УДК 004.056
DOI: 10.31673/2409-7292.2019.020616

**В.А. Савченко, О.Й. Мацько**

# УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ НА ОСНОВІ ТЕОРЕТИКО-ІГРОВОГО ПІДХОДУ

У статті розглядається концепція побудови Ігрової Моделі Кібербезпеки, як засобу, який кількісно ідентифікує ризики кібербезпеки та використовує цю метрику для визначення оптимального пакету засобів захисту відповідно до вкладених інвестицій. Така модель забезпечує максимальну спроможність системи працювати в складному кіберсередовищі, мінімізуючи ризик атаки. Оцінка ризику розраховується на основі сполучення моделі атаки з моделлю топології системи та моделі захисника на основі реалізації припущення щодо успішності нападів.

***Ключові слова:*** управління ризиками кібербезпеки, теорія ігор, ігрова модель, інвестиційний портфель, топологія системи

**Вступ**

Захист інформаційно-телекомунікаційних систем (ІТС) від кібератак поступово перетворюється на національну проблему. Сучасні кіберзлочинці дедалі частіше намагаються викрасти кошти чи приватну інформацію у той час як кібертерористи можуть створити загрозу безпеці громадянам та країні в цілому. Відтак, завдання мінімізації ризиків від різноманітних кібератак є вкрай актуальним.

Теоретичною основою для прийняття рішень щодо безпеки інформаційно-комунікаційних систем є досить значне число моделей і підходів, серед яких окремим напрямом виділяється група ігрових методів. Передбачається, що методи теорії ігор на основі аналізу операційного контенту системи стануть найбільш ефективним засобом при вирішенні питань інвестицій у системи безпеки телекомунікаційних мереж [1]. У результаті застосування теорії ігор можна одержати множину "портфелів безпеки", які є Парето-оптимальними за кількісними параметрами кіберризику та інвестиційних витрат. Ці оптимальні портфелі безпеки дозволяють службам захисту обрати набір засобів, які найкраще знижують загальний кіберризик з огляду на рівень інвестицій у систему безпеки. Таким чином забезпечується рентабельність інвестицій у безпеку мережі. Ігрова модель кібербезпеки (ІМКБ) зможе забезпечити реалізацію цілісного підходу до захисту мережі – від розуміння мети функціонування ІТС до засобів відбиття всіх можливих атак. Крім того, у такій моделі повинна враховуватись реакція порушника на будь-які захисні заходи, оскільки для кожної дії, яка робиться для поліпшення безпеки системи, порушник може робити відповідне коригування вибору найбільш доцільного наступного кроку.

Незважаючи на удавану простоту такої ідеї, при її практичній реалізації виникає проблема кількісної оцінки кіберризику у системі. Для наповнення ІМКБ необхідно формалізувати низку заходів щодо збору інформації для традиційної оцінки ризику та забезпечити перехід до чисельних показників, що описують систему в цілому. Тобто необхідно створити модель топології інформаційної системи та модель потенційного кібервпливу на неї.

**Постановка проблеми та визначення завдань дослідження**

Моделювання в кібербезпеці стикається з низкою проблем. По-перше, проблема починається з формування мети покращення безпеки системи та метрики вимірювання такого покращення. Тобто необхідно мати змогу кількісно оцінити ступінь підвищення кібербезпеки мережі. По-друге, слід забезпечити врахування можливих дій значної кількості експлойтів та засобів кібератак (наприклад, загальна база уразливостей (CVE) налічує понад 120 000 записів, а загальний перелік та класифікація шаблонів атак (CAPEC) нараховує понад 500 зразків атак) [2]. По-третє, необхідно враховувати численні шляхи реалізації атаки та вважати, що порушник може компрометувати декілька компонентів одночасно і може використовувати, на перший погляд, некритичні кіберкомпоненти, такі як обхід засобів захисту (наприклад, як у випадку атаки Stuxnet [3]). По-четверте, слід враховувати

можливість зміни поведінки порушника, оскільки для кожної дії, яку робить захисник для підвищення безпеки системи, порушник здійснить відповідну дію, щоб вибрати наступну найбільш перспективну атаку. Нарешті, інвестиції в кіберзахист повинні здійснюватися з урахуванням обмежених ресурсів, тому необхідно визначити, в які засоби інвестувати та де їх застосовувати, враховуючи такі обмеження.

Класичним підходом до кількісної оцінки кіберризику є оцінка збитку, який спричинено несприятливою подією, з урахуванням ймовірності, з якою ця подія може трапитися протягом певного періоду часу. Незважаючи на такий достатньо простий підхід, на практиці майже постійно використовуються якісні оцінки. У роботі Soo Hoo[7] визначені недоліки якісних підходів та запропоновано певну систематизацію рішень щодо моделювання захисту інформації, шляхом створення ймовірнісної моделі ризику за допомогою діаграм впливу та моделі щорічних втрат.

Іншим підходом є Методологія Операційного Аналізу та Дизайну Ризиків (MORDA) [4] – методологія, яка поєднує в собі загрози, що описуються деревом нападів та концепції впливу для виведення неупередженої метрики ризику. Однак процес їх моделювання потребує залучення декількох експертів з кібербезпеки та ручної розробки дерева атаки. За поглядами багатьох експертів дерева нападів є менш зручними при оцінці ризиків, спричинених інтелектуальними та високопрофесійними противниками. Зокрема в [5] показано, що дерева атак та дерева рішень, які визначають фіксовані ймовірності для порушника постійно занижують ризики захисника. Зокрема, вони не показують зміну ризику захисту у залежності від можливих рішень захисника. Нарешті, в [6] зазначає, що окрім суто технічних засобів, на кібербезпеку також впливають організаційні заходи, що застосовуються у роботі організації (наприклад, управління, навчання). У той же час організаційні питання є поза розглядом цього дослідження.

**Метою** даної статті є розробка складових елементів Ігрової Моделі Кібербезпеки відповідно до запропонованої концепції Парето-оптимальності з урахуванням поведінки порушника та захисника.

**Виклад основного матеріалу**

**1. Підхід щодо комплексної оцінки кіберінцидентів**

Сьогодні досить важко оцінити усю множину засобів та експлойтів порушників, що можуть бути застосовані з метою нападу. Деякі атаки можуть бути ненавмисними, інші – цілеспрямованими [7]. Багато засобів оцінки ризику кібербезпеки зосереджуються на аналізі засобів захисту, які застосовуються до відомих експлойтів [8]. В ІМКБ нам більше цікаво оцінити якість засобів безпеки та чи застосовуються захисні засоби для того, щоб зробити порушника недієздатним.

Враховуючи величезну кількість засобів здійснення атак, моделювання у кібербезпеці стикається з важким питанням: як всебічно оцінити параметри можливих кіберінцидентів? Частина дослідників вирішили цю проблему, зосереджуючичи увагу на наслідках кібератак [9], а не на причинах, які можуть спричинити ці наслідки.

Загальноприйнятим вважається вплив кіберінцидентів на конфіденційність, цілісність та доступність інформації. Кожен інцидент може призвести до певних наслідків. Існує широкий спектр способів обчислення чисельних показників впливу (Байєсівські мережі [9], діаграми впливу [10], графіки залежностей з накопиченням [11], моделі процесів [12]). Однак необхідно більш глибоко знати про різні фактори, які повинні бути враховані при обчисленні зазначених показників.

По-перше, чисельне значення впливу може бути різним залежно від типу кіберінциденту. Наприклад, припинення доступу до окремого ресурсу інформаційної системи може призвести до незначних втрат, тоді як модифікація (порушення цілісності) цього ж ресурсу може призвести до катастрофічних втрат. Засоби оцінки впливу повинні враховувати те, що залежність результатів атаки від факторів впливу може бути різною для кожного типу інциденту. Багато підходів, заснованих на дереві залежностей, зосереджуються

на оцінюванні доступності на основі урахування впливу комбінації окремих факторів [13]. Одинична залежність рідко підходить для урахування при оцінці всіх наслідків інциденту.

У більшості випадків використовуються спрощені моделі[12], які описуються формулою "ризик = загроза (T) × уразливість (V) × наслідок (C)". Експерти оцінюють загрози та уразливості у ймовірнісній формі. Наслідки можуть бути оцінені у будь-яких одиницях (наприклад, економічний прибуток, матеріальні збитки). Суть процесу полягає у визначенні наміру противника (загрози) та вибору доцільних засобів захисту у залежності від виду загрози [14]. Однак дехто з експертів висловлює занепокоєння щодо моделі ризиків на основі (T,V,C). Так, Cox [15] ілюструє приклади того, як (T,V,C) моделі можуть давати безглузді поради. Також Cox [16] відзначає, що оскільки значення V і C дійсно залежать від кількості зусиль, витрачених як порушником, так і захисником, тому вони не завжди можуть розглядатися як незалежні змінні.

Важливим аспектом ІМКБ є те, що вона повинна фокусуватися на комплексному захисті від загроз операційним результатам, а не просто на захисті від окремих ризиків. Ігрова модель визначає ризик окремого інциденту як добуток ймовірності виникнення кіберінциденту ($P_i$) та очікуваних збитків від нього ($L_i$).

$$Risk = \sum_{i=1}^{N} P_i L_i \,, \tag{1}$$

Також ігрова модель визначає загальний системний ризик (TSR), як підсумок всіх ризиків інциденту, пов'язаних з можливим набором інцидентів, які може спричинити порушник (1) [17]. Крім того, ризикоорієнтоване рішення може зосередити увагу на найгіршому сценарії ризику, визначеному рівнянням

$$Risk = \underset{i=1,N}{Max}\left[P_i L_i\right]. \tag{2}$$

Обидва способи визначення системного ризику представлені в Ігровій моделі (1) – (2).

Вираз (1) спрощено представляє загальний системний ризик TSR. Розраховане значення TSR – це наближена оцінка ризику у системі. При застосуванні моделі застосовується припущення, що всі складові ризику у сумі незалежні: збільшення однієї складової не впливає на загальний системний ризик більше, ніж локальний приріст.

У контексті зіткнення інтелектуального порушника із захистом системи порушник може одночасно скомпрометувати декілька компонентів для створення бажаного впливу (досягти втрат захисника). Тому засоби, які враховують лише ризик нападу не можуть визначати критичні сценарії. Більше того, вразливості, пов'язані з атакою на декілька компонентів, рідко залежать одна від одної (тобто, один і той же експлойт може бути ефективним проти декількох компонентів захисту одного типу). Тому ризики, пов'язані із наявністю компонентів захисту одного типу, не є тими самими, що ризики наявності різноманітних компонентів. Засоби, які не враховують подібні взаємозалежності, можуть ввести в оману та привести до неправильних рішень.

**Моделювання способів атаки.** Оскільки захисник мережі стикається з розумним противником, він повен бути в змозі ідентифікувати та захищатися від багатоступеневих атак. Завдяки взаємопов'язаності окремих елементів ІТС порушники можуть використовувати, здавалося б, некритичні компоненти, як спосіб обійти засоби захисту. Тому, необхідно враховувати, як поєднання інцидентів та некритичних системних ІТ-компонент сприяють ризикам. Окремий інцидент сам по собі може не вплинути, але може слугувати кроком для наступних атак. Багато засобів оцінки ризику [18] або не розглядають ці некритичні ресурси інформаційної системи, або моделюють їх неявно.

Популярний спосіб визначення шляхів атаки та моделювання поведінки порушників – через дерево нападів. Такі дерева, як правило, розробляються вручну[8], але їх ймовірнісні показники можна обчислити за допомогою моделей системної топології. Типове застосування таких моделей зосереджується на аналізі топологічної вразливості. Цей підхід був узагальнений у роботі [19] для обчислення системної метрики під назвою "*k*-нульовий день безпеки". Цей показник підраховує кількість унікальних експлойтів, які знадобляться для досягнення цілі. Ігрова Модель Кібербезпеки повинна ще більше узагальнювати цей підхід, використовуючи ймовірнісну модель порушника та враховуючи всі потенційні цілі удару.

**Моделювання поведінки порушника.** Ще одним складним фактором захисту є те, що на кожну дію, яку захисник робить для захисту системи, порушник здійснює відповідне коригування атаки, щоб знайти наступний більш перспективний крок. Дерева атаки фіксують варіанти обходу порушником захисних сил, але не відображають, як на дерево впливають заходи захисту. Щоб вирішити цю проблему, кібератаки та відповідні захисні дії, які можуть їм запобігти, треба розглядати як гру між двома гравцями [20]. Незважаючи на це, лише незначна кількість засобів управління ризиками одночасно включають кроки порушника та захисника. Ті, хто це робить, зосереджуються на: оптимізації конкретного засобу захисту, не розглядають декілька засобів одночасно, або мають невизначені способи, що стосуються відбиття атак [21]. У [22] порівнюють теоретичні рішення та теоретичні ігрові підходи до інвестицій в ІТ-безпеку, зосереджуючи увагу на фірмі та хакерові. У [23], з іншого боку, вважають теорію ігор взаємозалежною безпекою, але їхні рішення дискретні, тобто інвестувати чи ні. ІМКБ має узагальнювати поведінку порушника, застосовуючи ігрово-теоретичний підхід, заснований на обмеженнях, які нападає на атакуючу структуру системи та захист.

**Визначення найкращих інвестицій.** У [24] обчислюють граничну норму прибутковості інвестицій, орієнтуючись на зменшенні загрози. Їх модель дещо спрощена і високорівнева, заснована на значенні ризику втрати, загрози та вразливості (T,V,C). Тут збиток пов'язаний з активом, або множиною активів. Складні загрози, що призводять до суттєвих втрат, поєднуються в єдину загрозу, а засіб протидії їм зосереджується на зменшенні вразливості. Однак засіб нічого не знає про самі кіберкомпоненти, тому він не може зробити наступне: визначити шляхи, за допомогою яких порушник може отримати доступ до активу; засіб не може явно міркувати про диверсифікацію компонентів або зменшення привілеїв; нарешті, засіб не враховує жодних відповідей порушників на розгортання засобів захисту.

В даний час існує низка засобів оцінювання кіберризиків, які зосереджені на розподілі ресурсів за рейтингом ризику або виробляють список найбільш небезпечних ризиків для системи. Нажаль, класифікація ризиків не є придатною для розподілу ресурсів, оскільки класифіковані ризики не враховують як саме порушник адаптується перед діями захисника. Визначення найкращих засобів захисту та місця їх застосування сильно залежить від наявних ресурсів захисників. Тому ІМКБ має включати механізм роботи з портфелем інвестицій, оптимізуючи їх за обмежених ресурсів.

**2. Методологія Ігрової Моделі Кібербезпеки**

ІМКБ є алгоритмом, який базується на використанні трьох основних моделей: *топології* системи, середовища *загроз* та можливих *дій* захисника. Кожна з моделей робить свій внесок у загальний результат щодо визначення доцільного пакету інвестицій. ІМКБ автоматизує ряд можливостей експертного рівня (наприклад, виявлення шляху атаки та аналіз портфеля інвестицій), тому захисникам не потрібно робити це вручну. Коли ключові аспекти системи – захист або загрози змінюються (виявляються нові вразливості), захисник може оновити відповідну модель, на яку впливає зміна, і повторно застосувати ІМКБ для оцінки нових умов. ІМКБ розроблено для аналізу та інформування керівників на системному рівні щодо рішень про належні принципи проектування систем безпеки, цілеспрямоване

вдосконалення, економічно ефективні інвестиції у зменшення ризику та де слід застосовувати захисні засоби.

ІМКБ не може бути використана для аналізу на макрорівні. Її математична модель враховує те, як на порушника впливає конфігурація системи. Модель порушника в ІМКБ використовує такі фактори, як топологія мережі, відносини доступу та тип компонентів захисту. Це по суті замінює компоненти загрози та вразливості, що часто використовуються для (T,V,C) у багатьох моделях визначення ризику.

ІМКБ здійснює пошук за допомогою комбінаторики можливих кіберінцидентів, шляхів нападу, атак та засобів захисника. ІМКБ формулюється як гра двох осіб з нульовою сумою (де і порушник, і захисник присвоюють однакове значення для прибутку або втрати). Вона реалізує раціональний підхід до прийняття рішень щодо кібербезпеки, де обидва гравці використовують якнайкраще свої можливості і працюють, щоб найкращим чином протидіяти діям один одного. ІМКБ оптимізує своє рішення, припускаючи, що порушник знає або може дізнатися все про систему, яку він атакує. Суть гри в ІМКБ полягає в процесі налаштування гравцем-захисником захисту у своїй системі. Тоді гравець-порушник припускає, що система не має відомих вразливих місць і оцінює, наскільки важко було б йому компрометувати компоненти з найбільшим впливом. Гра продовжується, дозволяючи гравцеві-захиснику перенастроювати або використовувати додаткові захисні засоби. Після цього знову враховується те, що гравець-порушник переосмислить складність спричинення наслідків з урахуванням змін, що відбулися. Це інша гра, ніж та, що намагається захистити систему в режимі реального часу на тлі виявленої діяльності порушника. Спроби обдурити, затримати або стримувати порушника протягом короткого терміну мотивують іншу ігрову постановку. Зокрема різні варіанти показані у [25].

Показник ефективності у ІМКБ – це показник системного ризику, визначений за рівнянням (1) або (2) залежно від бажання захисника. Для кожного стану гри гравець-порушник генерує дерево атаки (яке враховує кілька компромісів), щоб виявити наслідки, які вони можуть спричинити. Гілки дерева-атаки забезпечують впливи та ймовірності, використані в рівнянні (1), щодо оцінки ризику. MiniMax використовується для вивчення того, як кожен засіб захисника може найкраще знизити показник ризику.

Оскільки захисник несе витрати то гра закінчується за двох умов. Перший – це коли гра визначає оптимальний набір засобів захисту, які слід використовувати, коли захисник витратив виділену на них суму грошей. Другий – це коли проводиться повний аналіз портфеля для обчислення межі Парето для кожної цінової точки.

На рис. 1 показано результат застосування ІМКБ, графік вартості та ефективності кожного варіанту портфеля. Точки на нижній межі показують Парето-оптимальні варіанти. Ця конкретна система мала номінальний кіберризик, коли не застосовувалися захисні засоби. ІМКБ показує, що ризик можна знизити до 110 тис. у.о., використовуючи всі засоби оборони та вклавши кошти у розмірі 45 тис. у.о. Однак інвестиція у розмірі лише 10 тис. у.о. може зменшити оцінку ризику до 190 тис. у.о. Це ілюструє, що для цієї системи можна отримати 90% найкращого можливого зниження ризику при 20% вартості цього максимального зниження.

Отже, навіть такий простий приклад застосування ІМКБ показує, що не обов'язково витрачати багато щоб досягти максимуму, оскільки лише незначна поступка у захисті здатна дати доволі суттєвий економічний прибуток. ІМКБ дає змогу вирішити таку проблему, візуалізуючи таким чином можливість прийняття оптимального чи квазіоптимального рішення.

**Моделювання наслідків інциденту.** Для визначення наслідків (втрат), спричинених кіберінцидентами $L_i$ з рівняння (1) ІМКБ використовує модель процесу, яка фіксує деталі атаки, такі як: тривалість діяльності ІТС, ресурси ІТС, часові обмеження та потоки управління. При цьому ресурси ІТС ув'язуються з наслідками атаки. Моделі процесів можуть бути імовірнісними та стохастичними, дозволяючи обмежити невизначеності, пов'язані з моделлю ІТС. Запуск комбінаторики щодо набору ефектів кіберінцидентів проти

всіх ІТС-ресурсів системи дозволяє оцінити вплив та критичну оцінку експертами з питань атак та дозволяє ІМКБ пройти всі можливі наслідки кіберінцидентів, які можна оцінити за допомогою MiniMax.

Впливи, що входять до моделі ІМКБ, повинні бути пов'язані з результатами атаки, яких не слід допускати (наприклад, смерть людини) або яких слід уникати, якщо це можливо. Якщо існує невизначеність параметрів або впливів, їх можна представити при розподілі. Це дає змогу визначити межі, пов'язані з невизначеністю (подібно до подання ймовірності втрат у моделях VAR [26]). Перш ніж запустити ІМКБ, користувач має вирішити, де він бажає опинитися на кривій розподілу впливу (тобто, який рівень впливів неприйнятний).

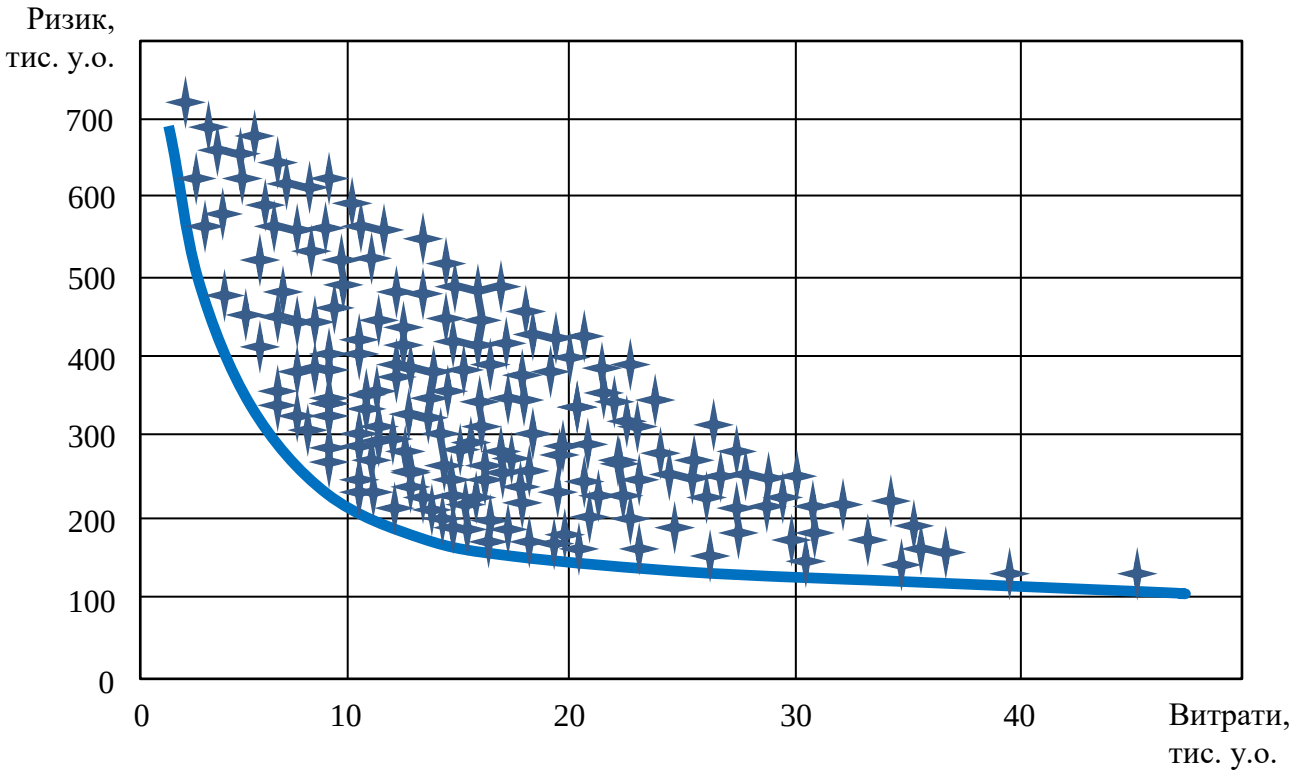



Рис. 1. Ефективність портфеля безпеки порівняно з вартістю

Моделі ІМКБ містять моделі процесів діяльності, пов'язаної з ІТС. Моделі рівня ІТС розробляються шляхом визначення діяльності та взаємопов'язаного процесу, пов'язаного з ресурсами (компонентами) ІТС. Прикладами ресурсів ІТС є обладнання, програмне забезпечення та дані. Процес захисту ІТС – це сукупність заходів, що спираються на ресурси ІТС, які необхідно виконати для підтримки деяких процесів під час атаки. Ці ІТС-процеси, як правило, отримуються шляхом відстеження залежностей від ІТС на мережевій діаграмі. Кожен ресурс ІТС на цьому шляху повинен виконувати діяльність для досягнення успіху. Кожна діяльність в галузі ІТС призначається тим впливам, які були б спричинені, якби на неї впливав кожен з різних кіберефектів моделі.

**Моделювання порушника.** Модель атаки визначає ймовірність того, що атаки матимуть успіх, враховуючи топологічні обмеження, які система надає порушнику. Для того, щоб порушник впливав на ресурси ІТС, які можуть спричинити значні наслідки, порушник повинен знайти шлях до них. Модель атаки визначає дві точки доступу для порушника. Порушники можуть спробувати увійти з Інтернету або бути інсайдерами. З будь-якої точки входу порушник може потім переміщатися по мережі, щоб дістатися до ресурсів ІТС, які можуть спричинити вплив. Модель порушника характеризує здатність порушника рухатися по мережі у вигляді серії кроків атаки, кожен з яких може досягти успіху. Модель атаки обумовлює ймовірність успіху нападу за такими характеристиками:

чи намагається порушник скомпрометувати компонент, до якого він може безпосередньо підключитися (тобто всередині мережі, в якій вони вже є), чи цей компонент знаходиться в іншій мережі, що вимагає переходу межі мережі для доступу;

чи той компонент того ж типу, що і компонент, який уже скомпрометований;

чи відомо, що компонент вразливий до відомих експлойтів, якими, можливо, володіє поточний порушник;

чи компонент є сервером, який містить одну або кілька мережевих служб;

чи можуть користувачі, які мають доступ до кожного ресурсу, використовувати ці ролі для доступу до інших компонентів мережі для створення впливів.

На рис. 2 показано приклад обчислення ймовірності успіху порушника для топології системи. Припустимо, що порушник спершу намагатиметься атакувати хост клієнта H-2. На діаграмі видно, що клієнт H-2 може бути успішно скомпрометований з-за меж мережі з ймовірністю $P(\text{S}|\text{зовнК.})$, де $S$ визначається як вдала атака. Якщо атакований хост є сервером тоді як ймовірність успіху буде використано $P(\text{S}|\text{зовнС.})$. Клієнт-хост H-2 також може бути скомпрометований зловмисним інсайдером із внутрішнім доступом з ймовірністю $P(\text{S}|\text{внутр.})=1-\prod_{i=1}^{N}(1-P(\text{S}|\text{U}_i))$, де $N$ позначає кількість користувачів $\text{U}_i$, які мають доступ.

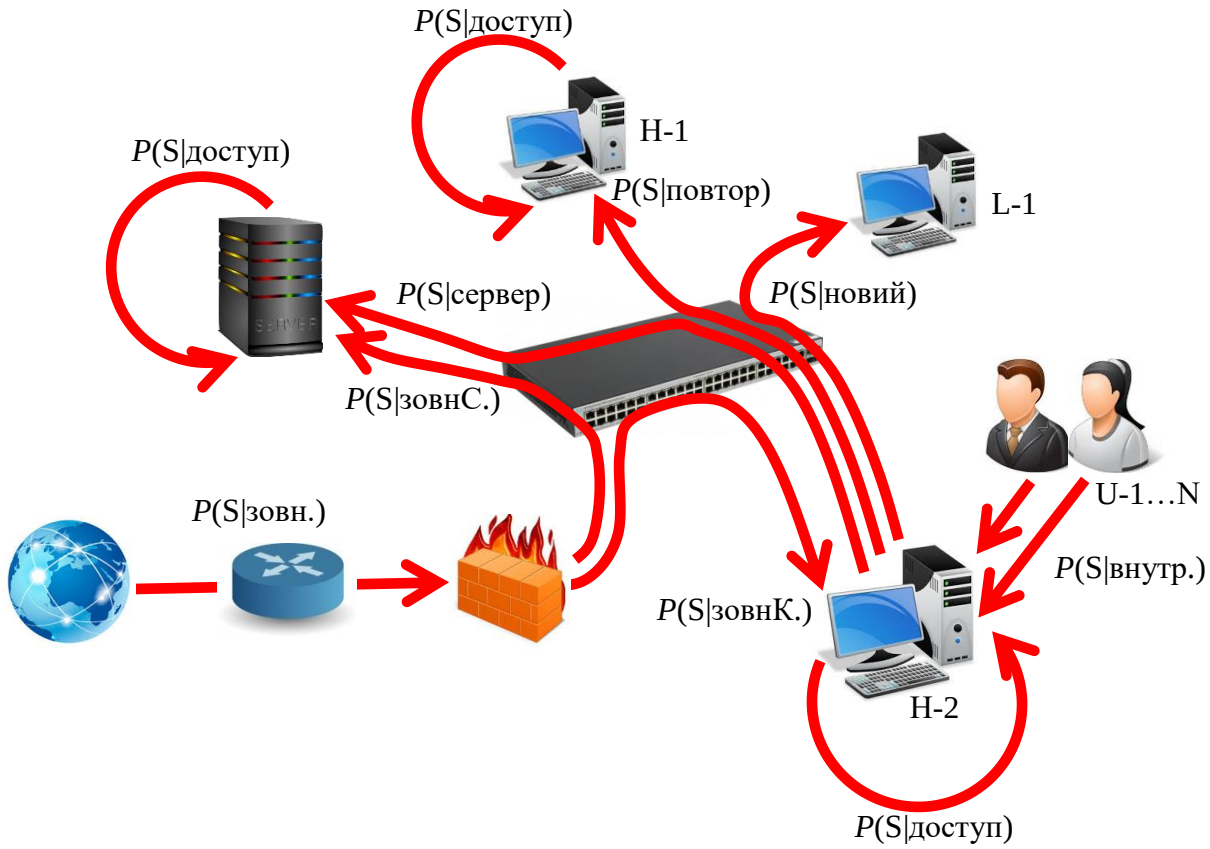



Рис. 2. Модель атаки

Після того, як хост H-2 зламано, порушник має доступ, і тому додатки або дані, що знаходяться на цьому хості, можуть бути порушені з імовірністю $P(\text{S}|\text{доступ})$. Оскільки хост H-1 – це той самий тип клієнта, що і H-2, то той самий експлойт, що використовується для компромісу H-2, має високі шанси також мати можливість скомпрометувати H-1 з ймовірністю $P(\text{S}|\text{повтор})$. Оскільки хост L-1 є клієнтським комп'ютером іншого типу, ніж H-1, у нього будуть інші шанси на успіх, а саме $P(\text{S}|\text{новий})$. Сервер може бути оцінений

ймовірністю *P*(S|сервер), оскільки він є іншим типом хостів, ніж Н-2, а оскільки це сервер, то сервери мають мережеві послуги, які також можна експлуатувати.

Імовірність успішної навігації по мережі та компрометація компонентів обчислюється за допомогою ланцюгового правила обчислення умовних ймовірностей

$$P(A_1, A_2, \ldots, A_n) = P(A_1 | A_2, \ldots, A_n) P(A_2 | A_3, \ldots, A_n) \ldots P(A_{n-1} | A_n) P(A_n).$$

**Моделювання способів здійснення атаки.** Для оцінки ризику за допомогою ІМКБ необхідно оцінити ймовірність того, що наслідки відбудуться, враховуючи особливості топології системи. Тому їй потрібна модель топології. Топологічна модель являє собою взаємозв'язок ресурсів ІТС. До них відносяться кіберкомпоненти, програми, дані, групи облікових записів користувачів та брандмауери контролю доступу, які реалізують довірчі відносини. Елементи в топологічній моделі включають як єдині ресурси ІТС, так і пули ресурсів ІТС, які представляють функціонально ідентичні групи ресурсів одного типу. Модель системної топології вимагає інформації про тип ресурсу для кожного ресурсу ІТС, і використовує це для оцінки того, коли той самий порушник з попереднього кроку може бути використаний повторно. Наявність підключень, правил брандмауера та доступ до ролей користувача визначає можливості та обмеження зв'язку між ресурсами ІТС.

З урахуванням моделі атаки (рис. 2) модель топології дозволяє автоматизувати обчислення дерева атак. Цей процес проілюстрований на рис. 3.

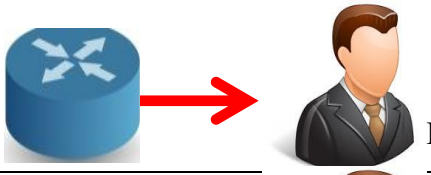
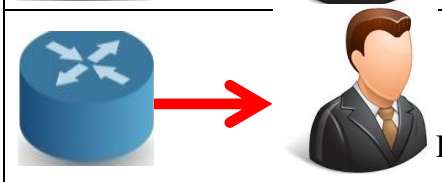
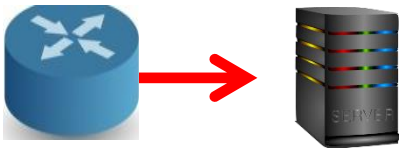
| | |
|---|---|
|  Н-2 | *P*(Н-2) = *P*(S\|зовн.) · *P*(S\|зовнК.) · *P*(S\|доступ) |
|  Н-1 | *P*(Н-1) = *P*(S\|зовн.) · *P*(S\|зовнК.) · *P*(S\|повтор) · *P*(S\|доступ) |
|  | *P*(Серв.) = *P*(S\|зовн.) · *P*(S\|зовнК.) · *P*(S\|сервер) · *P*(S\|доступ)<br>*P*(Серв.) = *P*(S\|зовн.) · *P*(S\|зовнС.) · *P*(S\|доступ) |
| … | … |

Рис 3. Розрахунок ймовірності проникнення у систему

На рис. 3 наведено фрагмент дерева атаки з мережі Інтернет тому, що раціональні порушники завжди використовуватимуть оптимальний шлях для компрометації компонента в системі. Оскільки ми оцінюємо ризики в контексті MiniMax і оскільки компроміс з інсайдерськими обліковими записами має менше шансів на успіх, ніж атаки з Інтернету, то з цього дерева їх доцільно видалити. Незважаючи на це, навіть такий невеликий приклад показує, що для реальної адекватної оцінки необхідно створити більш масштабне дерево атаки. В кінці кожного шляху в дереві атаки обчислюється очікуване значення (виходячи з найгіршого можливого впливу та ймовірності проходження кроків на шляху атаки). Створюючи дерево атаки, необхідно враховувати різні шляхи для досягнення однакових впливів. Це тому, що довірчі відносини (тобто, як вони накладаються правилами

брандмауера) не обов'язково є симетричними за напрямом і кожен шлях може мати різну ймовірність успіху.

Оскільки порушникові, щоб спричинити наслідки, можливо, доведеться поставити під загрозу кілька ресурсів ІТС, необхідно розглянути достатньо велику кількість кроків вперед для виявлення цих випадків. Дивлячись лише на крок вперед, порушник не може визначити багато критичних сценаріїв. У ІМКБ ця кількість кроків атаки для дослідження є параметром, який можна встановити. Зазвичай, якщо система не складається з багаторівневих оборонних меж, для більшості систем достатньо прогнозу на 3–4 кроки вперед.

**Обчислення оцінки ризику.** Дерево атаки, створене шляхом дослідження шляхів, містить інформацію, необхідну для складання оцінки ризику за допомогою рівняння (1). Кожна гілка дерева являє собою унікальний варіант для порушника. Кожен вузол на дереві представляє очікуване значення втрат захисника (EV), якщо порушник має намір застосувати цей варіант. EV – це поєднання втрати, спричиненої атакою, та ймовірністю виконання всіх кроків для реалізації атаки. Імовірність виконання всіх етапів випливає із застосування правила ланцюга щодо ймовірності виконання кожного кроку у гілці. Захисник, який грає в гру, отримує кредит за зменшення цих ризиків. Захисники системи можуть зосередитись на найгіршому випадку ризику на дереві, використовуючи рівняння (2), оскільки деякі захисні засоби можуть працювати для зменшення загального ризику, але нічого не роблять для зменшення найгіршого ризику у дереві (2). Кожне рівняння ризику може призвести до необхідності іншого захисного портфеля, щоб оптимально захищатись від нього.

**Моделювання засобів захисту.** Для того, щоб можна було оцінити дії захисника, ІМКБ аналізує варіанти засобів захисту, що застосовуються (табл. 1).

Таблиця 1

**Перелік засобів захисту**

| **Категорія засобів захисту** | | **Криптозахист** | **Управління конфігурацією сервера** | **…** |
|---|---|---|---|---|
| Метод захисту | | Encrypt Disk & transport Layer | Server Configuration Management | |
| Область застосування | | Mobile Dvc | Harden | |
| Назва засобу | | LUKS & TLS | EHR Server | |
| Вартість | встановлення | $1000 | $2000 | |
| | обслуговування | $0 | $2000 | |
| | застосування | $50 | $100 | |
| | ВСЬОГО | $1050 | $4100 | |
| Показники ефективності щодо захисту | Переривання | 0 | 20 | |
| | Модифікація | 40 | 20 | |
| | Фабрикація | 40 | 20 | |
| | Неавтор. використ. | 40 | 20 | |
| | Перехоплення | 60 | 20 | |

Як правило, засоби захисту зосереджені на зменшенні ймовірності успіху інцидентів. Зазвичай це здійснюється одним із двох способів. Перший – захист самих кіберресурсів, а другий – зміна доступу. Кожен засіб захисту вимагає оцінки ефективності. У таблиці наведено: категорія засобу, назва засобу, конкретні ресурси ІТС, які призначені йому для захисту, мета застовування засобу, кошторис витрат на використання засобу та оцінка ефективності засобу. Ця оцінка ефективності визначається 100 бальною шкалою. 0 означає,

що засіб не має жодної користі для запобігання ефекту, а оцінка 100 означає, що він зупиняє всі атаки, які спричинили б цей ефект. Інтерпретація полягає в тому, що оцінка, наприклад 40, означає, що 40% зловмисних експлойтів, які очікуються, не матимуть успіху.

Засоби захисту обираються у залежності від їх ефективності та вартості захисту. Підхід щодо захисту, заснований на аналізі дерев атак, дає змогу досліджувати різні варіанти захисту. Так, включення резервного сервера, наприклад, дає додатковий шлях для процесу і інцидент, що зачіпає оригінальний сервер, не спричинить впливу на додатковий сервер. Однак, оскільки ІМКБ розглядає дії порушника на декілька кроків вперед, то в решті решт, вона зможе визначити атаку порушника, яка скомпрометує обидва сервери. Ймовірність успіху атаки можна зменшити, змінивши топологію мережі або змінивши порядок контролю доступу. Ризики також можуть бути зменшені за рахунок об'єднання засобів захисту або, диверсифікувавши компоненти в системі, щоб та сама атака не могла повторно бути застосована на них.

Захист в ІМКБ може моделюватися і застосовуватися протягом усього життєвого циклу атаки. Захист може варіюватися від таких заходів, як перевірка працівника для зниження шансів на перетворення його на інсайдера, до засобів реагування (бек-апів), які повертають скомпрометований компонент в робочий стан протягом певного часу.

**Прийняття рішень за допомогою Ігрової Моделі Кібербезпеки.** Головним призначенням ІМКБ є забезпечення можливості приймання рішень щодо інвестицій у кібербезпеку. Оскільки кожен засіб захисту може зменшити кібер-ризик системи, враховуючи пов'язані з цим витрати, ІМКБ автоматично визначає оптимальний портфель (тобто, комбінацію засобів оборони) для будь-якого рівня інвестицій. Поєднання загального зменшення ризику із витратами – найкращий спосіб зрозуміти рентабельність інвестицій.

**Висновки**

Застосування ігрових моделей при вирішенні питань інвестицій у системи безпеки телекомунікаційних систем дає змогу одержати множину "портфелів безпеки", які є Парето-оптимальними за кількісними параметрами кіберризику та інвестиційних витрат. Ці оптимальні портфелі безпеки дозволяють службам захисту обрати набір засобів, які найкраще знижують загальний кіберризик з огляду на рівень інвестицій у систему безпеки. Таким чином забезпечується рентабельність інвестицій у безпеку мережі.

Ігрова модель кібербезпеки може забезпечити реалізацію цілісного підходу до захисту мережі – від розуміння мети функціонування ІТС до засобів відбиття всіх можливих атак. Крім того, у такій моделі враховується реакція порушника на будь-які заходи захисту, оскільки для кожної дії, яка робиться для поліпшення безпеки системи, порушник може робити відповідне коригування найбільш доцільного наступного кроку.

Напрямком подальших досліджень можуть бути різноманітні аспекти удосконалення ігрових моделей кібербезпеки, які б інкапсулювали можливості експертного, технічного та алгоритмічного рівнів захисту.

**Список використаної літератури**

1. Musman, S. and Turner, A. A game theoretic approach to cyber security risk management. Journal of Defense Modeling and Simulation: Applications, Methodology, Technology 2018, Vol. 15(2) 127–146.
2. MITRE. Making security measurable, https://makingsecuritymeasurable.mitre.org/
3. Lagner, R. To kill a centrifuge. The Langner Group, http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf
4. Buckshaw, DL, Parnell, GS, Unkenholz, WL. Mission Oriented Risk and Design Analysis of Critical Information Systems. Mil Op Res 2005; 2: 19–38.
5. Тецкий А. Г. Применение деревьев атак для оценивания вероятности успешной атаки web-приложения // Радіоелектронні і комп'ютерні системи, 2018, № 3(87) – С. 74-78.
6. Anderson, R. Why information security is hard-an economic perspective. In: Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC '01), Sheraton New Orleans Louisiana, USA, 10–14 December 2001, pp. 358–365.

7. Лукацкий А. Определение источника кибератак // Индекс безопасности. 2018. – № 2 (113), Том 21. С. 73-86.

8. Jajodia, S, Noel, S. Topological vulnerability analysis. In: Cyber situational awareness. Boston, MA: Springer, 2010, pp.139–154.

9. de Barros Barreto, A, Costa, PCG, Yano, ET. A semantic approach to evaluate the impact of. In: Proceedings of the 7th international conference on semantic technologies for intelligence, defense, and security (STIDS 2012), Fairfax, VA, USA, 23–26 October 2012.

10. Sommestad, T, Nordström, L. Modeling security of power communication systems using defense graphs and influence diagrams. 2009; 24.

11. Garvey, PR, Patel, SH. Analytical frameworks to assess the effectiveness and economic-returns of cybersecurity investments. In: Military communications conference (MILCOM), 2014.

12. Noel, S, Ludwig, J, Jain, P., Analyzing Mission Impacts of Cyber Actions (AMICA). In: Kott, Alexander (ed.) Workshop proceedings, Istanbul, Turkey, June 2015, pp.80–86.

13. Зегжда Д.П., Васильев Ю.С., Полтавцева М.А., Кефели И.Ф., Боровков А.И. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации. Вопросы кибербезопасности. –№ 2 (26). – 2018. – С. 2–15.

14. Bier, VM. Choosing what to protect. Risk Analysis 2007; 27: 607–620.

15. Cox, A. Some limitations of risk = threat × vulnerability × consequence for risk analysis of terrorist attacks. Risk Analysis 2008; 28(6): 1749–1761.

16. Cox, A. What's wrong with hazard-ranking systems? An expository note. Risk Analysis 2009; 29(7): 940–948.

17. Киричок Р. В. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення / Р. В. Киричок, П. М. Складанний, В. Л. Бурячок, Г. М. Гулак, В. А. Козачок // Наукові записки Українського науково-дослідного інституту зв'язку. - 2016. - № 3. - С. 48-61.

18. Carin, L, Cybenko, G, Hughes, J. Cybersecurity strategies: The QuERIES methodology. Computer 2008; 41: 20–26.

19. Lingyu, W, Jajodia, S, Singhal, A. k-zero day safety: Measuring the security risk of networks against unknown attacks. In: IEEE transactions on dependable and secure computing, 11 June 2013, pp.30–44.

20. Roy, S, Ellis, C, Shiva, S. A survey of game theory as applied to network security. In: 43rd Hawaii international conference on system sciences (HICSS), Koloa, 5–8 January 2010, Piscataway, NJ: IEEE Conference Publication.

21. Губанов Д. А., Калашников А. О., Новиков Д. А. Теоретико-игровые модели информационного противоборства в социальных сетях // Управление большими системами. 2017. Выпуск 31. 192-204.

22. Cavusoglu, H, Raghunathan, S, Yue, WT. Decision-theoretic and game-theoretic approaches to IT security investment: Impact of information systems on market structure and function: Developing and testing theories. Journal of Management Information Systems Fall, 2008; 25(2): 281–304.

23. Kunreuther, H, Heal, G. Interdependent security. Journal of Risk and Uncertainty 2003; 26: 231–249. DOI: 10.1023/A:1024119208153.

24. Gordon, L, Loeb, M. The economics of investment in information security. Journal ACM Transactions on Information and System Security (TISSEC) November 2002; 5(4): 438–457.

25. Roy, S, Ellis, C, Shiva, S. A survey of game theory as applied to network security. In: 43rd Hawaii international conference on system sciences (HICSS), Koloa, 5–8 January 2010, Piscataway, NJ.

26. Hulthen, R . Communicating the economic value of security investments; value at security Risl. In: WEIS 2008 – Seventh workshop on economics of information security, Hanover, N.H., 2008.

Надійшла: 11.05.2019 Рецензент: д.т.н., проф. Барабаш О.В.