МЕТОД ПІДВИЩЕННЯ ІНФОРМАТИВНОСТІ ДОСЛІДЖЕННЯ IP ПРОТОКОЛІВ КОМП'ЮТЕРНИХ МЕРЕЖ ЗА КРИТЕРІЯМИ БЕЗПЕКИ

УДК 004.3(075)

ВЕСЕЛОВСКАЯ Галина Викторовна
кандидат технических наук, доцент кафедры информационных технологий, доцент, кафедра информационных технологий факультета кибернетики и системной инженерии Херсонского национального технического университета,
Научные интересы: технологии повышения эффективности компьютерных систем и сетей.
E-mail: galina.veselovskaya@gmail.com

БАРАНЕНКО Роман Васильевич
кандидат технических наук, доцент кафедры информационных технологий, доцент, кафедра информационных технологий факультета кибернетики и системной инженерии Херсонского национального технического университета
Научные интересы: технологии повышения эффективности компьютерных систем и сетей.
E-mail: scrooger@yandex.ru.

ДЕРЕВЯНКО Євгений Иванович
студент магистратуры по специальности 8.05010201 "Компьютерные системы и сети"
кафедра информационных технологий факультета кибернетики и системной инженерии
Херсонского национального технического университета.
Научные интересы: технологии повышения эффективности компьютерных систем и сетей.

ВСТУП

На даний час, усе більш важливу роль відіграє безпека комп'ютерних систем і мереж, а також великого спектру мережних інформаційних систем, які функціонують на їх основі, що обумовлено рядом об'єктивних факторів.

У першу чергу, слід відзначити, що неналежне дотримання вимог безпеки, як правило, призводить до суттєвого порушення нормального режиму роботи підприємств та організацій і до значних збитків, які є незрівняно вищими за витрати на ефективні системи захисту.

До того ж, наслідки успішно реалізованих несанкціонованих дій зловмисників достатньо нерідко виявляються непоправними, призводячи не тільки до фактичного знищення комп'ютерної програмної та апаратної бази, спотворення та втрати критично важливої інформації, а й до краху підприємств та організацій у цілому.

Існування численних фундаментальних теоретичних і практичних рішень у галузі безпеки не знімає з розгляду означену вище проблему.

Наявність цілого ряду уразливостей сучасних технологій захисту та постійне напрацьовування зловмисниками нових технологій здійснення несанкціонованих дій, роблять високоактуальною подальшу активну роботу за зазначеним питанням, у рамках якого здійснювалися й дослідження та розробки даної публікації.

ПОСТАНОВКА ЗАДАЧІ

Одне з чільних місць у галузі забезпечення безпеки посідає безпечність протоколів комп'ютерних мереж і, зокрема, IP протоколу, який на даний час за фактом не є

достатньо захищеним, у цілому ряді випадків достатньо легко підпадаючи під дію різноманітних загроз.

Відповідно, актуальним є як вивчення витоків та особливостей уразливості IP протоколу комп'ютерних мереж, так і розробка методів і засобів для своєчасного передбачення відповідних несанкціонованих дій, а також належної протидії їм.

Особливо актуальними є ті методи, що дозволяють, за умови мінімальних додаткових витрат, встановлювати максимально можливі захисні бар'єри на шляху потенційних загроз безпеці на рівні IP протоколу комп'ютерних мереж.

Дослідженню та розробці одного з зазначених методів і присвячено дану статтю.

Зокрема, основну увагу акцентовано на аспекті застосування критеріїв безпеки як одному з потенційно найефективніших механізмів попереднього прогнозування та фактичного затвердження певного рівня безпечності IP протоколу комп'ютерних мереж.

РОЗВ'ЯЗОК ЗАДАЧІ

В основу вирішення поставленої проблеми, у першу чергу було покладено аналіз визначальних особливостей протоколу IP (Internet Protocol), який посідає одне з чільних місць у стеку (сімействі) протоколів комп'ютерних мереж TCP/IP, належачи до третього (мережного) рівня моделі взаємодії відкритих систем OSI та безпосередньо відповідаючи за міжмережну взаємодію.

Слід відзначити, що IP протокол комп'ютерних мереж, який було створено у шести послідовних версіях, від IPv1 до IPv6, на даний час характеризується наявністю лише двох реально діючих версій, якими є версії IPv4 та Ipv6 (інші перелічені версії належать до категорій не застосовуваних на практиці та теоретично-експериментальних розробок).

IP протокол версії IPv4 вирізняється тим, що є достатньо давно впровадженим, дуже поширеним та усталеним на практиці, але має суттєве обмеження за можливими розмірами побудованих із його застосуванням комп'ютерних мереж через недостатню довжину IP адреси, що може бути поставлена у відповідність кожному вузлу комп'ютерної мережі.

На відміну від нього, IP протокол версії IPv6 є порівняно новим і поступово, але неухильно, впроваджується до експлуатації, переважаючи тим, що дозволяє суттєво збільшувати масштаби реалізованих на його основі комп'ютерних мереж завдяки наданню ним можливостей IP адресації значно більшої кількості мережних вузлів.

Також IP протокол комп'ютерних мереж характеризується наявністю різноманітних можливостей апаратної та програмної реалізації (з набагато переважаючою роллю якості програмної реалізації зазначеного протоколу).

Указані реалізації у підсумку визначають реальну ефективність IP протоколу комп'ютерних мереж у конкретних умовах його застосування та для певних об'єктів захисту.

Виходячи з наявності декількох діючих версій IP протоколу комп'ютерних мереж, які характеризуються різною логікою роботи, а також із можливостей отримання різноманітних реалізацій зазначеного протоколу, кожна з яких буде мати свої специфічні особливості, надалі будемо віддавати перевагу застосуванню терміну IP протоколу комп'ютерних мереж у множинному числі, використовуючи для наочності більш коротке словосполучення "IP протоколи".

Показовим є те, що IP протоколам властивий цілий ряд визначальних переваг, які у першу чергу стосуються підвищеного обсягу та швидкості передачі даних, уніфікованості мережної інфраструктури, широти можливостей вибору обладнання тощо.

Саме завдяки зазначеним перевагам IP протоколів, набули широкого розповсюдження, активного практичного застосування та чудових перспектив подальшого розвитку найрізноманітніші IP мережі, основною з яких є глобальна комп'ютерна мережа Інтернет.

Разом із тим, IP протоколи вирізняються тією специфічною та дуже проблемною особливістю, що, згідно з початковою концепцією їх створення, вони не мали жодних власних (убудованих) механізмів забезпечення безпеки.

Через зазначену особливість, у разі використання IP протоколів, було можливим і зовсім нескладним перехоплення IP пакетів, наступне здійснення їх аналізу та несанкціонованого використання наявної у них інформації, а також їх спотворення (змінювання, фальсифікація та т.і.) або знищення.

Відповідно, з самого початку свого створення та подальшого розвитку, IP протоколи потребували застосування додаткових розвинених засобів і методів забезпечення їх безпеки, а саме:

— додаткових протоколів стеку протоколів TCP/IP (таких, як, наприклад, захищений протокол транспортного рівня

передачі даних IPSec, який початково був призначений для доповнення можливостей IP протоколу версії IPv6);

— додаткових організаційних, математичних, алгоритмічних, апаратних, програмних, апаратно-програмних технологічних рішень тощо.

Слід відзначити, що, протягом певного часу історії розвитку IP протоколів, було напрацьовано багато достатньо ефективних та усталених на практиці методів і засобів забезпечення безпеки зазначених протоколів.

Основу указаних методів і засобів традиційно складають класичні технології криптографії та різноманітні поєднання методів шифрування.

Разом із тим, останнім часом було також напрацьовано численні нові прогресивні концепції забезпечення безпеки IP протоколів.

Каталізатором їх активного створення стала не дуже втішна статистика, пов'язана як із інтенсивною розробкою нових мережних загроз, так і з реальним існуванням великої кількості потенційно можливих, реально здійснюваних та успішно реалізованих несанкціонованих дій, підгрунтям появи яких став недостатній рівень безпечності IP протоколів.

Слід відзначити, що, на фоні суттєвого обсягу та досягненого рівня якості нових високоефективних розробок, залишився також цілий ряд ще невирішених важливих проблем забезпечення безпеки IP протоколів.

Наприклад, свої суттєві корективи продовжує вносити такий специфічний і дуже потужний фактор уразливості систем безпеки, спрямованих на захист IP протоколів, як людський фактор, який є одним із найпровокаційніших, найнебезпечніших і найнекерованіших чинників виникнення ситуацій порушення безпеки.

Відповідно, важливу роль мають відігравати ті організаційні заходи, методи та моделі, що дозволяють ураховувати людський фактор, але їм продовжується приділятися неналежно мало уваги (в основному, через високу складність їх дослідження та розробки).

Зрозуміло, що, у зазначеній ситуації, коли існуючі методи та засоби забезпечення безпеки виявляються недостатньо дієвими, вкрай важливу роль відіграє розробка ще досконаліших технологій забезпечення безпеки IP протоколів.

Але, в очікуванні результатів створення нових засобів і методів забезпечення безпеки, втрачається певний і достатньо суттєвий час.

Відповідно, не менш визначального значення набуває максимально ефективне застосування існуючих технологій забезпечення безпеки IP протоколів, якнайповніше використання спектру та потужності їх можливостей.

У зв'язку з вище сказаним, стає надзвичайно актуальною задача знаходження резервів для отримання наступних результатів:

— виявлення найбільш оптимальних умов і підходів до застосування кожної окремо взятої з існуючих технологій забезпеченя безпеки IP протоколів;

— максимально вдалого вибору й інтеграції ряду окремих технологій забезпечення безпеки IP протоколів в єдиний високоефективний комплекс відповідно до специфіки конкретних умов та об'єктів захисту.

У цілому, постає задача найдоцільнішого та, відповідно, найпродуктивнішого використання можливостей не тільки давно існуючих, а й нещодавно створених технологій забезпечення безпеки, що, як правило, здатні рухати рівень безпеки стрімко вгору.

Натомість на практиці часто спрацьовує інерційність процесів поширення інформації про найсучасніші технології забезпечення безпеки, навчання ним та їх упровадження (як у цілому, так і, зокрема, щодо IP протоколів), що достатньо важко піддається прискорюючим впливам.

Не можуть стати дієвим важелем для подолання зазначеної інерційності і загальноприйняті системи формалізованих нормативних і додаткових критеріїв оцінювання безпечності систем захисту в цілому та, зокрема, мережних протоколів.

Проаналізуємо основні витоки сформульованої вище думки.

Критерії, що належать до категорії основних (нормативних, формалізованих, узагальнених) критеріїв безпеки, визначаються наступними характерними особливостями:

— є регламентованими (визначеними) нормативними документами організацій міжнародного, міждержавного (у рамках спільнот країн, таких як, наприклад, європейські країни) та державного рівня, згідно з чим, мають достатньо високий рівень узагальненості;

— відзначаються суттєвою відпрацьованістю й усталеністю, але й відповідною повільною динамікою оновлення;

— призначені переважно для визначення рівня (категорії) безпеки комп'ютерних систем і мереж, інформаційних технологій тощо.

Визначальними прикладами критеріїв указаної вище категорії є наступні:

— формалізовані критерії безпеки, що містяться у нормативних документах міжнародних організацій зі стандартизації ISO/IEC;

— узгоджені критерії оцінки безпеки інформаційних технологій європейських країн ITSEC (Information Technology Security Evaluation Criteria);

— критерії оцінки надійних комп'ютерних систем Міністерства оборони США;

— Державні стандарти України, що встановлюють терміни, визначення й основні положення щодо технічного захисту інформації;

— нормативні документи технічного захисту інформації (НД ТЗІ) 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу", 1.1-002-99 "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу" та т.і., що є чинними в Україні;

— ряд державних нормативних документів України, що законодавчо затверджують певні критерії безпеки та механізми регулювання їх дотримання (Закони України "Про захист інформації в інформаційно-телекомунікаційних системах", "Про телекомунікації" та "Про інформацію"; Накази Президента України "Про Положення про технічний захист інформації в Україні" та "Про Положення про порядок здійснення криптографічного захисту інформації в Україні"; Постанова Кабінету Міністрів України "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомуникаційних системах" тощо).

Слід відзначити, що, на даний час, світовою й європейською спільнотою здійснюються активні дії (виконуються дослідження та розробки, проводяться наукові конференції та семінари, здійснюються обговорення серед різних соціальних верств тощо) з метою уніфікації й інтеграції нормативних критеріїв безпеки окремих країн до систем критеріїв безпеки комп'ютерних систем, мереж та інформаційних технологій міждержавного (зокрема, європейського) та міжнародного рівня.

Критерії, що належать до категорії додаткових (доповнюючих, конкретизованих, специфічних) критеріїв безпеки, характеризуються наступними особливостями, що визначають їх високі потенційні можливості:

— розробляються з метою доповнення (конкретизації, деталізації) формалізованих критеріїв безпеки на основі аналізу й урахування специфіки (та відповідної статистики) певних класів об'єктів захисту та несанкціонованих дій щодо них;

— мають бути динамічно оновлюваними;

— повинні надавати реальну можливість їх ефективного практичного застосування для створення безпечних комп'ютерних систем і мереж, інформаційних технологій.

Таким чином, головна проблема полягає у тому, що, в реально діючій практиці, існуючі на даний момент загальноприйняті формалізовані нормативні та додаткові системи критеріїв безпеки є дуже узагальненими та теж занадто інерційними в силу того, що з самого початку мали за визначальну мету встановлення факту належності систем забезпечення безпеки до одного з декількох формалізованих класів безпеки.

Відповідно, такі критерії не можуть надавати належної дієвості щодо сприяння побудові ефективних систем захисту для конкретних умов та об'єктів захисту, включаючи урахування статистики властивих їм потенційних загроз і реально здійснюваних несанкціонованих дій.

Зокрема, загальноприйняті додаткові критерії безпеки, як правило, формувалися стосовно великих узагальнених класів апаратного та програмного забезпечення, інформаційних систем, галузей їх практичного застосування та т.і., таких як операційні системи, бази даних, мережні сервіси, Web-додатки, банківські інформаційні системи, апаратно-програмні комплекси для опрацьовування суворо секретної та конфіденційної службової інформації тощо.

Певні шляхи вирішення означеної вище проблеми надає запропонований авторами підхід, суть якого полягає у розробці та впровадженні представлених далі двох взаємопов'язаних рішень.

Перше рішення полягає у синтезі додаткової системи критеріїв безпеки IP протоколів, які виконують роль індикаторів повноти (вичерпності) та комплексності застосування прогресивних технологій забезпечення безпеки зазначених протоколів.

Указані додаткові критерії мають спиратися на існуючі нормативні та загальноприйняті додаткові системи критеріїв і доповнювати їх, забезпечуючи можливість перевірки повноти застосування найсучасніших методів і засобів забезпечення безпеки IP протоколів у будь-яких конкретних умовах і системах захисту.

Друге рішення полягає у забезпеченні можливості динамічної оновлюваності набору зазначених додаткових критеріїв на основі експертних оцінок (ітеративно, у режимі реального часу, у тому числі — виходячи з поточної статистики потенційних і реальних загроз, із урахуванням специфіки конкретних умов та об'єктів захисту тощо).

Розширення існуючих класифікаційних систем критеріїв безпеки IP протоколів вище означеною додатковою динамічно оновлюваною системою критеріїв у першу чергу передбачає формування базового переліку критеріїв, концепцій отримання й опрацьовування значень критеріїв, підходів до подальшого розвитку множини критеріїв, а також до реалізації роботи з системою критеріїв засобами та методами сучасних інформаційних технологій.

Формування початкового варіанту зазначеного базового переліку додаткових критеріїв безпеки IP протоколів здійснювалося на основі текстологічних методів вилучення експертних знань.

У підсумку, було отримано наведені нижче результати (вихідні переліки критеріїв розширеної класифікації).

Початковий варіант базової множини додаткових критеріїв безпеки IP протоколів, підтримуваної на основі застосування прогресивних концепцій, методів і засобів моделювання, склали наступні визначальні компоненти:

— критерій комплексного застосування хостових, мережних і комбінованих методів аналізу безпеки IP протоколів;

— критерій застосування гнучких, адаптивних підходів до моделювання систем забезпечення безпеки IP протоколів;

— критерій застосування динамічних моделей забезпечення безпеки IP протоколів, які дозволяють ураховувати стан передісторії, поточну динаміку та прогнози стосовно тенденцій змінювання ситуації й об'єктів захисту, з задіянням відповідної статистики;

— критерій застосування інтелектуальних правил у процесі моделювання систем безпеки IP протоколів;

— критерій застосування методів забезпечення безпеки IP протоколів на основі теорії прийняття рішень;

— критерій застосування методів забезпечення безпеки IP протоколів на основі спеціалізованих графових моделей;

— критерій застосування методів забезпечення безпеки IP протоколів на основі мережних моделей (нейронних мереж, фреймових мереж, розфарбованих мереж Петрі тощо);

— критерій застосування методів моделювання конкретних типів атак із метою аналізу їх уразливостей, створення моделей їх передбачення та протидії їм.

Початковий варіант базової множини критеріїв безпеки IP протоколів, підтримуваної на основі застосування сучасного спеціалізованого програмного забезпечення, склали наступні провідні компоненти:

— критерій застосування сучасних мережних програм моніторингу стану безпеки, які належать до категорії IP сканерів;

— критерій застосування сучасних інтелектуальних брандмауерів.

За основу формування конкретних програмних реалізацій додаткових систем критеріїв-індикаторів повноти та комплексності застосування прогресивних технологій забезпечення безпеки IP протоколів, пропонується за найдоцільніше брати табличні форми, складовими елементами рядків яких є кортежі значень, які належать до трьох послідовних рівнів деталізованості.

Відповідні значення формуються на основі експертних оцінок, висловлюваних у лінгвістичній і числовій формі.

Кортежі першого рівня деталізованості містять в якості значень показники-прапорці факту реалізованості певних критеріїв безпеки IP протоколів у конкретній системі захисту, з відповідними двома альтернативними станами (0/1, +/- або т.і.).

Кортежі другого рівня деталізованості містять за значення узагальнені показники-коефіцієнти реалізованості певних критеріїв безпеки IP протоколів у конкретній системі захисту, представлені у лінгвістичній і нормованій дискретизованій інтервальній шкалі.

Кортежі третього рівня деталізованості містять вагові показники-коефіцієнти реалізованості певних критеріїв безпеки IP протоколів у конкретній системі захисту, що висловлюють рівні стану реалізованості у оцінках локальних критеріїв безпеки кожного з чотирьох глобальних критеріїв конфіденційності цілісності, доступності й імітостійкості.

У цілому, узагальнений склад кортежу значень критеріїв-індикаторів потенційно забезпечуваного рівня безпеки IP протоколів набуде наступного вигляду:

$$< \{t(i,j)\}, \{fl(i,j)\}, \{(nm1(i,j), nm2(i,j))\}, \{(cf1(i,j), cf2(i,j))\}, \{(sf1(i,j), sf2(i,j))\}, \{(ac1(i,j), ac2(i,j))\}, \quad (1)$$

{(im1(i,j), im2(i,j))}>,

де:

— i — порядкові номери певних груп додаткових критеріїв безпеки IP протоколів;

— j — порядкові номери конкретних критеріїв усередині вказаних вище груп;

— t(i,j) — найменування додаткових критеріїв безпеки IP протоколів, які відповідають певним прогресивним технологіям, які мають застосовуватися з метою реалізації вичерпно повних і комплексних підходів;

— fl(i,j), nm1(i,j), nm2(i,j), cf1(i,j), cf2(i,j), sf1(i,j), sf2(i,j), ac1(i,j), ac2(i,j), im1(i,j), im2(i,j) — різні (стосовно інформативності та одиниць вимірювання) міри реалізованості додаткових критеріїв безпеки IP протоколів у конкретних умовах і в конкретних системах захисту;

— fl(i,j) є {0,1} — факт реалізованості (повної чи часткової) або нереалізованості критерію безпеки IP протоколів t(i,j);

— (nm1(i,j), nm2(i,j)) — узагальнена міра реалізованості критерію безпеки IP протоколів t(i,j), яка містить лінгвістичну експертну оцінку nm1(i,j) та відповідну числову оцінку nm2(i,j);

— (cf1(i,j), cf2(i,j)), (sf1(i,j), sf2(i,j)), (ac1(i,j), ac2(i,j)), (im1(i,j), im2(i,j)) — міри реалізованості глобальних критеріїв конфіденційності, цілісності, доступності й імітостійкості, забезпечувані за рахунок дотримання певного додаткового критерію безпеки IP протоколів t(i,j), які містять відповідні лінгвістичні та числові експертні оцінки.

Передбачається ведення бази знань та експертної системи на основі фактів та інтелектуальних правил-продукцій щодо умов і методів застосування нової системи критеріїв безпеки IP протоколів комп'ютерних мереж.

Базовий модуль інформаційної системи для дослідження IP протоколів комп'ютерних мереж за критеріями безпеки пропонується у форматі Web-додатку.

Передбачаються розвинені можливості здійснення зворотних зв'язків зазначеного базового модулю з користувачами, збирання й аналізу статистики взаємодії (у тому числі, можливості вільного поповнення системи інформацією, наступним аналізом її засобами експертної системи та відповідним поповненням бази знань).

ОСНОВНІ РЕЗУЛЬТАТИ ТА ВИСНОВКИ

Запропоновано новий актуальний метод формування додаткової системи критеріїв безпеки IP протоколів комп'ютерних мереж, який базується на застосуванні гнучкого динамічного підходу та сучасних інформаційних технологій.

Застосування вказаного методу дозволяє підвищити інформативність дослідження безпечності IP протоколів комп'ютерних мереж.

ЛІТЕРАТУРА:

1. Shangin V.F. Informatsionnaya bezopasnost kompyuternyih sistem i setey: Uchebnoe posobie / V.F. Shangin. — M.: ID FORUM, NITs INFRA-M, 2013. — 416 s.
2. Partyika T.L. Informatsionnaya bezopasnost: Uchebnoe posobie / T.L. Partyika, I.I. Popov. — M.: Forum, 2012. — 432 s.
3. Petrov S.V. Informatsionnaya bezopasnost: Uchebnoe posobie / S.V. Petrov, I.P. Slinkova, V.V. Gafner. — M.: ARTA, 2012. — 296 s.
4. Kupriyanov A.O. Obespechenie zaschityi personalnyih dannyih v informatsionnyih sistemah // Program. inzheneriya i inform. bezopasnost. – 2013. – № 4. – S. 27-34.
5. Malyuk A.A. Perspektivyi razvitiya "oblachnyih" tehnologiy. Informatsionnaya bezopasnost i zaschita personalnyih dannyih v "oblachnoy" srede // Vestn. Nats. issledovat. yader. un-ta "MIFI". – 2013. – T. 2, № 1. – S. 120-124.
6. Prokushev Ya.E. Sravnitelnyiy analiz sredstv programmno-apparatnoy zaschityi informatsii, primenyaemyih v informatsionnyih sistemah personalnyih dannyih / Ya.E. Prokushev, S.V. Ponomarenko // Informatsiya i bezopasnost. – 2012. – T. 15, № 1. – S. 31-36.
7. Razrabotka avtomatizirovannoy sistemyi otsenki zaschischennosti i formirovaniya rekomendatsiy po vyiboru sredstv zaschityi informatsionnyih sistem personalnyih dannyih / V.I. Averchenkov, M.Yu. Ryitov, O.M. Golembiovskaya, E.V. Leksikov // Vestn. kompyuter. i inform. tehnologiy. – 2012. – № 11. – S. 40-45.
8. Babash A.V. Informatsionnaya bezopasnost. Laboratornyiy praktikum: Uchebnoe posobie / A.V. Babash, E.K., Baranova, Yu.N. Melnikov. – M.: KnoRus, 2013. – 136 s.
9. Gromov Yu.Yu. Informatsionnaya bezopasnost i zaschita informatsii: Uchebnoe posobie / Yu.Yu. Gromov, V.O. Drachev, O.G. Ivanova. – St. Oskol: TNT, 2010. – 384 s.
10. Semenenko V.A. Informatsionnaya bezopasnost: Uchebnoe posobie / V.A. Semenenko. – M.: MGIU, 2010. – 277 s.