УДК 621.391 DOI: 10.30748/zhups.2021.70.11

В.В. Сальник[1], О.А. Гуж[1], В.С. Закусіло[1], С.В. Сальник[1], П.В. Бєляєв[2]

[1]*Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут ім. І. Сікорського", Київ*
[2] *Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків*

МЕТОДИКА ОЦІНКИ ПОРУШЕНЬ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

В роботі запропоновано методика оцінки порушень захищеності інформаційних ресурсів, що обробляються в інформаційно-телекомунікаційних системах (ІТС). Описано функції, які покладено на систему забезпечення безпеки в ІТС, як одного з елементів обробки інформаційних ресурсів. Вразливості складових частин ІТС призводять до порушення захищеності інформаційних ресурсів, що оброблюються в них, та відповідно сприяють реалізації множині загроз інформаційним ресурсам. Методика оцінки порушень захищеності інформаційних ресурсів розроблено на основі врахування множини вразливостей ІТС. Розглянуто множину загроз безпеці інформаційним ресурсам, типи атак які застосовуються на рівнях базової еталонної моделі взаємодії відкритих систем, також приклади проведення атак та варіанти впливу на ІТС, що надало представлення про можливості порушень при реалізації атак на інформаційні ресурси ІТС. До складу системи обробки інформаційних ресурсів зазвичай входить підсистема оцінки порушень захищеності. В основі побудови зазначеної підсистеми запропоновано взяти способи порушення стану захищеності інформаційних ресурсів, оцінки порушень захищеності інформаційних ресурсів від внутрішніх загроз та оцінки захищеності інформаційних ресурсів від зовнішніх загроз. Підсистема оцінки порушень захищеності інформаційних ресурсів враховує множину загроз та елементи ІТС. На основі проведеного аналізу множини загроз направлених на порушення рівня безпеки інформаційним ресурсам та елементам ІТС обробки інформаційних ресурсів було отримано аналітичні вирази для оцінки ймовірності реалізації порушень стану захищеності інформаційних ресурсів ІТС на рівнях базової еталонної моделі взаємодії відкритих систем. Застосування отриманої методики оцінки порушень захищеності дозволить розробити методи оцінки рівня порушень стану захищеності від загроз для встановлення ефективності функціонування підсистеми оцінки порушень захищеності в режимі реального часу, що підвищить загальний рівень інформаційної безпеки ІТС та інформаційних ресурсів, що в них оброблюються.

Ключові слова: *інформаційно-телекомунікаційна система, інформаційні ресурси, порушення захищеності, підсистема оцінки порушень захищеності, методика оцінки порушень захищеності.*

Вступ

Постановка проблеми. У зв'язку з тим, що система забезпечення безпеки (СЗБ) ІТС обробки інформаційних ресурсів має забезпечувати належний рівень інформаційної безпеки, керувати розмежуванням доступом, контролювати небезпечні подій, виявляти атаки на інформаційні ресурси (ІР), проводити оцінку порушення захищеності системи та вживати заходи щодо підтримання належного рівня інформаційної безпеки систем в ІТС, то СЗБ необхідно відслідковувати весь трафік, що циркулює в ІТС. Для цього СЗБ забезпечує своє функціонування на всіх рівнях еталонної моделі взаємодії відкритих систем (моделі OSI), здійснюючи при цьому: аналіз структури та вмісту інформаційних пакетів, контроль трафіку, оцінку станів функціонування елементів системи, тощо.

При використанні ІТС для управління інформаційними ресурсами, метою процесу порушення захищеності ІТС може бути приховане управління кінцевими та мережевими ресурсами або деструктивний вплив на інформаційні, програмні та апаратні засоби ІСТ. Реалізація цієї мети може досягатися за допомогою способів та методів направлених на вразливості ІТС. В свою чергу процес оцінки порушень захищеності інформаційних ресурсів потребує розробки та дослідження нових підходів направлених на підтримання належного рівня безпеки [1–2].

Аналіз останніх досліджень і публікацій. Питання реалізації загроз, класифікації вразливостей і загроз безпеці ІТС розглядалися в роботах [8–10].

До основних вимог, що висуваються при оцінці порушень захищеності належать: можливість розрахувати вірогідність реалізації загроз; можливість розрахувати час виявлення загроз та реалізації атаки; простота визначення вхідних параметрів даних,

тощо. В [7] представлено способи та методи захисту ІТС та процесу оцінки порушення захищеності ІТС. Однак ці підходи використовують різний математичний апарат, не враховують питання доступу суб'єктів до об'єктів, організації процесу захисту, не розглядають можливість реалізації різних типів атак на ІТС.

Метою статі є розробка методика оцінки порушень захищеності інформаційних ресурсів, що обробляються в інформаційно-телекомунікаційних системах для оцінювання імовірності реалізації певних порушень безпеки ІТС.

Об'єктом розгляду статті є процес забезпечення безпеки інформаційних ресурсів, що обробляються в ІТС.

Предметом дослідження є методика оцінки порушень захищеності інформаційних ресурсів в ІТС.

Виклад основного матеріалу

Під вразливістю будемо розуміти властивості ІТС, які можуть бути використані для реалізації доступу до ресурсів системи, що робить можливим виникнення порушень інформаційної безпеки. В свою чергу вразливість являє собою характеристику захищеності ІТС, а будь-яка вразливість ІТС несе в собі загрозу впливу на інформаційні ресурси за допомогою атаки [3]. До загроз безпеці ІТС поділяються на такі загрози, як: за ступенем наміру, за технічною реалізацією, за способом дії, за способом реалізації, за досягнутою метою, тощо.

Мета порушень захищеності інформаційних ресурсів може не збігатися з метою загрози, та може бути спрямована на отримання проміжного результату необхідного для подальшої реалізації загрози. У разі такої невідповідності порушення або атака розглядається, як етап підготовки до вчинення дій, спрямованих на реалізацію загрози. Результатом порушення захищеності або атаки є наслідки, які реалізуються за допомогою загрози або сприяли такій реалізації [4].

Вказані загрози впливають на безпеку ІТС та її компоненти, які забезпечують передачу інформації у відповідності з функціональними особливостями кожного об`єкта системи. В цілому підсистема забезпечення безпеки ІТС складається з множини елементів, таких як: управління, забезпечення цілісності, ідентифікації, розмежування доступі, виявлення вторгнень, оцінки захищеності, аудиту, які в свою чергу забезпечують підтримання належного рівня безпеки, як в окремих елементах ІТС так і в цілому. Важливе місце в ІТС займає оцінки порушень захищеності, яка функціонує в тісній взаємодії з іншими підсистемами. В цілому можливо відмітити, що для ефективного функціонування СЗБ в ІТС, підсистема оцінки порушень захищеності повинна проводити оцінку виходячи із даних про реалізації загроз, вразливостей та атак, направлених на ІТС або на її елементи системи. Загрози реалізуються на всіх рівнях мережевої моделі OSI та можуть впливати ІТС. В свою чергу вторгнення на ІТС реалізовується множиною способів, які направлені на досягнення проміжної або кінцевої мети, в наслідок чого відбувається: віддалене контролювання, блокування або захоплення елементів ІТС, тощо [5].

Розглядаючи практичну реалізацію порушень або проведення атак на інформаційні, програмні та апаратні засоби ІТС, варто зазначити, що об'єктами атак є правила і технічні процедури, які забезпечують з'єднання і обмін даними в ІТС, та відносяться до різних рівнів мережевої моделі OSI. Існують наступні типи атак, що застосовані на різних рівнях мережевої моделі OSI:

– 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.

Атаки, які реалізуються для проведення вторгнень в ІТС можливо поділити на 5 категорій. Кожна з яких містить множину типів атак, які використовуються для реалізації мети вторгнення. Кожен тип атаки несе загрозу ІТС на відповідних рівнях мережевої моделі OSI а також та виконує свою функцію, щодо здійснення деструктивного впливу на ІТС. До вказаних типів атак відносять:

– Side-channel атаки – атаки сторонніми каналами, що направлені на вразливості в практичній реалізації криптосистеми. Ці атаки використовують інформацію про фізичні процеси в пристрої, які не розглядаються в описі криптографічного алгоритму. До найбільш застосованих Side-channel атак належать: timing attack, fault–induction attack, probing attack electromagnetic analysis attacks, power analysis attack, та інші атаки.

– DoS атаки – це атаки, спрямовані на виникнення ситуацій, коли у ІТС, що піддається вторгненню, відбувається відмова в обслуговуванні. Ці атаки характеризуються генерацією великого об`єму трафіка, що призводить до перенавантаження та

блокування сервера. До найбільш застосованих DoS атак належать: pod, back, neptune, smurf, land, teardrop атаки;

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

– R2L атаки характеризуються отриманням доступу незареєстрованого користувача до ІТС з боку віддаленої станції. До R2L атак належать: ftp_write, imap, guess_passwd, phf, spy, multihop, warezclient та інші атаки;

– Probe-атаки – полягають в скануванні мережевих портів за для отримання конфіденційної інформації. До Probe-атак відносяться на наступні типи: satan, ipsweep, nmap, portsweep, та інші.

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

На підставі зазначеного та враховуючі множину способів впливу на ІТС виникає питання розробки способів та методів оцінки порушень захищеності інформаційних ресурсів, що обробляються в інформаційно-телекомунікаційних системах для оцінювання імовірності реалізації певних порушень безпеки ІТС.

Показники реалізації порушення захищеності ІТС та здійснення впливу на ІР залежать від: кваліфікації того хто проводить деструктивні дії, наявності обладнання яке застосовується для впливу, покладених задач, стратегії та мети здійснення порушення, тощо. Реалізація впливу направлена на вразливості об'єкту порушення та низький рівень забезпечення безпеки ІТС. Також порушник має множину інструментів для реалізації порушень, які в свою чергу впливатимуть на ймовірність його реалізації.

Постановка задачі. 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 вразливості системи та може бути реалізована на прикладному, транспортному, мережевому, канальному рівнях. В свою чергу множина типів порушень направлена на вразливості системи складає множину варіантів проведення порушень: $Z = z_1, z_2, ..., z_n$, множина потоків даних – $V = v_{BA}(t) \cup v_A(t)$; кількість повідомлень з атаками – v_A; кількість повідомлень без атак v_{BA}; достовірність оцінки стану захищеності типу $D1$ та $D2$; інтервал часу проведення оцінювання стану захищеності T_1 та T_2, множина параметрів трафіку $X(t)$; множина параметрів індикаторів $S(t)$; множина ідентифікованих станів вхідних даних методу при впливі зовнішніх атак $XMi(t) = \{x'(t)\}$; множина ідентифікованих станів вхідних даних методу при впливі внутрішніх атак $XVi(t) = \{x'(t)\} \cup \{s'(t)\}$; множина можливих порушень безпеки $\Lambda(t)$; множина засобів протидії порушенням захищеності $U(t)$; місткість бази знань – $Z_I(X(t), S(t), X_{i1}(t), \Lambda_i, U_i)$; ризик виникнення порушень $R(t)$ у момент *t*; множина оптимальних значень засобів протидії порушенням $\overline{U}$. 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 методику оцінки порушень захищеності інформаційних ресурсів для оцінки імовірності реалізації певних порушень безпеки ІР на рівнях моделі OSI.

Допущення: під час отримання інформації, зміни в топології мережі не відбуваються, службові повідомлення передаються без помилок, база знань навчена параметрам атак з баз NSL-KDD та KYOTO, розміри інформаційних та службових повідомлень не змінюються.

Показники ефективності управління станом захищеності ІТС:

$D1 = f\left(X(t), \Lambda_i, U_i, R(t)\right)$ – достовірність прийняття управлінського рішення щодо оцінки порушення стану захищеності при впливі зовнішніх атак;

$D2 = f\left(X(t), S(t), \Lambda_i, U_i, \overline{U}\right)$ – достовірність прийняття управлінського рішення щодо оцінки порушення стану захищеності при впливі внутрішніх атак;

T – інтервал часу прийняття управлінського рішення щодо оцінки порушення стану захищеності.

Обмеження на процес оцінки порушення стану захищеності:

$\Omega = \{D > D_{isn}, T \le T_{isn}\}$, де D_{isn} – достовірність прийняття управлінського рішення щодо оцінки порушення стану захищеності існуючими методами;

t_{isn} – час прийняття управлінського рішення щодо оцінки порушення стану захищеності.

Методика оцінки порушення стану захищеності ІР в ІТС включає наступні етапи:

– аналіз умов функціонування ІР в ІТС та визначення вхідних даних;

– отримання вхідних даних: параметри трафіку $X(t)$; індикатори кіберзагроз $S(t)$;

– розподіл вхідних даних параметрів трафіку

$X_k(t) = \{X_H(t)\} \cup \{X_M(t)\}$;

– ідентифікація (DoS, U2R, R2L, Probe, Side) типів атак;

– визначення показників ефективності оцінювання порушення стану захищеності.

Сутність методики полягає у відтворенні процесу управління ІР з урахуванням впливу атак на ІТС. Метою розробки є експериментальне дослідження способів та методів управління станом захищеності иа порушень захищеності ІР в ІТС та вибір їх оптимальних параметрів, з точки зору прийнятих критеріїв ефективності. При цьому до методики пред'являються наступні вимоги: відображати умови функціонування ІТС та процес управління ІР в ІТС; забезпечувати можливість порівняльної оцінки ефективності способів та методів оцінки порушення станом захищеності ІР в ІТС; гарантувати точність та достовірність результатів розробки. Так як ІТС працює на всіх рівнях моделі OSI, а атаки можуть бути рівнозначними для всіх рівнів OSI та елементів ІТС, то доцільно провести визначення імовірностей порушень, як для їх типових значень на рівнях моделі OSI. 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 та інше [6]. Виходячи із вказаного, значення імовірності порушення на окремому рівні моделі OSI в загальному вигляді матиме вигляд:

$$R = P_z \cdot P_v \cdot \varpi, \qquad (1)$$

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 ІТС на окремому рівні моделі OSI при використанні СЗБ може бути застосована до виявлення j_z типів атак, у разі реалізації варіантів проведення атак Z, де $Z = 1,...,Z$, буде визначатися:

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

Так як варіанти проведення порушень Z можуть бути реалізовано j_z типами атак, то існування джерела проведення порушення Z визначається апріорною імовірністю $\pi(z)$.

Імовірність реалізації варіантів проведення порушень на окремому рівні моделі OSI типами атак j_z від джерела атак матиме вигляд:

$$P_Z = \pi(z) P(j_z / z). \qquad (3)$$

Імовірність порушення на окремому рівні моделі OSI за деякий час t, може здійснитися j_z типами атак з деякою частотою λ.

Імовірність того, що на відрізку часу відбудеться порушення визначатиметься:

$$P_t = \lambda t / x. \qquad (4)$$

Імовірність того, що серед x рівних частин часу відбудеться j_z типів порушень буде визначатися:

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

Для отримання оцінки порушень стану захищеності ІТС на окремому рівні моделі OSI необхідно врахувати об`єкти ІР, які можуть бути атаковані. Виходячи із вказаного імовірність здійснення j_z типів атак на множину об'єктів КС l буде обчислюватись:

$$P(j_z, l) = \prod_{i=1}^{l} P_i^{j_z}. \qquad (6)$$

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

Загальна оцінка мінімального часу, протягом якого відбувається порушення на рівні моделі OSI визначатиметься:

$$P(\min_t \sum_{j \in R(i)} \zeta_j \langle t) = 1 - \int_{\substack{x_i \ldots x_N \\ \sum_{j \in R(i)} x_j \geq t_i \forall_i}} \ldots \int \prod_j f_j(x_j) \cdot dx_1 \cdot \ldots \cdot dx_N. \qquad (7)$$

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

$$P_r = \max_j P_i^j, \; j = 1 \ldots j_z, \qquad (8)$$

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

Імовірність здійснення k порушень за час t буде розподілена за законом Пуассона. Отже, в якості гіпотези закону розподілу атак, приймемо закон розподілу Пуассона, а середнє значення порушень визначатиметься:

$$Y = \frac{1}{x} \sum_{i=1}^{x} y_i, \qquad (9)$$

де y_i – значення випадкової величини на i-ому відрізку часу при x – кількості інтервалів часу.

– Враховуючі те, що кожен елемент системи містить СЗБ навчену оцінювати захищеність ІТС на основі виявлених порушень стану захищеності, то імовірність порушення буде визначатися:

$$P_B = \min P_i^b, b_b = 1...b_n . \quad (10)$$

Розглянуті вирази, свідчать про те, що оцінка стану порушення в ІТС залежить від швидкості адаптації існуючих СЗБ до нових загроз. А рівень безпеки ІР буде залежить від вибору стратегії порушення захищеності ІТС.

Висновки

Описано основні функції, що покладено на СЗБ, як один з елементів ІТС управління та обробки ІР. Вразливості, що наявні в ІТС викликають порушення захищеності ІТС та становлять загрозу ІР. Представлена множина загроз реалізується атаками, які можливо представити 5 категоріями. Множина атак на ІТС спрямовані на засоби, що працюють на всіх рівнях мережевої моделі OSI та становлять функціональні елементи ІТС. Тому підсистема оцінки порушень захищеності ІТС має враховувати множину всіх можливих загроз та множину всіх елементів ІТС. На основі проведеного аналізу загроз ІР та структурних складових ІТС розроблено модель оцінки порушення захищеності КС на різних рівнях моделі OSI та отримано аналітичні вирази для оцінювання імовірності реалізації певних порушень безпеки ІР на всіх рівнях мережевої моделі OSI.

Дана розробка дозволить побудувати відповідні методи оцінки порушення захищеності ІР В ІТС для визначення ефективності функціонування СЗБ в режимі реального часу.

Список літератури

1. Васильєв Ю. Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2015. № 1(29). С. 112-119.
2. Корпань Я.В. Класифікація загроз інформаційній безпеці в комп'ютерних системах при віддаленій обробці даних. *Реєстрація, зберігання і обробка даних*. 2015. № 17(2). С. 39-46.
3. Мехед Д. Б., Ткач Ю. М., Базилевич В. М., Гур'єв В. І., Усов Я. Ю. Аналіз вразливостей корпоративних інформаційних систем. *Захист інформації*. 2018. № 20(1). С. 61-66.
4. Грищук Р., Охрімчук В., Ахтирцева В. Джерела первинних даних для розроблення шаблонів потенційно небезпечних кібератак. *Захист інформації*. 2016. № 18(1). С. 21-29.
5. Яковів І. Інформаційно-телекомунікаційна система, концептуальна модель кіберпростору і кібербезпека. *Information Technology and Security*. 2017. № 5(9). С. 134-144.
6. Бурячок В. Л. Сучасні системи виявлення атак в інформаційно-телекомунікаційних системах і мережах. *Інформаційна безпека*. 2013. № 1. С. 33-40.
7. Антонюк А. О., Моделювання систем захисту інформації. Ірпінь : НУ ДПС України. 2015. 123 с.
8. Alshboul Y., Streff K. Analyzing Information Security Model for Small-Medium Sized Businesses. *Twenty-first Americas Conference on Information Systems*. Puerto Rico, 2015. 231 p.
9. Safa N. S., Solms R.V., Furnell S. Information security policy compliance model in organizations. *Computers & Security*. 2016. Vol. 56. P. 70-82.
10. Nazareth D. L., Choi J. A system dynamics model for information security management. *Information & Management*. 2015. Vol. 52. P. 123-134.

Надійшла до редколегії 06.09.2021
Схвалена до друку 16.11.2021

Відомості про авторів:

Сальник Володимир Васильович
начальник сектору
Інституту спеціального зв'язку та захисту інформації
Національного технічного університету України
"Київського політехнічного інституту ім. І. Сікорського",
Київ, Україна
https://orcid.org/0000-0003-0534-3822

Гуж Олександра Андріївна
курсант
інституту спеціального зв'язку та захисту інформації
Національного технічного університету України
"Київського політехнічного інституту ім. І. Сікорського",
Київ, Україна
https://orcid.org/0000-0002-9122-846X

Закусіло Вікторія Олегівна
курсант
інституту спеціального зв'язку та захисту інформації
Національного технічного університету України
"Київського політехнічного інституту ім. І. Сікорського",
Київ, Україна
https://orcid.org/0000-0002-3301-3372

Information about the authors:

Volodymyr Salnyk
Head of Sectort
Institute of Special Communication and Information
Protection of National Technical University
of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute",
Kyiv, Ukraine
https://orcid.org/0000-0003-0534-3822

Oleksandra Guzh
Cadet
Institute of Special Communication and Information
Protection of National Technical University
of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute",
Kyiv, Ukraine
https://orcid.org/0000-0002-9122-846X

Viktoria Zakusilo
Cadet
Institute of Special Communication and Information
Protection of National Technical University
of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute",
Kyiv, Ukraine
https://orcid.org/0000-0002-3301-3372

Сальник Сергій Васильович
кандидат технічних наук
провідний науковий співробітник
інституту спеціального зв'язку та захисту
інформації Національного технічного
університету України
"Київського політехнічного інституту ім. І. Сікорського",
Київ, Україна
https://orcid.org/0000-0003-4463-5705

Бєляєв Павло Васильович
молодший науковий співробітник
Харківського національного університету
Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0003-0650-6232

Sergey Salnyk
PhD in Engineering
Leading Researcher
Institute of Special Communication and Information
Protection of National Technical University
of Ukraine "Igor Sikorsky
Kyiv Polytechnic Institute",
Kyiv, Ukraine
http://orcid.org/0000-0003-4463-5705

Pavlo Bieliaiev
Junior Researcher
of Ivan Kozhedub Kharkiv
National Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0003-0650-6232

МЕТОДИКА ОЦЕНКИ НАРУШЕНИЙ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

В.В. Сальник, А.А. Гуж, В.О. Закусило, С.В. Сальник, П.В. Беляев

В работе предложена методика оценки нарушений защищенности информационных ресурсов, обрабатываемых в информационно-телекоммуникационных системах (ИТС). Описаны функции, возложенные на систему обеспечения безопасности в ИТС, как один из элементов обработки информационных ресурсов. Рассмотрено множество угроз безопасности информационным ресурсам, типы атак применяемых на уровнях базовой эталонной модели взаимодействия открытых систем, а также примеры проведения атак и варианты воздействия на ИТС, что дало представление о возможности нарушений при реализации атак на информационные ресурсы ИТС. В состав системы обработки информационных ресурсов обычно входит подсистема оценки нарушений защищенности. В основе построения указанной подсистемы предложено взять способы нарушения защищенности информационных ресурсов, оценки нарушений защищенности информационных ресурсов от внутренних угроз и оценки защищенности информационных ресурсов от внешних угроз. Подсистема оценки нарушений защищенности информационных ресурсов учитывает множество угроз и элементов ИТС. На основе проведенного анализа множества угроз, направленных на нарушение уровня безопасности информационным ресурсам и элементам ИТС обработки информационных ресурсов, были получены аналитические выражения для оценки вероятности реализации нарушений состояния защищенности информационных ресурсов ИТС на уровнях базовой эталонной модели взаимодействия открытых систем. Применение полученной методики оценки нарушений защищенности позволит разработать методы оценки уровня нарушений состояния защищенности от угроз для установления эффективности функционирования подсистемы оценки нарушений защищенности в режиме реального времени, что повысит общий уровень информационной безопасности ИТС и обрабатываемых в них информационных ресурсов.

Ключевые слова: *информационно-телекоммуникационная система, информационные ресурсы, нарушения защищенности, подсистема оценки нарушений защищенности, методика оценки нарушений защищенности.*

METHODS OF ASSESSMENT OF INFRINGEMENTS OF INFORMATION RESOURCES IN INFORMATION AND TELECOMMUNICATION SYSTEMS

V. Salnyk, O. Guzh, V. Zakusilo, S. Salnyk, P. Bieliaiev

The method of estimation of infringements of protection of the information resources processed in information and telecommunication systems (ITS) is offered in work. Describes the functions assigned to the security management system in ITS, as one of the elements of information resource processing. Vulnerabilities in the components of ITS lead to violation of the security of information resources processed in them, and, accordingly, contribute to the realization of a set of threats to information resources. The methodology of estimation of infringements of protection of the information resources has been developed based on taking into account of sets of ITS vulnerabilities. The set of threats to the security of information resources is considered, the types of attacks used at the levels of the basic reference model of the interaction of open systems are considered in this work. As well as examples of attacks and options for influencing ITS, which gave an idea of the possibility of violations in the implementation of attacks on information resources of ITS. The information resources processing system usually includes security violation assessment subsystem. As a basis of formation of the specified subsystem it is offered to take ways of violation of the state of security of information resources, an estimation of violations of protection of information resources from internal threats and an estimation of protection of information resources from external threats. The subsystem for assessing violations of the security (security violation assessment subsystem) of information resources takes into account a set of threats and elements of ITS. The analysis of a set of threats aimed at violating the level of security of information resources and ITS elements of information resources processing was obtaining. Based on the analysis analytical expressions were obtained to assess the probability of violations of ITS information resources at the levels of the basic reference model of open systems interaction. The application of the obtained methodology of security violations assessing will allow to develop methods of an estimation of a level of violation of the state of security against threats to establish the effectiveness of security violation assessment subsystem functioning in real time, which will increase the overall level of ITS information security and information resources processed in them.

Keywords: *information and telecommunication system, information resources, security violation, security violation assessment subsystem, methodology of security violations assessing.*