DOI 10.20535/2411-1031.2019.7.1.184217
УДК 004.056.53

СЕРГІЙ САЛЬНИК,
АНТОН СТОРЧАК,
АРТЕМ МИКИТЮК

МОДЕЛЬ ПОРУШЕННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ КОМУНІКАЦІЙНИХ СИСТЕМ

Представлено модель порушення захищеності інформаційних ресурсів, що обробляються в комунікаційних системах. Описано основні функції системи забезпечення безпеки як одного з елементів комунікаційної системи. Показано, що вразливості її складових призводять до порушення захищеності інформаційних ресурсів та сприяють реалізації загроз їх безпеці. Модель порушення захищеності інформаційних ресурсів розроблено на основі множини вразливостей комунікаційних систем. Розглянуто перелік загроз безпеці інформаційних ресурсів, види атак на всіх рівнях базової еталонної моделі взаємодії відкритих систем, приклади реалізації атак та стратегії проведення атак зловмисником: вплив варіанту атаки на окремий об'єкт або множину об'єктів комунікаційної системи, вплив множини варіантів атак на окремий об'єкт або множину об'єктів комунікаційної системи. Це дозволило встановити можливості зловмисника при реалізації атак на інформаційні ресурси комунікаційних систем. Розроблену модель запропоновано взяти за основу побудови підсистеми оцінювання захищеності інформаційних ресурсів комунікаційної системи. Крім цього використано методи оцінювання захищеності інформаційних ресурсів від внутрішніх та зовнішніх загроз. Підсистема оцінювання захищеності комунікаційних систем враховує множини всіх можливих загроз та елементів комунікаційних систем. На основі проведеного аналізу загроз безпеці інформаційних ресурсів та структурних складових комунікаційних систем отримано аналітичні вирази для оцінювання імовірності реалізації порушень захищеності інформаційних ресурсів комунікаційних систем на всіх рівнях базової еталонної моделі взаємодії відкритих систем. Встановлено, що виявлення атак в комунікаційних системах залежить від швидкості адаптації системи забезпечення безпеки до нових загроз. Використання отриманої моделі порушення захищеності дозволить розробити методи оцінювання рівня захищеності від внутрішніх та зовнішніх загроз для визначення ефективності функціонування системи захисту інформації в режимі реального часу. Це дозволить підвищити загальний рівень захищеності комунікаційних систем та інформаційних ресурсів, що в них обробляються.

Ключові слова: комунікаційні системи; інформаційні ресурси; порушення захищеності; підсистема оцінювання захищеності; модель порушення захищеності.

Постановка проблеми. У зв'язку з тим, що система забезпечення безпеки (СЗБ) комунікаційних систем має реалізовувати прийняту політику безпеки, керувати розмежуванням доступу, контролювати відповідності загальносистемного середовища еталону, сигналізувати про небезпечні події, виявляти атаки на інформаційні ресурси (ІР), проводити оцінку захищеності системи та вживати заходи щодо підтримання належного рівня безпеки систем електронних комунікацій або комунікаційних систем (КС) [1], [2], то СЗБ необхідно відслідковувати весь трафік, що циркулює в КС. Для цього СЗБ забезпечує своє функціонування на всіх рівнях базової еталонної моделі взаємодії відкритих систем (Open System Interconnection Reference Model – моделі OSI), здійснюючи при цьому: контроль з'єднань, аналіз структури та вмісту мережевих пакетів, контроль трафіку, оцінку станів функціонування елементів системи.

При використанні КС в управлінні інформаційними ресурсами, метою порушення захищеності КС може бути приховане управління кінцевими та мережевими ресурсами або

вплив на інформаційні, програмні та апаратні засоби КС. Реалізація зазначеної мети досягається методами, що направлені на використання вразливостей КС. Це може призвести, наприклад, до втрати ІР внаслідок віддаленого керування вузловим або мережевим обладнанням або його захоплення [2]. Моделювання порушення захищеності ІР, що обробляються в КС, потребує розробки та дослідження нових підходів.

Аналіз останніх досліджень і публікацій. Питання протидії реалізації загроз, класифікації вразливостей і загроз безпеці КС та моделювання систем захисту ІР в КС розглядалися в [3] - [11]. До основних вимог, що висуваються при побудові моделей порушення захищеності ІР в КС належать: можливість розрахувати ймовірність реалізації загрози в залежності від використаних засобів захисту, вразливостей в них і рівня підготовки зловмисника; можливість розрахувати час виявлення атаки в залежності від використаних засобів захисту, вразливостей в них і рівня підготовки зловмисника; простота визначення вхідних параметрів моделі. В [8] представлено класичні і сучасні моделі процесу захисту ІР та процесу порушення захищеності ІР, що обробляються в КС. Відомі підходи до моделювання захисту і порушення захищеності ІР використовують різний математичний апарат, враховують питання доступу суб'єктів до об'єктів, вартості захисту ІР, організації процесу захисту, але не розглядають вплив різних типів атак на ймовірність реалізації загроз на окремих рівнях моделі OSI.

Метою статі є оцінювання імовірності реалізації загроз шляхом розроблення моделі порушення захищеності інформаційних ресурсів КС на різних рівнях взаємодії відкритих систем.

Виклад основного матеріалу дослідження. Під вразливістю розуміємо властивості КС (архітектурний, програмний, організаційний або інший недолік), які можуть бути використані для здійснення доступу до інформаційних ресурсів системи, що робить можливим виникнення загрози вторгнення. Водночас, вразливість являє собою певну характеристику КС, а будь-яка вразливість КС несе в собі загрозу впливу на ресурси системи за допомогою атаки [3]. Класифікацію загроз безпеці ІР КС представлено на рис. 1.

Загрози безпеці інформаційним ресурсам																										
За ступенем наміру дії		За характером дії		За джерелом загрози		За впливом на властивості інформації			За технічною реалізацією			За способом дії на об'єкт			За розміром нанесеного збитку				За способом реалізації		За досягнутою метою		За кінцевим результатом		
навмисні	ненавмисні	активні	пасивні	внутрішні	зовнішні	конфіденційність	цілісність	доступність	сканування	відмова в обслуговуванні	вторгнення	безпосередні	на КС управління	опосередковані	загальні	локальні	часткові	імітаційні	вплив однієї загрози	вплив множини загроз	проміжні	кінцеві	віддалений контроль	блокування	захоплення

Рисунок 1 – Класифікація загроз безпеці ІР КС

Мета порушення захищеності КС може не збігатися з метою атаки, та може бути спрямована на отримання проміжного результату необхідного для подальшої реалізації загрози. У разі такої невідповідності порушення захищеності КС розглядається як етап підготовки до реалізації загрози. Результатом порушення захищеності є наслідки, які сприятимуть реалізації атаки [4].

Вказані загрози впливають на КС та її компоненти, які забезпечують передачу інформації у відповідності до функціональних особливостей кожного об’єкта системи. Загальна структура КС представлена на рис. 2.

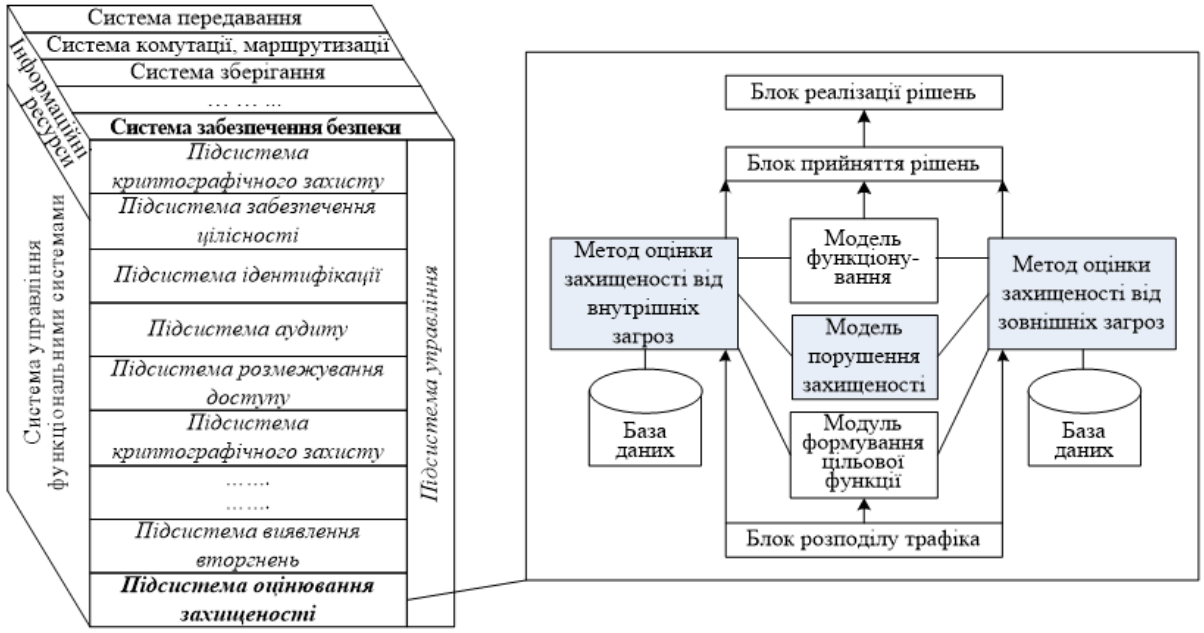

Рисунок 2 – Структура КС

З рис. 2 видно, що КС складається з множини взаємопов’язаних функціональних підсистем, серед яких є СЗБ. СЗБ містить такі підсистеми: управління, криптографічного захисту, забезпечення цілісності, ідентифікації, розмежування доступу, моніторингу, виявлення вторгнень, оцінювання захищеності, журналювання та аудиту, які і забезпечують підтримання належного рівня безпеки. Важливе місце в СЗБ займає підсистема оцінювання захищеності, яка функціонує в тісній взаємодії з іншими підсистемами, зокрема: підсистемою виявлення вторгнень, на основі якої здійснюється ідентифікація зовнішніх атак на КС або внутрішніх атак на ІР; підсистемою навчання, яка забезпечує наповнення бібліотек параметрами можливих атак, порушень, станів захищеності та функціонування системи; підсистеми прогнозування яка здатна прогнозувати порушення в КС або атак на ІР.

В цілому можливо відмітити, що для ефективного функціонування СЗБ, підсистема оцінювання захищеності повинна проводити власне оцінювання, виходячи із даних про реалізації основних типів атак, направлених на систему із зовні (зовнішні) або на елементи системи перебуваючи вже в середині системи (внутрішні) та з урахуванням множини стратегій порушення її захищеності.

Загрози реалізуються на всіх рівнях мережевої моделі OSI та можуть впливати ззовні на об`єкти КС (потік даних, мережевий вузол, кінцевий пристрій), а також із середини (трафік даних, програмно-апаратна частина КС).

Вторгнення реалізуються множиною способів (вплив загрози на один чи декілька об’єктів; множина загроз на один об’єкт чи декілька об’єктів). Вказані способи направлені на досягнення проміжної або кінцевої мети, внаслідок цього відбувається: відмова в обслуговуванні, віддалене контролювання, блокування або захоплення частини системи або КС в цілому [5].

Розглядаючи практичне здійснення порушень або атак на інформаційні, програмні та апаратні засоби КС, варто зазначити, що об’єктами атак є правила і технічні процедури, які здійснюють з’єднання і обмін даними в КС та відносяться до різних рівнів мережевої моделі OSI. Можуть бути наступні види впливу атак на різних рівнях мережевої моделі OSI [2]:

– прикладний рівень – відмова в доступі до прикладних програм, отримання або зміна пріоритету обслуговування окремих видів трафіку, відмова в обслуговуванні, відмова у сервісі, порушення з'єднання мережі;

– транспортний рівень – порушення доставки великих пакетів даних, побудова фальшивих пакетів, переповнення буферу, порушення в обслуговуванні шляхом частої відправки запитів, надсилання великої кількості пакетів запитів;

– мережевий рівень – порушення доставки повідомлень, порушення маршрутизації, відмова в обслуговуванні певного класу трафіку, надсилання неправдивих повідомлень, атака ICMP-запитами, підроблення адрес;

– канальний рівень – порушення синхронізації, відмова в доступі, відмова в сервісі, підміна MAC-адреси, самостійна розсилка даних;

– фізичний рівень – відмова в сервісі, розрив зв'язку, додавання шуму, відмова у перетворенні сигналів, перехоплення та прослуховування.

Атаки, які застосовуються для проведення вторгнень в КС можливо поділити на 5 категорій. Кожна з категорій містить множину типів атак, які використовуються для досягнення мети вторгнення. В свою чергу кожен тип атаки несе загрозу КС на відповідних рівнях мережевої моделі OSI та виконує свою функцію, щодо здійснення деструктивного впливу на КС. До вказаних категорій атак відносять [12]:

– Side-channel атаки – атаки сторонніми каналами, що спрямовані на вразливості в практичній реалізації криптосистеми. На відміну від теоретичного криптоаналізу, атаки сторонніми каналами використовують інформацію про фізичні процеси в пристрої, які не розглядаються в теоретичному описі криптографічного алгоритму. До найбільш поширених Side-channel атак належать: probing attack, timing attack, fault–induction attack, power analysis attack, electromagnetic analysis attacks;

– DoS атаки – це мережеві атаки, спрямовані на виникнення ситуацій, коли у системі, що піддається вторгненню, відбувається відмова в обслуговуванні. Вказані атаки характеризуються генерацією великого обсягу трафіка, що призводить до перенавантаження та блокування сервера. До найбільш поширених DoS атак належать: back, land, neptune, pod, smurf, teardrop атаки;

– U2R атаки – пропонують отримання зареєстрованим користувачам привілей локального суперкористувача (мережевого адміністратора). До U2R атак належать наступні типи атак: buffer_overflow, loadmodule, perl, rootkit;

– R2L атаки, що характеризуються отриманням доступу незареєстрованого користувача до КС з боку віддаленої станції. Поділяють R2L атаки на: ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster;

– Probe-атаки – полягають в скануванні мережевих портів з метою отримання конфіденційної інформації. Probe-атаки поділяються на такі типи: ipsweep, nmap, portsweep, satan.

Вказані типи атак за своєю функцією можуть впливати на функціональні можливості елементів КС, зокрема: управління передачею даних, обмін пакетами, організацію з'єднань, міжмережевий обмін, енергетичні характеристики мережевих засобів, доступ до кодування, управління інформацією.

На підставі викладеного та враховуючи множину способів впливу на КС, сукупність елементів КС, в яких циркулюють ІР або які забезпечують функціонування системи необхідно змоделювати порушення захищеності КС.

Стрімкий розвиток інформаційних технологій обмежує можливість швидкої адаптації існуючих СЗБ до нових загроз та взаємодію елементів СЗБ з елементами інфраструктури КС, які значно розширюють варіанти впливу на КС та СЗБ [4], підкреслює актуальність моделювання порушення захищеності КС.

Показники реалізації порушення захищеності КС та здійснення вторгнень в КС залежать від кваліфікації того хто реалізує порушення; обладнання, яке застосовується для

реалізації, покладених задач; стратегії здійснення порушення. Зловмисник, до того ж, розраховує на вразливості об'єкту порушення та низький рівень забезпечення безпеки КС. Також він володіє множиною інструментів для реалізації порушень/атак, які в свою чергу впливатимуть на ймовірність успішного їх здійснення.

Припустимо, що КС складається з N елементів системи, на які може впливати зловмисник за допомогою множини типів порушень. Така множина типів порушень або атак направлена на використання вразливостей системи та може реалізовуватися на прикладному, транспортному, мережевому, канальному, фізичному рівнях. Порушення, що направлені на вразливості системи утворюють множину варіантів проведення порушень: $Z = z_1, z_2, ..., z_n$. Імовірність порушень в КС за час t залежить від частоти атак λ. Кожен з N елементів системи містить СЗБ навчену оцінювати порушення захищеності КС на основі виявлення атак, що являє собою множину варіантів виявлення атак $B = \{b_1, b_2, ..., b_n\}$.

Необхідно розробити модель порушення захищеності КС для оцінювання імовірності реалізації загроз безпеці IP на рівнях моделі OSI.

Так як КС працює на всіх рівнях моделі OSI, а атаки можуть бути рівнозначними для елементів КС, то доцільно провести визначення імовірностей реалізації порушень захищеності на різних рівнях моделі OSI [7]. Разом з цим, кожний рівень моделі OSI матиме власне значення коефіцієнту захищеності від атак, виходячи із кількості типів атак, які впливають на окремий рівень моделі OSI; статистичних даних щодо впливу на кожен окремий рівень; можливостей СЗБ щодо оцінки захищеності та виявлення атак.

Виходячи із вказаного, значення імовірності порушення на окремому рівні моделі OSI матиме вигляд:

$$R = P_z \cdot P_v \cdot \varpi, \tag{1}$$

де P_z – імовірність реалізації типу порушення на окремому рівні моделі OSI;

P_v – імовірність використання вразливостей на окремому рівні моделі OSI;

ϖ – коефіцієнт здійснення атаки на окремому рівні моделі OSI.

Як наслідок, імовірність того, що КС на окремому рівні моделі OSI при використанні СЗБ може застосовуватися до виявлення j_z типів атак, у разі реалізації варіантів проведення атак Z, де $Z = 1, ..., Z$, визначатиметься:

$$P_a = 1 - \prod_{z=1}^{Z} \left(1 - P_{j_z}\right). \tag{2}$$

Так як варіанти проведення порушень Z можуть реалізовуватись j_z типами атак, то існування джерела проведення порушення Z визначається апріорною імовірністю $P(z)$. Водночас, реалізація варіантів проведення порушення Z типами атак j_z визначатиметься імовірністю $P(j_z / Z)$. Тоді імовірність реалізації варіантів проведення порушень на окремому рівні моделі OSI типами атак j_z від джерела атак матиме вигляд:

$$P_Z = P(z) P(j_z / z) \tag{3}$$

Імовірність порушення на окремому рівні моделі OSI за деякий час t, може здійснитися j_z типами атак з деякою частотою λ. З цього виходить, що час t доцільно розподілити на x рівних частин. Тоді імовірність того, що на відрізку часу відбудеться порушення визначатиметься:

$$P_t = \lambda t / x \tag{4}$$

В свою чергу на окремому рівні моделі OSI імовірність того, що серед x рівних частин часу відбудеться j_z типів порушень визначатиметься:

$$p_{j_z}(t) = \left(\frac{\lambda t}{x}\right)^{j_z} \left(1 - \frac{\lambda t}{x}\right)^{x - j_z} \tag{5}$$

Для отримання повної картини захищеності КС на окремому рівні моделі OSI необхідно врахувати об'єкти КС, які можуть бути атаковані. Тому реалізація варіантів проведення порушень Z на об'єкт КС l може описуватися законом розподілу імовірності. До об`єктів, на які може поширитись дана імовірність, можливо віднести:

$P(Z/l)$ – імовірність впливу варіанту проведення атаки Z на окремий обєкт КС l;

$P(Z/\sum l)$ – імовірність впливу варіанту проведення атаки Z на множину об'єктів КС l;

$P(\sum Z/l)$– імовірність впливу множини варіантів проведення атак Z на окремий об'єкт КС l;

$P(\sum Z/\sum l)$– імовірність впливу множини варіантів проведення атак Z на множину об`єктів КС l.

Тобто

$$P(z/l): z \to l; \tag{6}$$

$$P(z/\sum l): z \to \sum l; \tag{7}$$

$$P(\sum z/l): \sum z \to l; \tag{8}$$

$$P(\sum z/\sum l): \sum z \to \sum l. \tag{9}$$

Виходячи із вказаного ймовірність здійснення j_z типів атак на множину об'єктів КС l буде обчислюватись:

$$P(j_z, l) = \prod_{i=1}^{l} P_i^{j_z}. \tag{10}$$

Імовірність здійснення вдалого порушення на окремому рівні моделі OSI, визначатиметься імовірністю того, що порушення буде проведено на відрізку часу $1/t$. Відповідно до закону Пуассона отримаємо вираз:

$$P_k = 1 - e^{-\lambda/t}. \tag{11}$$

Враховуючи множину варіантів проведення атак в КС на окремому рівні мережевої моделі OSI, для представлення повної моделі порушення доцільно розглянути ймовірності здійснення порушення на L рівні моделі OSI та ймовірність атак у КС в цілому.

Розглядаючи ймовірність порушень у КС в цілому необхідно врахувати мінімальний час, протягом якого відбувається порушення на кожному рівні моделі OSI.

Імовірність здійснення вдалого порушення на N елемент системи шляхом застосування j_z типів атак матиме вигляд:

$$P_r = \max_j P_i^j,\ j = 1 \ldots j_z, \tag{12}$$

де P_i^j – імовірність здійснення j_z типів атак на i елемент.

Якщо $k(t)$ – частина вдало атакованих N елементів j_z типами атак, то кожен такий елемент має імовірність реалізації $j_z(1 - j_z(t))$ нових вдалих порушень інших елементів. Таким чином, кількість атакованих елементів за відрізок часу становитиме:

$$n = j_z N \cdot K(1 - j_z)dt. \tag{13}$$

У разі, якщо кількість елементів N в системі буде постійною, то отримаємо:

$$n = d(j_z N) = N dj_z. \tag{14}$$

Імовірність здійснення k порушень за час t розподіляється за законом Пуассона, а середнє значення порушень визначатиметься:

$$Y = \frac{1}{x}\sum_{i=1}^{x} y_i \tag{15}$$

де y_i – значення випадкової величини на i-ому відрізку часу при x – кількості інтервалів часу з можливим відхиленням:

$$\sigma \approx \frac{S_y}{\sqrt{x}} = \sqrt{\frac{1}{(x-1)}\sum_{i=1}^{x}(y_i - Y)^2} = S_y \quad (16)$$

де S_y –середнє значення помилки.

Перевірка гіпотези про розподіл кількості атак на відрізку часу за законом Пуассона здійснюється за допомогою критерію узгодженості Пірсона за виразом:

$$F = \sum_{i=1}^{k} \frac{(m_i - x\lambda_i)^2}{x\lambda_i} \quad (17)$$

де $\lambda_i = \frac{m_i}{x}$ – частота порушень з i -тою кількістю атак;

m_i – кількість випадків з i -тою кількістю атак на відрізку часу.

Розглянуті вирази (1) - (17), свідчать про те, що виявлення атак в КС залежить від швидкості адаптації існуючих СЗБ до нових загроз. А рівень безпеки ІР залежить від вибору стратегії порушення захищеності КС.

Висновки. Описано основні функції, що покладено на СЗБ, як одного з елементів КС управління та обробки ІР. Вразливості, що наявні в КС викликають порушення захищеності КС та становлять загрозу ІР. Множина загроз реалізується атаками, які можливо представити 5 категоріями. Множина атак, а також вторгнень в КС, спрямовані на засоби, що працюють на всіх рівнях мережевої моделі OSI та становлять функціональні елементи КС. Тому підсистема оцінювання захищеності КС враховуватиме множину всіх можливих загроз та множину всіх елементів КС.

На основі проведеного аналізу загроз ІР та структурних складових КС розроблено модель порушення захищеності ІР КС на різних рівнях моделі OSI та, як наслідок, отримано аналітичні вирази для оцінювання імовірності реалізації певних порушень безпеки ІР на всіх рівнях мережевої моделі OSI.

У перспективах подальших досліджень є розроблення методів оцінювання рівня захищеності КС від внутрішніх та зовнішніх джерел загроз для визначення ефективності функціонування СЗБ в режимі реального часу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Ю. Васильєв, “Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури”, *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, № 1 (29), с. 51-61, 2015.

[2] Я. В. Корпань, “Класифікація загроз інформаційній безпеці в комп’ютерних системах при віддаленій обробці даних”, *Реєстрація, зберігання і обробка даних*, т. 17 № 2, с. 39-46, 2015.

[3] Д. Б. Мехед, Ю. М. Ткач, В. М. Базилевич, В. І. Гур’єв, та Я. Ю. Усов, “Аналіз вразливостей корпоративних інформаційних систем”, *Захист інформації*, т. 20, № 1, с. 61-66, 2018.
doi: 10.18372/2410-7840.20.12453.

[4] Р. Грищук, В. Охрімчук, та В. Ахтирцева, “Джерела первинних даних для розроблення шаблонів потенційно небезпечних кібератак”, *Захист інформації*, №18 (1), с. 21-29, 2016.
doi: 10.18372/2410-7840.18.10109.

[5] І. Яковів, “Інформаційно-телекомунікаційна система, концептуальна модель кіберпростору і кібербезпека”, *Information Technology and Security*, № 5 (9), с. 134-144, 2017.

[6] С. В. Сальник, О. Я. Сова, та Д. А. Міночкін, “Аналіз методів виявлення вторгнень у мобільні радіомережі класу MANET”, *Сучасні інформаційні технології у сфері безпеки та оборони*, № 1 (22), с. 103-112, 2015.

[7] В. Л. Бурячок, "Сучасні системи виявлення атак в інформаційно-телекомунікаційних системах і мережах. Модель вибору раціонального варіанта реагування на прояви стороннього кібернетичного впливу", *Інформаційна безпека*, № 1, с. 33-40, 2013.
[8] А. О. Антонюк, *Моделювання систем захисту інформації*. Ірпінь, Україна: Національний університет ДПС України, 2015.
[9] Y. Alshboul, and K. Streff, "Analyzing Information Security Model for Small-Medium Sized Businesses", in *Proc. 21st Americas Conference on Information Systems*, Puerto Rico, 2015.
[10] N. S. Safa, R. V. Solms, and S. Furnell, "Information security policy compliance model in organizations", *Computers & Security*, vol. 56, pp. 70-82, 2016. doi:10.1016/j.cose.2015.10.006.
[11] D. L. Nazareth, and J. Choi, "A system dynamics model for information security management", *Information & Management*, vol. 52, iss. 1, pp. 123-134, 2015. doi:10.1016/j.im.2014.10.009.
[12] P. Aggarwal, and S. K. Sharma "Analysis of KDD dataset attributes-class wise for intrusion detection", *Procedia Computer Science.* vol. 57, pp. 842–851, 2015 doi: 10.1016/ j.procs.2015.07.490.

Стаття надійшла до редакції 12.02.2019.

REFERENCE

[1] Y. Vasiliev, "Classification and analysis of threats to information security in key information infrastructure systems", Legal, normative and metrological provision of the information security system in Ukraine, № 1 (29), pp. 56-61, 2015.
[2] Y.A. Korpan, "Classification of information security threats to computer systems for remote data processing", *Data Recording, Storage & Processing* ,vol. 17, no. 2, pp.39-46, 2015.
[3] D. Mehed, Y. Tkach, V. Bazilevich, V. Guriev, and Y. Usov, "Analysis of corporate information systems vulnerability", *Ukrainian Information Security Research Journal*, vol 20, no. 1, pp. 61-66, 2018. doi: 10.18372/2410-7840.20.12453
[4] R. Grishchuk, V. Okhrimchuk, and V. Akhtyrtseva, "Sources of primary data for developing templates for potentially dangerous cyber attacks", *Ukrainian Information Security Research Journal*, vol. 18, no. 1, pp. 21-29, 2016. doi: 10.18372/2410-7840.18.10109.
[5] I. Yakoviv, "Information-telecommunication system, conceptual model of cyberspace and cybersecurity", *Information Technology and Security*, vol 5, iss. 2, pp. 134-144, 2017.
[6] S. V. Salnyk, O.Y. Sova, D.A. Minochkin, "Methods analysis of intrusion detection in manet class mobile radio networks", *Modern Information Technologies in the Sphere of Security and Defence*, no. 1 (22) , pp. 103-112, 2015.
[7] V. L. Buryachok, "Modern systems of intrusion detection in information and telecommunication systems and networks. The selection model of rational variant of responding to the occurrence of extraneous influence cybernetic", *Informational security*, no.1, pp.33-40, 2013.
[8] A. O. Antoniuk, Modeling of information security systems, Irpin, Ukraine: National University of State Tax Service of Ukraine, 2015.
[9] Y. Alshboul, K. Streffб "Analyzing Information Security Model for Small-Medium Sized Businesses", in *Proc. 21st Americas Conference on Information Systems*, Puerto Rico, 2015
[10] N. S. Safa, R. V. Solms, S. Furnell, "Information security policy compliance model in organizations", *Computers & Security*, vol. 56, pp. 70-82, 2016. doi:10.1016/j.cose.2015.10.006
[11] D. L. Nazareth, J. Choi, "A system dynamics model for information security management", *Information & Management*, vol. 52, issue 1, pp. 123-134, 2015. doi:10.1016/j.im.2014.10.009.

[12] P. Aggarwal, and S.K. Sharma “Analysis of KDD dataset attributes-class wise for intrusion detection”, Procedia Computer Science. vol. 57, pp. 842–851, 2015. doi: 10.1016/ j.procs.2015.07.490.

SERHII SALNYK,
ANTON STORCHAK,
ARTEM MYKYTIUK

COMMUNICATION SYSTEM INFORMATION RESOURCE SECURITY BREACH MODEL

The article presents a model of information resources security breach processed in communication systems. The basic functions of the security system as one of the elements of the communication system are described. It is shown that the vulnerabilities of its components lead to a violation of the security of information resources and contribute to the realization of threats to their security. The information resources security breach model is developed based on multiple vulnerabilities of communication systems. The list of security threats to information resources, attacks types at all levels of the basic reference model of open systems interaction, examples of attacks implementation and strategy of carrying out attacks by an attacker are considered: the impact of an attack option on a single object or multiple objects of the communication system, the impact of multiple attack options on a separate object or set of objects of a communication system. This allowed establishing the capabilities of the attacker when carrying out attacks on information resources of communication systems. The developed model is proposed to be used as a basis for building a subsystem of assessment of the security of information resources of the communication system. Also, methods of assessing the security of information resources against internal and external threats have been used. The security assessment subsystem of communication systems takes into account many possible threats and elements of communication systems. Based on the analysis of security threats to information resources and structural components of communication systems, analytical equations were obtained to assess the probability of realization of violations of the information resources security of communication systems at all levels of the basic reference model of open systems interaction. It has been found that the detection of attacks in communication systems depends on the speed at which the security system adapts to new threats. Using the obtained model of security breach will allow developing methods for assessing the level of protection against internal and external threats to determine the effectiveness of the information security system in real-time functioning. This will increase the overall security of the communication systems and information resources that they process.

Keywords: communication systems; information resources; security breach; security evaluation system; security breach model.

Сальник Сергій Васильович, кандидат технічних наук, заступник завідувача кафедри безпеки державних інформаційних ресурсів, Інститут спеціального зв’язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна.

ORCID: 0000-0003-4463-5705.

E-mail: s.sergey@i.ua.

Сторчак Антон Сергійович, старший викладач кафедри безпеки державних інформаційних ресурсів, Інститут спеціального зв’язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, Україна.

ORCID: 0000-0002-5267-3122.

E-mail: storchakanton@gmail.com.

Микитюк Артем В'ячеславович, заступник завідувача кафедри кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0002-8307-9978.

E-mail: mukuta8888@gmail.com.

Salnyk Serhii, candidate of technical sciences, deputy head at the security of state information resources academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Storchak Anton, senior instructor at the security of state information resources academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Mykytiuk Artem, deputy head at the cybersecurity and application of information systems and technology academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.