Захист інформації та кібернетична безпека

УДК 004.056 DOI: 10.30748/soi.2019.158.12

А.С. Сторчак, С.В. Сальник

Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут ім. І. Сікорського", Київ

МЕТОД ОЦІНЮВАННЯ РІВНЯ ЗАХИЩЕНОСТІ МЕРЕЖЕВОЇ ЧАСТИНИ КОМУНІКАЦІЙНОЇ СИСТЕМИ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ ВІД КІБЕРЗАГРОЗ

У статті представлено удосконалений метод оцінки рівня захищеності мережевої частини комунікаційної системи спеціального призначення від кіберзагроз на основі алгоритму розподільчої ідентифікації та динамічного програмування. Однією зі складових систем забезпечення безпеки комунікаційних систем є підсистема оцінки рівня захищеності, яка призначена для визначення ефективності застосовуваних засобів захисту. Метою роботи є розробка методу оцінки захищеності інформації, яка обробляється в комунікаційній системі, на основі керованих багатокрокових процесів прийняття рішень, для підвищення ефективності управління захистом інформації, з огляду на характеристики процесу захисту. Визначено величину ризику на кожному етапі процесу захисту і визначено правило вибору засобів захисту, які мінімізують значення ризиків на всіх етапах. Процес оцінки захисту комунікаційних систем і процес застосування засобів захисту реалізуються за етапами. На кожному кроці отримано деяку сукупність даних про стан захищеності системи, яка залежить від реалізованих послуг безпеки, що характеризують систему забезпечення безпеки та впливають на вибір використовуваних захисних механізмів. Визначено вектори процесу оцінки захищеності і процесу реалізації засобів захисту, які забезпечують мінімізацію значення ризиків на всіх етапах функціонування системи захисту. Суть методу полягає у оцінюванні рівня захищеності комунікаційних систем з використанням розподільчої ідентифікації параметрів кібератак, проведенням вибору щодо застосування заходів із захисту системи при повному статистичному описі комунікаційної системи та врахуванням стратегій впливу на неї на основі динамічного програмування. Отримано рекурентні співвідношення та правило використання засобів захисту, які визначають порядок вибору оптимальних захисних заходів і є основою для знаходження оптимальних або близьких до них алгоритмів використання засобів захисту при апріорній невизначеності. Вони дозволяють визначити ступінь захищеності інформаційних систем на основі дослідження змін його характеристик.

Ключові слова: *кіберзагроза, системи спеціального призначення, захищеність, метод оцінювання, комунікаційна система.*

Вступ

Стрімкий розвиток та поширення систем електронних комунікацій або комунікаційних систем спеціального призначення (КС) обробки інформації вимагає забезпечення постійного контролю коректного їх використання та впливу кіберзагроз на стан та властивості системи (хостову або мережеву їх частину).

Основними особливостями побудови та застосування КС є: динамічна топологія; децентралізоване управління елементами та системами; спільний доступ вузлів до середовища передачі трафіку; масштабованість; необхідність збору значної кількості інформації про стан мережі на різних рівнях мережевої моделі OSI. Зазначені особливості КС обумовлюють множину вразливостей, які можуть бути використані зловмисниками для порушення рівня захищеності КС, проведення вторгнень у КС або здійснення інших деструктивних дій з метою порушення властивостей інформаційних ресурсів або впливу на сам процес функціонування КС.

З метою забезпечення безпеки інформаційних ресурсів, що зберігаються та обробляються засобами КС, та елементів КС від кіберзагроз, в КС передбачена система забезпечення безпеки, яка у своєму складі містить: підсистему криптографічного захисту, підсистему ідентифікації, підсистему забезпечення цілісності, підсистему розмежування доступу, підсистему виявлення вторгнень, підсистему реагування, підсистему аудиту, підсистему оцінки захищеності тощо. Коректність функціонування системи забезпечення безпеки в цілому реалізує підсистема

оцінювання захищеності, яка ґрунтуються на роботі методів оцінки захищеності від кіберзагроз (на рівні хоста або кінцевих елементів) та методів оцінки захищеності від зовнішніх кіберзагроз (на рівні мережі). Дані методи застосовуються з метою оцінки рівня організації та реалізації безпеки КС, забезпечення безпеки інформаційних ресурсів та визначення достатності реалізованих засобів захисту при наявних вразливостях системи та впливі дій зловмисника та атак.

Робота даних методів вивчалася науковцями та описана в роботах [1–12]. Основними недоліками існуючих методів оцінювання захищеності є громіздка структура побудови, неврахування можливості роботи на різних рівнях моделі OSI, неврахування ресурсних обмежень та неможливість застосування при непередбачуваній мережевій активності, низька точність оцінювання, погана пристосованість до роботи в режимі реального часу, не врахування особливостей функціонування КС спеціального призначення.

В наслідок чого виникає доцільність висунути множину **вимог** до методів оцінювання рівня захищеності з метою їх застосування в КС, а саме: застосування методу в середовищі, яким характеризується КС, збільшення точності оцінювання захищеності, зменшення часу оцінювання, збільшення швидкості прийняття управлінського рішення, здатність обробляти великі масиви даних, функціонування при обмежених обчислювальних ресурсах, невелика математична складність, розподілення процесу прийняття управлінського рішення на внутрішню та зовнішню складові виходячи із характеристичних і параметричних особливостей складових та відповідно до рівнів моделі OSI .

Метою статті є розробка методу оцінки рівня захищеності мережевої частини комунікаційної системи спеціального призначення від кіберзагроз.

Об'єктом розгляду даної статті є процес забезпечення безпеки КС.

Предметом дослідження є метод оцінки рівня захищеності мережевої частини комунікаційної системи спеціального призначення від кіберзагроз.

Виклад основного матеріалу

Захищеність КС являє собою сукупність станів, в яких забезпечується безпека інформаційних ресурсів, тобто їх конфіденційність, цілісність і доступність. Процес оцінювання захищеності КС передбачає перевірку можливості порушення таких станів доступними зловмиснику способами. У зв`язку з тим, що підсистема оцінювання рівня захищеності має виявляти зміни стану захищеності як КС так і системи управління нею, то сама підсистема повинна відслідковувати весь трафік (службовий та інформаційний), що циркулює в КС. Для цього підсистема повинна функціонувати на всіх рівнях моделі OSI, здійснюючи при цьому контроль з`єднань, аналіз структури та вмісту мережевих пакетів, контроль власного трафіка. Джерелом вхідних даних для оцінювання рівня захищеності КС може бути образ різних за своєю природою об`єктів: символів, тексту, зображення, звуку, пакетів інформації, сигналів, сигнатур атак та інше. Ці дані надходять із підсистеми збору інформації, у вигляді вектору параметрів вхідного трафіка, які відображають щільність передачі, кількість пакетів, об`єм даних, тривалість з`єднання, кількість з`єднань тощо.

На відміну від автоматизованих систем комунікаційні системи включають в себе системи передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою електромагнітних засобів, мережі зв’язку, електричні кабельні мережі в частині, в якій вони використовуються для цілей передачі сигналів), що забезпечують передачу електронних інформаційних ресурсів, у тому числі засоби і пристрої зв’язку, комп’ютери, іншу комп’ютерну техніку, інформаційно-телекомунікаційні системи, які мають доступ до мережі передачі даних. У зв’язку з цим, з одного боку, кількість варіантів здійснення порушень рівня захищеності КС суттєво збільшується в порівнянні з автоматизованими системами, а з іншого боку, обмежені обчислювальні можливості мережевих вузлів не дозволяють проводити аналіз мережевої активності в режимі реального часу та з підтриманням належного рівня точності, використовуючи при цьому значну кількість параметрів, якими описується вхідний трафік (як інформаційний, так і службовий).

Існуючі підсистеми оцінювання рівня захищеності передбачають прийняття рішень щодо виявлення кіберзагроз на основі обробки множини різнорідних параметрів даних. Загроза в свою чергу реалізується різнонаправленими кібератаками (атаками). Інформація під час проходження системою аналізується за відповідними параметрами на предмет виявлення порушень захищеності. У результаті чого на виході підсистеми оцінювання рівня захищеності з`являється ознака рішення щодо відсутності, або наявності зміни стану рівня захищеності КС.

В якості навчальної множини існуючі підсистеми оцінювання рівня захищеності КС використовують конкретні різновиди атак, представлені в базі даних KDD-99. Ця база даних містить близько 8 000 000 записів щодо аномальних з`єднань та близько 2 000 000 відомостей про нормальний тип з`єднання. Кожен запис являє собою образ мережевого з`єднання, включає 41 параметр мережевого трафіка (табл. 1), серед яких міститься три типи ознак: символьні, логічні та числові. У загальному вигляді вони містять інформацію про тривалість з’єднання, тип протоколу, кількість спроб реєстрації тощо [13].

Таблиця 1

Параметри мережевого трафіка

№ з/п	Параметр	Опис	Рівень впливу
Основні ознаки			
1.	*duration*	Тривалість з'єднання (у секундах)	мережа
2.	*protocol_type*	Тип протоколу (TCP, UDP, etc.)	вузол, мережа
3.	*service*	Сервіс атакованого рівня	вузол
4.	*flag*	Статус з'єднання	вузол
5.	*src_bytes*	Вхідний потік, байт	вузол, мережа
6.	*dst_bytes*	Вихідний потік, байт	вузол, мережа
7.	*land*	Співпадіння адрес, 1 якщо з'єднання від/до того самого вузла	вузол, мережа
8.	*wrong_fragment*	Кількість неправильних фрагментів	вузол, мережа
9.	*urgent*	Кількість термінових пакетів	вузол, мережа
Статистичні ознаки			
10.	*count*	Кількість з'єднань з співпадаючим вузлом в поточній сесії	вузол
11.	*serror_rate*	% з'єднань що мали помилки „SYN"	вузол , мережа
12.	*rerror_rate*	% з'єднань що мали помилки „REJ" та з`єднання з однаковим вихідним вузлом	вузол
13.	*same_srv_rate*	% з'єднань з однаковим сервісом	вузол, мережа
14.	*diff_srv_rate*	% з'єднань на різні сервіси	вузол
15.	*srv_count*	Кількість з'єднань на такий самий сервіс.	мережа
16.	*srv_serror_rate*	% з'єднання з помилкою „SYN" в пакеті	вузол, мережа
17.	*srv_rerror_rate*	% з'єднання, що мають помилки „REJ"	вузол, мережа
18.	*srv_diff_host_rate*	% з'єднань з різними вузлами	вузол, мережа
Ознаки окремого з`єднання			
19.	*hot*	Кількість „гарячих" індикаторів	мережа
20.	*num_failed_logins*	Кількість невдалих спроб входу	мережа
21.	*logged_in*	Вдалий вхід в систему - 1, невдалий - 0	вузол
22.	*num_compromised*	Кількість "компроментуючих" умов	вузол, мережа
23.	*root_shell*	Доступ з адміністративними повноваженнями - 1; інакше 0	вузол
24.	*su_attempted*	1, якщо виконувалась "su root"; інакше 0	вузол
25.	*num_root*	Кількість спроб доступу з правами користувача	вузол
26.	*num_file_creations*	Кількість операцій створення файлів	вузол
27.	*num_shells*	Кількість спроб використання запитів на надання доступу	вузол
28.	*num_access_files*	Кількість операцій с файлами контролю доступу	мережа
29.	*num_outbound_cmds*	Кількість вихідних команд для FTP сесії	мережа
30.	*is_hot_login*	1, якщо логін належав до "гарячого" списку	мережа
31.	*is_guest_login*	1, якщо "гостьовий" вхід	мережа
Додаткові ознаки			
32.	*dst_host_count*	Кількість з`єднань до вузла, встановлених віддаленою стороною та використовуючих різні служби	мережа
33.	*dst_host_srv_count*	Кількість з`єднань до вузла, встановлених віддаленою стороною та використовуючих одну службу	мережа
34.	*dst_host_same_srv_rate*	% з`єднань до вузла, встановлених віддаленою стороною та використовуючих одну службу	мережа
35.	*dst_host_diff_srv_rate*	% з`єднань до вузла, встановлених віддаленою стороною та використовуючих різні служби	мережа
36.	*dst_host_same_src_port_rate*	% з`єднань до вузла з поточним джерелом	мережа
37.	*dst_host_srv_diff_host_rate*	% з`єднань до вузла з різним джерелом	мережа
38.	*dst_host_serror_rate*	% з`єднань з помилкою типу SYN для даного приймача	мережа

Закінчення табл. 1

39.	*dst_host_srv_serror_rate*	% з`єднань з помилкою типу SYN для служби приймача	мережа
40.	*dst_host_rerror_rate*	% з`єднань з помилкою типу REJ для даного приймача	мережа
41.	*dst_host_srv_rerror_rate*	% з`єднань з помилкою типу REJ для служби приймача	мережа

На основі вхідних параметрів трафіка відбувається перевірка на наявність порушень захищеності та маркування їх як “порушення” або “не порушення”. Вказаний запис складається з 42 полів. Перші 41 поле описують ознаки мережевого трафіка, а останнє 42-е поле вказує на тип трафіка, який описується. Вказане поле може приймати значення “normal”, якщо дане мережеве з`єднання відноситься до “нормального” стану трафіка, або найменування типу атак (наприклад, “ipsweep”). Дане поле також необхідне для виконання процесу навчання системи.

Вирішуючи задачу класифікації кібератаки (наприклад по її сигнатурі) підсистема оцінювання рівня захищеності ставить у відповідність наведеним вище параметрам мережевого трафіка 29 типи найбільш часто застосованих атак, які поділяються на 5 категорії:

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

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

– R2L атаки – отримання доступу незареєстрованого користувача до мережі з боку віддаленої станції. Поділяють R2L атаки на: ftp_write, guess_passwd, imap, multihop, phf, spy, warezclient, warezmaster та інші атаки.

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

– На сьогодні, дослідники встановили та відокремлюють ще одну категорію атак, яка притаманна саме КС – 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 пристроях, які не розглядаються в теоретичному описі криптографічного алгоритму. До Side-channel атак належать: probing attack, timing attack, fault–induction attack, power analysis attack, electromagnetic analysis attacks та інші атаки. Дана категорія атак може вплинути на рівень захищеності як мережевої так і хостової частини комунікаційної системи спеціального призначення.

Після чого, відкласифіковані параметри вхідних даних (атак) співвідносяться до множини управляючих рішень щодо варіантів реагування на кожен окремий тип атаки. В наслідок чого встановлюється рівень захищеності КС.

З огляду на вищезазначене розробляємий метод оцінки захищеності має враховувати наступні особливості КС:

– переважно якісний характер показників, що враховуються під час аналізу захищеності КС;

– необхідність обліку великої кількості показників;

– складний взаємозв’язок показників якості захисту з показниками якості функціонування КС;

– взаємозв’язок та взаємозалежність елементів КС.

Виходячи із зазначеного пропонується провести розробку методу оцінки рівня захищеності мережевої частини комунікаційної системи спеціального призначення від кіберзагроз шляхом удосконалення існуючого методу оцінки рівня захищеності мережі, з урахуванням вищезазначених вимог, для застосування методу в КС.

Позначення вихідних даних. Розглядається ситуація рівноймовірнісного знаходження системи у стані протікання порушень захищеності КС. В один і той же час відбуваються як порушення захищеності на мережевій частині КС, так і пошук варіантів протидій на можливі порушення. Для моделювання такої ситуації будується навчальна вибірка, яка має в собі 20 % нормальних повідомлень та 80 % аномальних повідомлень, які містять типи загроз (порушень). Також будується база з варіантами протидій на множину виявлених порушень. Так як кожен тип порушень характеризує множину цілей при їх проведенні у КС, дії яких направлені на мережеву частину КС. Саме тому для оцінки рівня захищеності відбувається ідентифікація вхідних даних (типів порушень) на основі параметрів даних, які характеризують саме мережеву частину КС. Загальна кількість параметрів $x_i = 18$, до них належать: x_1 – du-

ration, x_2 – hot, x_3 – num_failed_logins, x_4 – num_outbound_cmds, x_5 – srv_count, x_6 – srv_serror_rate, x_7 – srv_rerror_rate, x_8 – srv_diff_host_rate, x_9 – dst_host_count, x_{10} – dst_host_srv_count, x_{11} – dst_host_same_srv_rate, x_{12} – dst_host_diff_srv_rate, x_{13} – dst_host_same_src_port_rate, x_{14} – dst_host_srv_diff_host_rate, x_{15} – dst_host_ serror_rate, x_{16} – dst_host_srv_serror_rate, x_{17} – dst_host_rerror_rate, x_{18} – dst_host_srv_rer-ror_rate.

Вхідний трафік, який несе в собі мову, відео, передачу даних тощо, складається з параметрів мережевого трафіка. В якості вхідних даних застосовується параметри бази даних KDD Cup 2009 Data, які характеризують вищевказані параметри [13].

Під час виявлення порушень буде застосовуватись механізм логічного виводу для опису бази вхідних параметрів. На підставі співставлення вхідних параметрів, у системі правил буде формуватись рішення щодо їх класифікації.

В наслідок чого, як вже зазначалось, відбувається співвідношення рівня захищеності КС до можливих видів порушень та встановлюється рівень захищеності КС.

Вихідним значенням є: значення ідентифікованої поведінки та проаналізованого стану КС у вигляді $Y_n = 1(t)$ – "неконтрольований" вплив, або $Y_n = 0$, "контрольований" вплив. Також на виході отримуються класифікаційні параметри виявленої поведінки та пропозицій для підсистеми реалізації рішень відносно варіантів реагування на виявлене порушення.

Обмеження та допущення. Для ідентифікації поведінки розглянуто штучні порушення (сигнатури атак), що є загрозами для КС. Пошукова вибірка порушень удосконаленого методу обмежена кількістю навчальної вибірки існуючого методу. Передбачена можливість проведення навчання новим (нововиявленим) типам поведінки в ході моделювання системи. Кожна нововиявлена поведінка фіксується як вторгнення. Процес порушення є квазістаціонарним на інтервалі часу $(t_0 ... T)$. При побудові імітаційної моделі доцільно врахувати характеристику існуючих КС. Вважатимемо, що у складі кожної КС функціонує система управління (СУ), що складається з множини підсистем, які виконують функції управління внутрішніми (хостовими) та зовнішніми (мережевими) ресурсами відповідно до рівнів моделі OSI. Вказана СУ здатна проводити виявлення неточності та неповноти даних вхідного трафіка.

Необхідно: підвищити показники ефективності функціонування методу оцінки рівня захищеності мережевої частини комунікаційної системи спеціального призначення від кіберзагроз, а саме збільшення точності, швидкості та повноти оцінки та зменшення інтервалу часу оцінки до рівня реального часу, шляхом удосконалення існуючого методу відповідно до вищезазначених вимог.

Суть розробки методу полягає у: оцінці рівня захищеності КС з використанням розподільчої ідентифікації параметрів кібератак з проведенням вибору щодо застосування заходів із захисту системи при повному статистичному описі КС та врахуванням стратегій впливу на неї на основі динамічного програмування.

Новий метод оцінювання захищеності комунікаційних систем спеціального призначення від зовнішніх загроз

Оцінювання рівня захищеності мережевої частини КС від кіберзагроз може відбуватись тільки у разі проведення ідентифікації параметрів порушень, які реалізуються множиною різнонаправлених та різних за своїм змістом атак.

Тому проведемо ідентифікацію вхідних даних (параметрів даних) трафіка.

I. Під ідентифікацією розумітимемо знаходження оптимальної в деякому сенсі моделі, побудованої за результатами спостережень над вхідними та вихідними змінними об'єкта, а саме набором параметрів трафіку [14]. Завданням ідентифікації є зворотне завдання системного синтезу.

З урахуванням завдань ідентифікації виділяють два типи [15]:

– структурна ідентифікація, яка дозволяє визначити форму моделі з деякого заданого класу функцій;

– параметрична ідентифікація, яка визначає параметри моделі.

Однак виходячи із поставленого завдання, щодо ідентифікації вхідних даних на основі параметрів кібератак (сигнатур), буде застосована саме параметрична ідентифікація

При параметричній ідентифікації дані про об'єкт обробляються для отримання про нього апостеріорної інформації. При цьому оцінюються параметри обраної моделі. У найпростіших випадках така оцінка може виконуватися по графіку перехідної характеристики.

Для ідентифікації об'єкта довільного порядку використовується метод найменших квадратів, що потребує мінімізації середнього квадрата неузгодженості правої і лівої частин рівняння:

$$S = \int_0^T \left[\sum_{i=0}^{n} a_i \cdot y^{(i)}(t) - \sum_{j=0}^{m} b_j \cdot x^{(j)}(t) \right]^2 dt \to \min , \quad (1)$$

де $y^{(i)}$ і $x^{(j)}$ – похідні *i*-го і *j*-го порядку від функцій вихідного і вхідного сигналів.

Рішення завдання (1) зводиться до системи:

$$\begin{cases} \dfrac{\partial S}{\partial a_i} = 0, i = 0,...,n; \\ \dfrac{\partial S}{\partial b_j} = 0, i = 0,...,m. \end{cases} \quad (2)$$

Перетворюючи (2) відповідно до рівняння (1), отримаємо систему лінійних алгебраїчних рівнянь:

$$\begin{cases} \sum\limits_{i=0}^{n} a_i \cdot \int\limits_0^T y^{(i)}(t) \cdot y^{(k)}(t)dt - \sum\limits_{j=0}^{m} b_j \cdot \int\limits_0^T x^{(j)}(t) \cdot y^{(k)}(t)dt = 0, \\ k = 0,...,n \\ \sum\limits_{i=0}^{n} a_i \cdot \int\limits_0^T y^{(i)}(t) \cdot x^{(k)}(t)dt - \sum\limits_{j=0}^{m} b_j \cdot \int\limits_0^T x^{(j)}(t) \cdot x^{(k)}(t)dt = 0, \\ k = 0,...,m. \end{cases} \quad (3)$$

Для вирішення системи (3) щодо невідомих параметрів $a_n,...,a_0$ та $b_m,...,b_0$ необхідно знати похідні вхідного і вихідного сигналів об'єкта, які знаходяться в результаті згладжування функцій $X(t)$ і $Y(t)$ на відрізку $t \in [0,T]$. Для розрахунку коефіцієнта b_1 використаємо формулу: $b_1 = a_2 \cdot y_0^{(1)}$.

Похибка чисельного диференціювання, як правило, досить висока, тому схему визначення коефіцієнтів, потрібно використовувати диференціювання аналітичних виразів для $X(t)$ і $Y(t)$.

При побудові моделі оцінки захищеності за експериментально отриманими даними поширеною є ситуація, для якої практично вся інформація, що використовується обробником для розв'язання поставленої задачі, обмежується вибіркою вихідних даних. Тому для розв'язання задачі параметричної ідентифікації використовують методи, орієнтовані виключно на інформацію про невідповідність між виходами об`єкта та моделі.

В загальному випадку для довільної моделі $y = f(X, A)$ відомої структури рівень невідповідності між виходами об`єкта та моделі $\varepsilon_i = z_i - \tilde{y}_i$, $i = \overline{1,n}$ залежить від вибору параметрів моделі, тобто елементів вектора $A = [a_0, a_1, ..., a_l]$. Тому, якщо ввести показник якості параметричної ідентифікації, який інтегрує в собі всю інформацію про рівні нев'язок ε_i, $i = \overline{1,n}$ і містить відомості про залежність рівня невідповідності між виходами об`єкта та моделі від значень параметрів моделі, то мінімізація цього показника дозволить визначити оптимальні параметри моделі.

Для рішення задачі параметричної ідентифікації застосуємо показники:

$$Q = \sum_{i=1}^{n} \varepsilon_i^2 = \sum_{i=1}^{n} (z_i - f(X_i, A))^2. \quad (4)$$

Функція $Q(A)$ неперервно залежить від $a_0, a_1, ..., a_l$ і дозволяє обчислити частинні похідні $\partial Q / \partial a_i$, $i = \overline{0,l}$, скласти з них систему рівнянь виду

$$\frac{\partial Q}{\partial a_i} = 0, \; i = \overline{0,l},$$

та знайти оптимальні параметри моделі. Отримані таким шляхом оцінки називають оцінками за методом найменших квадратів, бо оптимізація параметрів моделі призводить до мінімуму (4) показника Q, тобто за мінімумом суми квадратів нев'язок.

Оскільки структура $f(X_i, A)$ не змінюється під час оцінювання параметрів $A = [a_0, a_1, ..., a_l]$, кількісні значення функціоналу Q є залежними тільки від вибору значень оцінок $a_0, a_1, ..., a_l$, тобто Q можна розглядати як функції параметрів: $Q = Q(a_0, a_1, ..., a_l)$. Тоді задачу параметричної ідентифікації можна сформулювати так: підібрати на множині $\{A\}$ можливих значень параметрів моделі такі значення оцінок $\tilde{A}$, щоб функції $Q(A)$ досягли своїх мінімумів, тобто метою цього аналізу є пошук

$$\tilde{A} = \arg \min_{A \in \{A\}} Q(A).$$

При оцінюванні параметрів регресійної моделі, виходячи з умов мінімізації суми квадратів невідповідність, загальні формули для обчислення оцінок легко отримати у матричній формі запису:

$$Q = \varepsilon^T \varepsilon = (Z - X\tilde{A})^T (Z - X\tilde{A}) =$$
$$= Z^T Z - 2Z^T X\tilde{A} + \tilde{A}^T X^T X\tilde{A},$$
$$\frac{\partial Q}{\partial \tilde{A}} = -2X^T Z + 2X^T X\tilde{A} = 0,$$
$$\tilde{A} = (X^T X)^{-1} X^T Z.$$

Матриця коваріацій оцінок має вигляд:

$$C\{\tilde{A}\} = \sigma_e^2 (X^T X)^{-1}.$$

Оцінка дисперсії помилки розраховується за формулою:

$$\tilde{\sigma}_e^2 = \frac{1}{n-l} \sum_{i=1}^{n} \varepsilon_i^2 = \frac{S^{(l)}}{n-l},$$

де l – кількість параметрів регресійної моделі; $S^{(l)}$ – сума квадратів нев'язок цієї моделі.

II. Наступним кроком буде проведення оцінки рівня захищеності мережевої частини комунікаційної системи спеціального призначення від кіберзагроз на основі ідентифікованих даних та пошуку відповідності цих даних множині варіантів впливу на загрози.

У моделях, які характеризуються динамічною структурою побудови, до яких і належить мережева частина КС, стан захищеності являє собою часовий

зріз властивості захищеності інформації і описується значенням відповідного показника в певний фіксований момент часу.

Процес отримання оцінки рівня стану захищеності КС x і процес застосування засобів забезпечення захищеності (ЗЗ) u реалізуються по крокам (етапам). На кожному n-му кроці отримується деяка сукупність даних про стан захищеності системи x_n, яка залежить від реалізованих варіантів впливу на порушення безпеки λ, що характеризують стан захищеності КС і впливають на вибір використовуваних захисних механізмів. Використовуючи отримані і вже відомі відомості про стан захищеності системи $x_n, x_{n-1},...,$ приймається рішення u_n про застосування засобів забезпечення захищеності, яке може залежати і від раніше прийнятих рішень u_{n-1}, u_{n-2}. Якщо $n = 1,2,...,N$, то повна сукупність даних про стан захищеності системи x, рішень про застосування засобів забезпечення безпеки u та реалізовані варіантів впливу на порушення безпеки λ можна описати векторами:

$$x = X_N = \{x_1,...,x_N\},$$
$$u = U_N = \{u_1,...,u_N\},$$
$$\lambda = \Lambda_N = \{\lambda_1,...,\lambda_N\}.$$

Слід врахувати, що задіяні на будь-якому кроці ЗЗ u_n можуть вплинути на параметри впливу на порушення безпеки $\lambda_{n+1}, \lambda_{n+2},...$ на наступних кроках, а також на обсяг і якість одержуваних на цих кроках даних про стан захищеності КС $x_{n+1}, x_{n+2},...$. Така наявність зворотного зв'язку характерна для КС загального вигляду, в яких всі або деякі компоненти рішення u_n є діями, що управляють змінами впливу на порушення безпеки λ_n та має місце в КС. Оскільки будь-які вжиті ЗЗ впливають на значення λ_n і на подальших кроках, то такі багатокрокові процеси прийняття рішення є керованими [16].

Математичним відображенням цього зворотного зв'язку є залежність розподілів ймовірностей значень λ_n і x_n від послідовності попередньо застосованих ЗЗ $U_{N-1} = \{u_1,...,u_{N-1}\}$. Повний статистичний опис багатокрокового процесу для будь-якої сукупності прийнятих ЗЗ $u_1, u_2,...$ досягається завданням послідовності умовних розподілів ймовірності для спостережуваних даних і параметрів для всіх значень $n = 1,2,...,N$, добуток яких утворює спільну щільність ймовірностей встановлення порушень $x = X_n$ і $\lambda = \Lambda_n$ при заданій послідовності ЗЗ $u = U_n$ [16].

При виборі рішень про застосування необхідних ЗЗ u_n використовуємо тільки ті дані спостереження, які отримані до n-го кроку включно, тобто $\{x_1,...,x_n\} = X_n$. Тому правило прийняття рішення про застосування ЗЗ u_n можна задати ймовірнісною мірою з щільністю ймовірностей ϕ_n, яка залежить від X_n, а також від сукупності попередніх рішень $\{u_1,...,u_n\} = U_{n-1}$. У цьому випадку величина ϕ_n буде визначатися виразом:

$$\phi_n = \phi_n(u_n \mid X_n, U_{n-1}), \quad (5)$$

Знаходження оптимальної послідовності прийняття ЗЗ для багатокрокової процедури проводиться методами динамічного програмування в загальній стохастичній формі, які при певних обмеженнях на умови розподілу ймовірності для x_n і λ_n та функцію втрат $g(u,\lambda,x) = g(U_N, \Lambda_N, X_N)$, призводять до ефективної обчислювальної процедури знаходження оптимальних рішень і до аналітичних результатів. При цьому оптимальна послідовність прийняття ЗЗ визначається системою рекурентних співвідношень, яка містить послідовність мінімізацій і усереднень для величин апостеріорних ризиків.

Величина середнього ризику виникнення порушень визначається виразом:

$$R(\varphi) = R(\Phi_N) = M\left\{g\left(U_N, \Lambda_N, X_N\right)\right\},$$

де $\Phi_N = \left(\varphi_1, \varphi_2,..., \varphi_N\right)$ – сукупність щільностей ймовірностей (5), кожна з яких задає правило прийняття ЗЗ на n-му кроці, а їх добуток – вирішальне правило в цілому.

Нехай оптимальному правилу прийняття рішення при реалізованих засобах забезпечення захищеності відповідає сукупність Φ_{N0}. Тоді мінімальний (байєсів) середній ризик виникнення порушень:

$$R(\Phi_{N0}) = \min_{\Phi_N} M\left\{g(U_N, \Lambda_N, X_N)\right\} =$$
$$= \min_{(\varphi_1,...,\varphi_{N-1})}\left[\min_{\varphi_N} M\left\{g(U_N, \Lambda_N, X_N) \mid X_N, U_N\right\}\right]. \quad (6)$$

Умовне математичне сподівання в (6) являє собою функцію апостеріорного ризику виникнення порушень при сукупності прийнятих ЗЗ U_N і даних про стан системи X_N:

$$R_N(U_N, X_N) = M\left\{g(U_N, \Lambda_N, X_N) \mid X_N, U_N\right\}. \quad (7)$$

Математичне сподівання функції втрат з урахуванням (7) задається виразом:

$$M\left\{g(U_N, \Lambda_N, X_N)\right\} = M\left\{R_N(U_N, X_N)\right\} =$$
$$= M\left\{\int R_N(U_N, X_N)\varphi_N(u_N \mid X_N, U_{N-1})du_N\right\}.$$

Тоді вираз у квадратних дужках в (6) можна записати у вигляді:

$$\min_{(\varphi N)} M\left\{M\left\{g(U_N, \Lambda_N, X_N) \mid X_N, U_N\right\}\right\} =$$
$$= M\left\{\min_{(uN)} R_N(U_N, X_N)\right\}.$$

Мінімум виразу $\int R_N(U_N, X_N)\varphi_N(u_N \mid X_N, U_{N-1})du_N$ досягається для функції:

$$\varphi_N = \varphi_{N0} = \varphi_{N0}(u_N \mid X_N, U_{N-1}) = \delta(u_N - u_{N0}(X_N)),$$

де $u_{N0}(X_N)$ – значення u_N, при якому досягається мінімум підінтегрального виразу $R_N(U_N, X_N)$. Це значення визначає оптимальне байєсове правило рішення на N-му кроці. Воно знаходиться з умови:

$$\begin{aligned} &R_N(u_{N0}(X_N), U_{N-1}, X_N) = \\ &= \min_{u_N} R_N(U_N, X_N) = \tilde{R}_N(U_{N-1}, X_N), \end{aligned} \tag{8}$$

$$\begin{aligned} &\tilde{R}_N(U_{N-1}, X_N) = \min_{uN} R_N(U_N, X_N) = \\ &= \min_{u_N} \int g(U_N, \Lambda_N, X_N) p(\Lambda_N \mid X_N, U_{N-1}) d\Lambda_N \end{aligned} \tag{9}$$

є апостеріорний ризик порушення захищеності, мінімізований прийнятими ЗЗ u_N на останньому кроці, а $p(\Lambda_N \mid X_N, U_{N-1})$ – апостеріорна щільність ймовірності сукупності послуг безпеки $\Lambda_N = (\lambda_1, ..., \lambda_N)$, яка залежить тільки від стану захищеності ІС на n-му кроці X_N і від ЗЗ, що приймаються $U_N = (u_1, ..., u_{N-1})$.

Апостеріорний ризик на $(N-1)$ кроці знаходиться з повного апостеріорного ризику виникнення порушень мінімізацією по u_n і усередненням по x_N:

$$\begin{aligned} R_{N-1}(U_{N-1}, X_{N-1}) &= M\left\{\tilde{R}_N(U_{N-1}, X_N) \mid X_{N-1}, U_{N-1}\right\} = \\ &= \int \tilde{R}_N(U_{N-1}, X_N) p_N(x_N \mid X_{N-1}, U_{N-1}) dx_N. \end{aligned}$$

Тоді вираз (6) можна записати у вигляді:

$$R(\Phi_{N0}) = \min_{(\varphi_1 \ldots \varphi_{N-1})} M\left\{R_{N-1}(U_{N-1}, X_{N-1})\right\}. \tag{10}$$

Виконавши мінімізацію за останньою з функцій $\varphi_1, ..., \varphi_{N-1}$ представимо (6) наступним чином:

$$R(\Phi_{N0}) = \min_{(\varphi 1, \ldots \varphi_{N-2})} \left[M\left\{\tilde{R}_{N-1}(U_{N-2}, X_{N-1})\right\}\right].$$

Оптимальне байєсове правило рішення на $(N-1)$-му кроці визначається функцією, яка знаходиться з рівняння $u_{N-1,0}(X_{X-1})$, аналогічно умові (9):

$$\begin{aligned} &R_{R-1}(u_{N-1,0}(X_{X-1}), U_{N-2}, X_{N-1} = \\ &= \min_{(u_{N-1})} R_{N-1}(U_{N-1}, X_{N-1}) = \tilde{R}_{N-1}(U_{N-2}, X_{N-1}). \end{aligned}$$

Продовжуючи мінімізації для $n = N-2, N-3, ...,$ отримаємо співвідношення, яке визначає оптимальне правило вибору ЗЗ на будь-якому кроці:

$$\begin{aligned} \tilde{R}_n(U_{n-1}, X_n) &= R_n(u_{n0}(X_n), U_{n-1}, X_n) = \\ &= \min_{(u_n)} R_n(U_n, X_n). \end{aligned} \tag{11}$$

Апостеріорний ризик на n-му кроці $R_n(U_n, X_n)$ задається співвідношенням, що послідовно визначає функції апостеріорного ризику:

$$\begin{aligned} R_n(U_n, X_n) &= M\left\{\tilde{R}_{n+1}(U_n, X_{n+1}) \mid X_n, U_n\right\} = \\ &= M\left\{\min_{(u_{n+1})} R_{n+1}(U_{n+1}, X_{n+1}) \mid X_n, U_n\right\}. \end{aligned} \tag{12}$$

Спільно з виразами (7) і (8) для кінцевого значення апостеріорного ризику і рівнянням (11) це співвідношення визначає оптимальне багатокрокове правило прийняття ЗЗ.

Разом з виразом (12) можна ввести еквівалентне йому рекурентне співвідношення для апостеріорних ризиків виникнення порушень $\tilde{R}_n(U_{n-1}, X_n)$, мінімізованих вибором ЗЗ $u_n, u_{n+1}, ..., u_N$. Воно отримується з (11) і (12) і має вигляд:

$$\begin{aligned} &\tilde{R}_n(U_{n-1}, X_n) = \\ &= \min_{u_n} \int \tilde{R}_{n+1}(U_n, X_{n+1}) p_{n+1}(X_{n+1} \mid X_n, U_n) dx_{n+1}. \end{aligned} \tag{13}$$

Його відмінністю від (12) є зміна порядку застосування операцій обчислення математичного сподівання і мінімізації. Щільність ймовірності $p_{n+1}(X_{n+1} \mid X_n, U_n)$, що входить до складу (12) і (13), визначається через щільності $p_n(x_n \mid \Lambda_n, X_{n-1}, U_{n-1})$ і $p_n(\lambda_n \mid \Lambda_n, \Lambda_{n-1}, U_{n-1})$ за звичайними правилами теорії ймовірностей.

Також під час моделювання процесу оцінки стану захищеності КС має бути враховано ще і стратегії проведення впливу на КС з метою проведення деструктивних дій на КС:

Тому, для отримання повної картини захищеності КС як на окремому рівні моделі OSI так і на окремі елементи КС з боку об`єкту впливу на КС, необхідно врахувати саме об`єкти КС, які можуть бути атаковані. Тому реалізація варіантів проведення порушень Z на окремі об`єкти КС $l$ може бути описана законом імовірності. До об`єктів на які може поширитись дана імовірність можливо віднести:

$P(Z / l)$ – імовірність впливу варіантів проведення кібератак Z на окремий об`єкт КС l;

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

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

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

Тобто:

$$P(z / l) : z \to l; \tag{14}$$

$$P(z / \sum l) : z \to \sum l; \tag{15}$$

$$P\left(\sum z / l\right): \sum z \to l\,; \quad (16)$$

$$P\left(\sum z / \sum l\right): \sum z \to \sum l\,. \quad (17)$$

Виходячи із вказаного імовірність здійснення j_z кібератак на множину об'єктів КС l буде обчислюватись:

$$P(j_z, l) = \prod_{i=1}^{l} P_i^{j_z}\,. \quad (18)$$

Враховуючі те, що кожен елемент КС містить систему оцінки захищеності, то імовірність встановлення рівня захищеності буде визначатися:

$$P_B = \min_b P_i^b, \quad b = 1...b_n\,. \quad (19)$$

В цілому структурна схема оцінювання рівня захищеності мережевої частини КС від кіберзагроз зазначена на рис. 1.

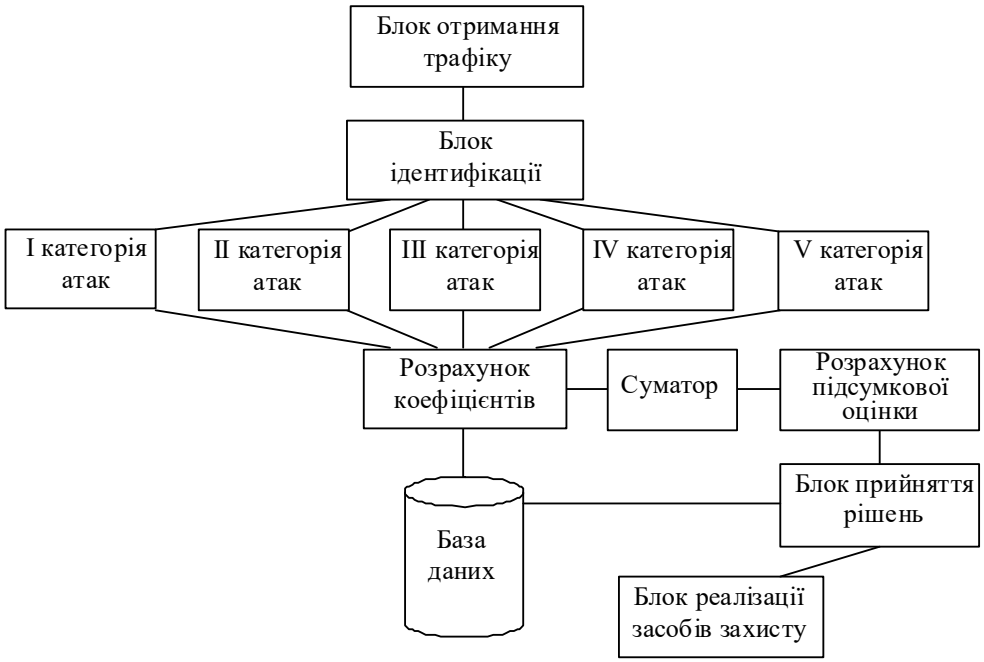

Рис. 1. Схема реалізації оцінювання рівня захищеності мережевої частини КС

Результати експериментальних досліджень

В ході імітаційного моделювання побудови запропонованого методу в середовищі MATLAB було сформовано навчальну вибірку, яка має в собі 20% нормальних з`єднань та 80% аномальних, які містять зазначені типи порушень (атак).

Процес оцінки захищеності в ході моделювання включає наступні кроки:

1. Отримання вхідних даних $X(t) = 1,...,41$.

2. Ідентифікація вхідних даних (посигнатурно):

2.1. На рівні хоста $X_V(t) = \{x_b(t)\}$;

2.2. На рівні мережі $X_M(t) = \{x_m(t)\}$, $m = 1,..,18$.

3. Перевірка коректності ідентифікації.

4. Оцінка рівня захищеності моделі.

5. Програмування в середовищі MATLAB.

6. Випробування та дослідження властивостей імітаційної моделі. Придатність імітаційної моделі для вирішення завдань, пов'язаних з оцінкою рівня захищеності КС:

6.1. Оцінка адекватності моделі.

6.2. Оцінка стійкості моделі.

6.3. Оцінка чутливості моделі.

7. Економічна оцінка ефективності виявлення вторгнень.

Результати досліджень щодо оцінки рівня захищеності КС показали, що:

– отримані результати підтверджують той факт, що якість ідентифікації та оцінки стану моделі залежить від кількості еталонів окремих класів в навчальній виборці. Також при невеликій кількості еталонів помилки не перевищує 10 %;

– точність та час прийняття рішень щодо оцінки рівня захищеності мережевої частини комунікаційної системи спеціального призначення від кіберзагроз в порівнянні з методом [4–5] покращились.

Висновки

У статті представлено удосконалений метод оцінки рівня захищеності мережевої частини комунікаційної системи спеціального призначення від кіберзагроз на основі алгоритму розподільчої ідентифікації та динамічного програмування.

Суть методу: полягає в оцінці рівня захищеності КС з використанням розподільчої ідентифікації параметрів кібератак з проведенням вибору щодо застосування заходів із захисту системи при повному статистичному описі КС та врахуванням стратегій впливу на неї на основі динамічного програмування.

На відміну від існуючого методу, який оцінює рівень захищеності на основі повної вибірки параметрів кібератак, які не враховують характеристичні особливості функціонування КС, шляхом послідовного аналізу процесу впливу аномалій на інформаційну систему та без можливості пошуку нових типів кібератак та підбору управлінських рішень направлених на підтримання рівня захищеності системи, що призводить до зменшення рівня точності та збільшення часу прийняття рішень, удосконалений метод забезпечує оцінку рівня захищеності КС на основі множини параметрів (сигнатурним шляхом), які відображають саме функціонування елементів мережевої частини КС з функцією паралельно-розподільчої ідентифікації нових типів кібератак та врахуванні стратегій їх впливу на КС, з використанням методу динамічного програмування та алгоритму розподільчої ідентифікації методом найменших квадратів.

Даний метод дозволяє: зменшити час прийняття рішення щодо оцінки рівня захищеності КС на 17–22%, збільшення точності прийняття рішення з ідентифікації кібератаки на 16–23%, при збереженні повноти навчальної вибірки запропонованого методу не нижче, ніж у існуючих методів, за рахунок використання алгоритму розподільчої ідентифікації, ідентифікації нових типів кібератак.

У ході подальших досліджень буде розроблено метод оцінки рівня захищеності хостової частини комунікаційної системи спеціального призначення від кіберзагроз.

Список літератури

1. Кучернюк П.В. Модель загроз безпеки в інформаційно-комунікаційних системах на основі регресійного аналізу / П.В. Кучернюк, А.О. Довгаль // Електроніка та зв'язок: науково-технічний журнал. – 2017. – Т. 22, № 2(97). – С. 79-84.
2. Голобородько М.Ю. Методи числової оцінки рівня захищеності інформації у сегменті корпоративної інформаційної системи / М.Ю. Голобородько, О.А. Курченко, О.С. Кирись // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України ім. І. Черняховського. – 2014. – № 2(51). – С. 137-139.
3. Дудикевич В.Б. Аналіз моделей захисту інформації в інформаційних мережах держави / В.Б. Дудикевич, І.Р. Опірський // Системи обробки інформації. – 2016. – № 4(141). – С. 86-89.
4. Велігура А.В. Оцінювання стану інформаційної безпеки підприємства / А.В. Велігура // Управління проектами та розвиток виробництва. – 2014. – № 4(52). – С. 28-39.
5. Гловацький В.В. Методи оцінювання стану безпеки та загроз інформаційних ресурсів / В.В. Гловацький // Зв'язок. – 2016. – № 5. – С. 13-16.
6. Гарасимчук О.І. Оцінка ефективності систем захисту інформації / О. І. Гарасимчук, Ю.М. Костів // Вісник КНУ ім. М. Остроградського. – 2011. – № 1(66), Ч. 1. – С. 16-20.
7. Хнигічева А.М. Моделювання захищеності складних інформаційно-комунікаційних систем із використанням логіко-ймовірнісного методу / А.М. Хнигічева, О.М. Новіков, А.О. Тимошенко // Наукові вісті НТУУ "КПІ". Інформаційні технології, системний аналіз і керування. – 2010. – № 6. – С. 70-77.
8. Грищук Р.В. Кількісна оцінка рівня захищеності об'єктів електронно-обчислювальної техніки з урахуванням їх функціонування в умовах інформаційного конфлікту / Р.В. Грищук // Вісник ЖДТУ Технічні науки: інформатика, обчислювальна техніка. – 2008. – № 3(46). – С. 113-120.
9. Бурячок В.Л. Алгоритм оцінювання ступеня захищеності спеціальних інформаційно-телекомунікаційних систем / В.Л Бурячок // Захист інформації. – 2011. – № 3(52). – С. 19-27.
10. Ільяшов О.А. До питання захисту інформаційно-телекомунікаційної сфери від стороннього кібернетичного впливу / О.А. Ільяшов, В.Л. Бурячок // Наука і оборона. – 2010. – № 4. – С. 35-40.
11. Потій О.В. Дослідження методів оцінки ризиків безпеці інформації та розробка пропозицій з їх вдосконалення на основі системного підходу / О.В. Потій, А.В. Лєншин // Збірник наукових праць Харківського національного університету Повітряних Сил. – 2010. – № 2(24). – С. 85-91.
12. Методика оцінки кібернетичної захищеності системи зв'язку організації / І.М. Козубцов, Л.М. Козубцова, В.В. Куцаєв, Т.П. Терещенко // Сучасні інформаційні технології у сфері безпеки та оборони. – 2018. – № 1(31). – С. 43-46.
13. Офіціальний сайт KDD Cup 1999 Data [Електронний ресурс]. – Режим доступу: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.
14. Будкова Л.В. Комплексна оцінка характеристик та ідентифікація трафіку в інформаційних телекомунікаційних мережах / Л.В. Будкова, В.І. Корнієнко // Системи обробки інформації. – 2013. – № 2(109). – С. 207-211.
15. Герасіна О. В. Методика інтелектуальної ідентифікації та прогнозування трафіку в інформаційних телекомунікаційних мережах / О.В. Герасіна // Системи обробки інформації. – 2018. – № 1(152). – С. 94-99. https://doi.org/10.30748/soi.2018.152.14.
16. Сторчак А.С. Метод оцінки захищеності інформації на основі багатокрокових процесів прийняття рішень / А.С. Сторчак // Восточно-Европейский журнал передовых технологий. – 2013. – № 6(12). – С. 82-85.

References

1. Kucherniuk, P.V. and Dovhal, A.O. (2017), "Model′ zahroz bezpeky v informatsiyno-komunikatsiynykh systemakh na osnovi rehresiynoho analizu" [Model threats to security of information and communications systems based on regression analysis], *ElectronCommun*, Vol. 22, No. 2(97), pp. 79-84.
2. Goloborodko, M.Yu., Kurchenko, O.A. and Kyrys′, O.S. (2014), "Metody chyslovoyi otsinky rivnya zakhyshchenosti informatsiyi u sehmenti korporatyvnoyi informatsiynoyi systemy" [Methods of numerically assessing the level of information security in the corporate information system segment], *Research papers collection of the Center of military and strategic studies*, No. 2(51), pp.137-139.
3. Dudykevych, V.B. and Opirskyi, I.R. (2016), "Analiz modelei zakhystu informatsii v informatsiinykh merezhakh derzhavy" [Analysis of models of information security in information networks of state], *Information Processing Systems*, No. 4(141), pp. 86-89.
4. Veligura, A.V. (2014), "Otsinyuvannya stanu informatsiynoyi bezpeky pidpryyemstva" [Evaluation of enterprise information security], *Project management and development of production*, No. 4(52), pp. 28-39.
5. Glovatsky, V.V. (2016), "Metody otsinyuvannya stanu bezpeky ta zahroz informatsiynykh resursiv" [Methods of assessing the state of security and threats to information resources], *Communication*, No. 5, pp. 13-16.
6. Harasymchuk, O.I. and Kostiv, Y.M. (2011), "Otsinka efektyvnosti system zakhystu informatsiyi" [Assessment of the effectiveness of information security systems], *Transactions of Kremenchuk Mykhailo Ostrohradskyi National University*, No. 1(66), pp. 16-20.
7. Khnigicheva, A.M., Novikov, O.M. and Tymoshenko, A.O. (2010), "Modelyuvannya zakhyshchenosti skladnykh informatsiyno-komunikatsiynykh system iz vykorystannyam lohiko-ymovirnisnoho metodu" [Modeling the security of complex information and communication systems using the logic-probabilistic method], *Research Bulletin of the National Technical University of Ukraine "Kyiv Polytechnic Institute"*, Vol. 6, pp. 70-77.
8. Hryshchuk, R.V. (2008), "Kil′kisna otsinka rivnya zakhyshchenosti ob'yektiv elektronno-obchyslyuval′noyi tekhniky z urakhuvannyam yikh funktsionuvannya v umovakh informatsiynoho konfliktu" [A quantitative estimation protected level is taking into account functioning objects of electroncomputing devices in the conditions of informative conflict], *The journal of Zhytomyr state technological university. Series: engineering*, No. 3(46), pp. 113-120.
9. Buriachok, V.L. (2011), "Alhorytm otsiniuvannia stupenia zakhyshchenosti spetsialnykh informatsiino-telekomunikatsiinykh system" [The algorithm for estimating the security of special information-telecommunication systems], *Information security*, No. 3(52), pp. 19-27.
10. Il'yashov, O.A. and Buryachok, V.L. (2010), "Do pytannya zakhystu informatsiyno-telekomunikatsiynoyi sfery vid storonn′oho kibernetychnoho vplyvu" [Protection of the information and telecommunication sphere from external cybernetic invasion], *Science and Defense*, No. 4, pp. 35-40.
11. Potii, O.V. and Lienshyn, A.V. (2010), "Doslidzhennia metodiv otsinky ryzykiv bezpetsi informatsii ta rozrobka propozytsii z yikh vdoskonalennia na osnovi systemnoho pidkhodu" [Research of information security assessment methods and guidelines design about its improvement on the ground of system approach], *Scientific Works of Kharkiv National Air Force University*, No. 2(24), pp. 85-91.
12. Kozubtsov, I.M., Kozubtsova, L.M., Kutsayev, V.V. and Tereshchenko, T.P. (2018), "Metodyka otsinky kibernetychnoyi zakhyshchenosti systemy zv″yazku orhanizatsiyi" [Method of assessment of the cybernetic protection of the organization communication system], *Modern Information Technologies in the Sphere of Security and Defence*, No. 1(31), pp. 43-46.
13. The official site of KDD Cup 1999 Data (1999), *Data files*, available at: www.kdd.ics.uci.edu/databases/kddcup99/kddcup99.
14. Budkova, L.V. and Korniyenko, V.I. (2013), "Kompleksna otsinka kharakterystyk ta identyfikatsiya trafiku v informatsiynykh telekomunikatsiynykh merezhakh" [Complex estimation of characteristics and traffic identification in information telecommunication networks], *Information Processing Systems*, No. 2(109), pp. 207-211.
15. Herasina, O.V. (2018), "Metodyka intelektualnoi identyfikatsii ta prohnozuvannia trafiku v informatsiinykh telekomunikatsiinykh merezhakh" [Method of intellectual identification and prediction of traffic in information telecommunication networks], *Information Processing Systems*, No. 1(152), pp. 94-99. https://doi.org/10.30748/soi.2018.152.14.
16. Storchak, A.S. (2013), "Metod otsinky zakhyshchenosti informatsiyi na osnovi bahatokrokovykh protsesiv pryynyattya rishen′" [Method of secured information assessment based on multistage decision-making processes], *Eastern-European Journal of Enterprise Technologies*, No. 6(12), pp. 82-85.

Надійшла до редколегії 16.08.2019
Схвалена до друку 10.09.2019

Відомості про авторів:

Сторчак Антон Сергійович
старший викладач Інституту спеціального зв'язку
та захисту інформації Національного технічного
університету України "Київський політехнічний інститут
ім. І. Сікорського",
Київ, Україна
https://orcid.org/0000-0002-5267-3122

Information about the authors:

Anton Storchak
Senior Instructor of Institute
of Special Communications and Information Protection
of National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute",
Kyiv, Ukraine
https://orcid.org/0000-0002-5267-3122

Сальник Сергій Васильович
кандидат технічних наук
заступник завідувача кафедри
Інституту спеціального зв'язку та захисту інформації
Національного технічного університету України
"Київський політехнічний інститут
ім. І. Сікорського",
Київ, Україна
https://orcid.org/0000-0003-4463-5705

Sergey Salnyk
Candidate of Technical Sciences
Deputy Head of the Department
of Institute of Special Communications
and Information Protection
of National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute",
Kyiv, Ukraine
http://orcid.org/0000-0003-4463-5705

МЕТОД ОЦЕНКИ УРОВНЯ ЗАЩИЩЕННОСТИ СЕТЕВОЙ ЧАСТИ КОММУНИКАЦИОННОЙ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ ОТ КИБЕРУГРОЗ

А.С. Сторчак, С.В. Сальник

В статье представлен усовершенствованный метод оценки уровня защищенности сетевой части коммуникационной системы специального назначения от киберугроз на основе алгоритма распределительной идентификации и динамического программирования. Одной из составляющих систем обеспечения безопасности коммуникационных систем является подсистема оценки уровня защищенности, которая предназначена для определения эффективности применяемых средств защиты. Целью работы является разработка метода оценки защищенности информации, обрабатываемой в коммуникационной системе, на основе управляемых многошаговых процессов принятия решений, для повышения эффективности управления защитой информации, учитывая характеристики процесса защиты. Определена величина риска на каждом этапе процесса защиты и определены правила выбора средств защиты, которые минимизируют значение рисков на всех этапах. Процесс оценки защиты коммуникационных систем и процесс применения средств защиты реализуются по этапам. На каждом этапе получена совокупность данных о состоянии защищенности системы, которая зависит от реализованных услуг безопасности, характеризует систему обеспечения безопасности и влияет на выбор используемых защитных механизмов. Определены векторы процесса оценки защищенности и процесса реализации средств защиты, которые обеспечивают минимизацию значения рисков на всех этапах функционирования системы защиты. Суть метода заключается в оценке уровня защищенности коммуникационных систем с использованием распределённой идентификации параметров кибератак, выбора мер защиты системы при полном статистическом описании коммуникационной системы и с учетом стратегий воздействия злоумышленника на нее на основе динамического программирования. Получены рекуррентные соотношения и правило использования средств защиты, которые определяют порядок выбора оптимальных защитных механизмов и является основой для поиска оптимальных или близких к ним алгоритмов использования средств защиты при априорной неопределенности. Они позволяют определить степень защищенности коммуникационных систем на основе исследования изменений её характеристик.

Ключевые слова: *киберугрозы, системы специального назначения, защищенность, метод оценки, коммуникационная система.*

EVALUATION METHOD OF NETWORK PART SECURITY LEVEL IN THE COMMUNICATION SYSTEMS FOR SPECIAL PURPOSES AGAINST CYBER THREATS

A. Storchak, S. Salnyk

The article presents an improved method for assessing the level of security of the network part of a special-purpose communication system from cyber threats based on the distribution identification algorithm and dynamic programming. One of the components of security systems for communication systems is a subsystem for assessing the level of security, which is designed to determine the effectiveness of the applied protection. The aim of the work is to develop a method for assessing the security of information processed in a communication system, based on managed multi-step decision-making processes, to increase the effectiveness of information security management, taking into account the characteristics of the protection process. The amount of risk at each stage of the protection process is determined and the rule for the selection of protective equipment that minimizes the risk at all stages is defined. The process of assessing the protection of communication systems and the process of applying protective equipment are implemented in stages. At each stage, a set of data on the security status of the system is obtained, which depends on the implemented security services, characterizes the security system and affects the choice of protective mechanisms. The vectors of the process of assessing security and the process of implementing protective equipment are determined that ensure minimization of the significance of risks at all stages of the functioning of the protection system. The essence of the method is to assess the level of security of communication systems using distributed identification of the parameters of cyberattacks, select measures to protect the system with a complete statistical description of the communication system and taking into account the strategies for the attacker to influence it based on dynamic programming. The recurrence relations and the rule of using protective equipment are obtained, which determine the procedure for choosing the optimal protective mechanisms and are the basis for searching for optimal or close algorithms for using protective equipment with a priori uncertainty. They allow you to determine the degree of security of communication systems based on the study of changes in its characteristics.

Keywords: *cyber threats, special purpose systems, security, evaluation method, communication system.*