності інформаційно-телекомунікаційного ІТВ, функціонуючого під впливом кібернетичних атак з інтенсивністю λ, будемо розуміти ймовірність того, що відновлювальний ІТВ опиниться працездатним (буде нормально функціонувати) в довільний момент часу.

Визначимо через *p0(t)* ймовірність працездатності ІТВ в момент часу *t,* а через *p1(t)* ймовірність непрацездатності ІТВ в умовах потоку кібернетичних атак. Тоді зазначимо, що

$$p0(t) + p1(t) = 1. \quad (1)$$

Розглянемо формулу для ймовірності *p*0*(t)* під час впливу кібернетичних атак на ІТВ при враженні маршрутизатора, коли випадкові величина *t*м*i* та *t*вм*i* (рис. 2) розподілені за експоненціальним законом з параметрами λ*z*м = 1/*T*нфм, μм = 1/*T*вм,

де λ*z*м – інтенсивність потоку кібернетичних атак на кореневий маршрутизатор;

μм – інтенсивність відновлення кореневого маршрутизатора;

*T*нфм – статистична оцінка середнього значення випадкової величини *t*м*i*;

*T*вм статистична оцінка середнього значення випадкової величини *t*вм*i*.

Тоді для аналізу ймовірності $p0(t)$ ІТВ можливо долучити наступну формулу [9]:

$$p_0(t) = \frac{1}{1+K_{\text{в}}}\left[1+K_{\text{в}} \times e^{-\lambda\left(\frac{1+K_{\text{в}}}{K_{\text{в}}}\right)t}\right], \quad (2)$$

де Kв = Tвм/Tнфм – показник норми відновлення ІТВ (за рахунок відновлення працездатності маршрутизатора).

Такий показник $p0(t)$ формули (2) будемо вважати нестаціонарним коефіцієнтом готовності ІТВ до кібернетичних атак, оскільки він залежить від часу – t [9] (рис. 4).

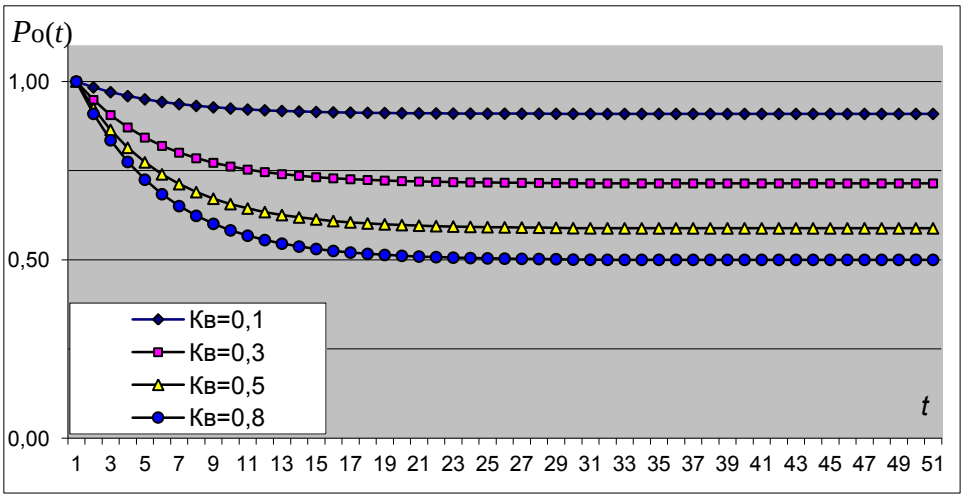

Рис. 4. Зображення поведінки нестаціонарного коефіцієнта готовності ІТВ – $p0(t)$ в залежності від часу при різних значеннях Kв

Використовуючи формулу (2), виводимо формулу (3) для коєфіцієнту готовності маршрутизатора до кібернетичних атак:

$$\lim p0(t) = K\text{гм} = 1/(1+ K\text{вм}) = T\text{нфм} /(T\text{нфм} + T\text{вм}). \quad (3)$$

Це означає, що існує стале значення ймовірності $p0(t)$, яке не залежить від часу. Таким чином ймовірність отримати вузол зв'язку працездатним у довільний момент часу в сталому режимі експлуатації, через деякий час після моменту $t = 0$ відповідає постійній величині, яку називають стаціонарним коефіцієнтом готовності. Зазначимо, що формула (3) вірна при довільних функціях розподілення випадкових величин tмi та Tвмi. Ця формула добре відображує фізичну суть коефіцієнта готовності, як відносну долю часу, під час якої ІТВ знаходиться в працездатному стані.

Тоді статистична оцінка коефіцієнту готовності маршрутизатора:

$$K^*\text{гм} = 1/(1+ K^*\text{вм}) = T^*\text{нфм} /(T^*\text{нфм} + T^*\text{вм}), \quad (4)$$

де T^*нфм – статистична оцінка середнього значення випадкової величини tмi (рис. 2) в сталому режимі (коли $t \to \infty$)

$$T^*\text{нфм} = (1/n)\sum_{j=1}^{n} t_{\text{ě}j},$$

T^*вм – статистична оцінка середнього значення випадкової величини tвмi (рис. 2)

$$T^*\text{вм} = (1/n)\sum_{j=1}^{n} t_{\text{âě}j}.$$

Розглянемо випадок, коли кібернетична атака з інтенсивністю λzs впливає на s-й сервіс, де s = 1, …, S (рис. 3). В момент впливу кібернетичної атаки на сервіс s він втрачає працездатність та перемикається на режим відновлення. Оскільки всі сервіси існують незалежно, тоді для s-го сервісу можливо визначити формулу коефіцієнта готовності Kгs та K^*гs,

де s = 1, …, S аналогічно наведеним вище для маршрутизатора формулам (3) та (4), але з

індексом *s*, а саме:

$$K\text{г}s = 1/(1+ K\text{в}s) = T\text{нф}s /(T\text{нф}s + T\text{в}s), \quad (7)$$

$$K^*\text{г}s = 1/(1+ K^*\text{в}s) = T^*\text{нф}s /(T^*\text{нф}s + T^*\text{в}s), \quad (8)$$

де $T^*\text{нф}s = 1/n \sum_{j=1}^{n} t_{sj}$, $T^*\text{в}s = 1/n \sum_{j=1}^{n} t_{âsj}$.

Для того, щоб застати підсистему сервісів *S* в довільний момент часу *t* в сталому режимі у працездатному стані, необхідно щоб в момент часу *t* були працездатні всі сервіси одночасно. З точки зору надійності таку підсистему можливо уявити, як структурну схему з *S* сервісів з коефіцієнтом готовності *K*г*s*, який розраховується за формулою (9):

$$K\text{г}s = \prod_{i=1}^{S} K\text{г}i = \prod_{i=1}^{S} T\text{нф}i /(T\text{нф}i + T\text{в}i). \quad (9)$$

Визначимо розрахунок коефіцієнта *K*г для ІТВ, функціонуючого в умовах впливу кібернетичних атак на маршрутизатор з інтенсивністю λ*z*м та на всі сервіси *s* з інтенсивністю λ*zs* (рис. 1). Використовуючи формулу повної ймовірності [12] для сталого режиму функціонування ІТВ, остаточно отримаємо:

$$K\text{г} = \boldsymbol{P}\text{м}K\text{гм} + \prod_{i=1}^{S} \boldsymbol{P}sK\text{г}i, \quad (10)$$

де *K*гм та *K*г*s* розраховуються за формулами (4) та (9) відповідно, а $\boldsymbol{P}$м та $\boldsymbol{P}s$ згідно [13] за формулою (11)

$$\boldsymbol{P}\text{м}=\lambda z\text{м}/(\lambda z\text{м}+\lambda zs), \ \boldsymbol{P}s=\lambda zs/(\lambda z\text{м}+\lambda zs) \text{ де } \boldsymbol{P}\text{м}+\boldsymbol{P}s = 1. \quad (11)$$

Під коефіцієнтом вразливості ІТВ – *Kvr* слід вважати співвідношення інтенсивності потоку атак, які пройшли скрізь захист СКБ – λ*z* до інтенсивності загального потоку λ на вході ІТВ. Відповідно *K*з – коефіцієнт захищеності ІТВ дорівнює 1– *Kvr* [10].

$$Kvr = \lambda z/\lambda, \ K\text{з}=1 – Kvr = 1 – \lambda z/\lambda.$$

Приклад розрахунків

Розглянемо випадок, якщо на кореневий маршрутизатор та сервіси в кількості *S* = 5 впливає не виявлена СКБ кібернетична атака з інтенсивністю відповідно λ*z*м = 1/*T*нфм = 0,01, λ*zs* = 1/*T*нф*s* = 0,02 де *s* = 1, …, 5. Тоді середній час нормального функціонування маршрутизатора *T*нфм = 100 годин, а час нормального функціонування *s*–го сервісу *T*нф*s* = 50 годин, де *s*=1, …, 5. Середній час відновлення працездатності маршрутизатора *T*вм дорівнює 10 годин, а час відновлення працездатності кожного *s* – го сервісу *T*в*s* = 2,5 години, де *s* = 1, …, 5. Розрахуємо при цих вихідних даних значення стаціонарного коефіцієнта готовності ІТВ – *K*г, коефіцієнта вразливості ІТВ – *Kvr* та коефіцієнта захищеності ІТВ – *K*з.

Рішення. Використовуючи формулу (3), (7), (9 – 11) проведемо розрахунки:

*K*гм = *T*нфм /(*T*нфм +*T*вм) = 100/(100,0 + 10,0) = 0,9091;

*K*г*i* = *T*нф*i*/(*T*нф*i* + *T*в*i*) = 50,0/(50,0 + 2,50) = 0,9504;

*K*г*s* = Π*i* *K*г*i* = $0{,}9523^5$ = 0,7458.

Згідно формули (11) розраховуємо значення $\boldsymbol{P}$м та $\boldsymbol{P}s$:

$\boldsymbol{P}$м = λ*z*м/(λ*z*м + λ*zs)* = 0,01/(0,01 + 0,02) = 0,3333,

$\boldsymbol{P}s$ = 1– 0,3333 = 0,6667.

За допомогою виразу (10) розраховуємо значення коефіцієнта готовності *K*г ІТВ в цілому:

*K*г=0,3333 * 0,9091+ 0,6667 * 0,7458 = 0,80022.

У випадку, коли інтенсивність загального потоку кібернетичної атаки λ = 10,0 а λz = 0,03. Тоді *K*з = 1 – *Kv r*= 1 – 0,03/10,0; *K*з = 1 – 0,003 = 0,997, що відповідає нормам захищеності для ІТВ.

Висновки

Таким чином побудована модель для кількісної оцінки ефективності захищеності ІТВ від кібернетичних атак. Проведений аналіз функціонування ІТВ, функціонуючого в умовах кібернетичних атак, дозволив обґрунтувати модель процесу функціонування ІТВ, як відновлювальної системи з обмеженою надійністю елементів та обґрунтувати показники для

розрахунків ефективності функціонування: коефіцієнти готовності, вразливості та захищеності ІТВ.

В подальшому можливо вирішувати ряд практичних завдань, в тому числі оцінити наступне:

якщо надана оцінка активів ІТВ, то використовуючи надану модель можливо буде оцінити втрати нанесені кібернетичними атаками відповідно кожному компоненту ІТВ, а саме кореневому маршрутизатору, сервісу *s* або самій СКБ, яка здійснює захист ІТВ від кібернетичних атак;

оцінити вплив на ефективність кібернетичного захисту таких параметрів, як: час створення шкідливого програмного забезпечення, час оновлення технічного забезпечення, час оновлення обізнаності особового складу та час оновлення вектора організаційних заходів;

розрахувати час відновлення ІТВ у відповідності до вимог допустимого часу непрацездатності ІТВ без наслідків у контурі управління військами.

Рішенню цих задач буде присвячено подальший напрямок досліджень.

ЛІТЕРАТУРА

1. „The Global Risks Report 2019” < URL: https://www.oxfordmartin.ox.ac.uk/publications/world-economic-forum-global-risks-report-2019.

2. Бондаренко І.Д. Діяльність СБ України щодо захисту критичної інфраструктури від кібератак: матеріали всеукр. наук.-практ. конф. „Кібербезпека в Україні: правові та організаційні питання”(Одеса, 30 листопада 2018). Одеса. С. 127 – 129.

3. Аналітична доповідь до Щорічного послання президента України до Верховної Ради України „Про внутрішнє та зовнішнє становище України в 2018 році”. – К. : НІСД, 2018. С. 45 – 47 с. Електронна версія: www.niss.gov.ua

4. Буренин А.Н. Легков К.Е. Первов М.С. Вероятностно-временные характеристики функционирования защищенной агрегативной автоматизированной системы управления сложной системой в условиях интенсивных кибератак. // Наукоемкие в космчесских исследованиях Земли. 2018. Т. 10. № 5. С. 56–53.

5. Легков К.Е., Буренин А.Н. Модели обнаружения атак при управлении оборудованием современной инфокоммуникационной сети специального назначения. Науково-технічний журнал „Наукоемкие технологии в космических исследованиях Земли”. 2013. № 5. С. 26 – 31.

6. Семенов С.Г., Лисица Д.А., Мовчан А.В. GERT-модель начальной генерации кода кибератаки несанкционированного доступа к ресурсам компьютерной системы одноранговой сети. Вісник Національного технічного університету „ХПІ”. Харків. 2016. Вип. № 44. С. 147 – 161.

7. Котенко В.И., Саенко И.Б., Коциняк М.А., Лаута О.С. Оценка киберустойчивости компьютерных сетей на основе моделирования кибератак методом преобразования стохастических сетей. Труди СПИИРАН. 2017. Вип. 6(55). С. 160 – 184.

8. Давиденко В.П. Воронін Є.М. Основи військової кібернетики. Ленінград: ЛВВІУЗ. 1980. 312 с.

9. Жердєв М.К. Лєнков С.В. Креденцер Б.П. Фізичні основи теорії надійності. Підручник. Київський національний університет імені Тараса Шевченка, 2006.

10. Куцаєв В.В. Радченко М.М. Методика оцінки кібернетичної захищеності інформаційно-телекомунікаційного вузла. Збірник наукових праць ВІТІ. Київ, 2018. Вип. № 2.

11. Чередніченко О.М. Куцаєв В.В. Гук О.М. Шугалій О.О. Аналіз кібернетичних інцидентів на території України та базові методи кібернетичного захисту від них. Збірник наукових праць ВІТІ. Київ, 2018. Вип. № 3.

12. Вентцель Е.С. Теория вероятностей. 6-е изд.стер. М.: Высш. шк. В. 1999. С. 134.