ТЕХНІЧНІ НАУКИ

УДК 004.9

ЗАСОБИ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ

Б. В. Дурняк, Т. М. Майба

Українська академія друкарства
вул. Підголоско, 19, Львів, 79020, Україна

Розглянуто засоби захисту комп'ютерних мереж з таких поглядів: стандартів захисту інформаційних систем, вибраних вимог до забезпечення процесу функціонування, а також забезпечення певного рівня захисту ІТ, який визначається інтегральним параметром. Висвітлено вплив технологічних процесів на можливість побудови системи управління на прикладі поліграфічних технологічних процесів.

Ключові слова: *стандарти безпеки інформативних систем, засоби захисту, атаки, небезпека.*

Задачі захисту комп'ютерних мереж досліджуються досить широко. Оскільки проблеми захисту інформаційних мереж є актуальними для довільних випадків їх використання, то відомі методи захисту можна розглядати з таких поглядів:

– стандартів захисту інформаційних систем, які сукупно з прикладними задачами розглядаються як інформаційні технології (*ІТ*);
– вибраних вимог до забезпечення процесу функціонування *ІТ*;
– забезпечення певного рівня захисту *ІТ*, який визначається деяким вибраним інтегральним параметром.

Основною ціллю будь-яких стандартів, зокрема стандартів захисту інформації, є уніфікація, якщо можливо, більшості задач, які виникають під час розв'язування задач захисту інформаційних систем або *ІТ* загалом. Тому стандарти переважно описують вимоги до організації системи *ІТ* в загальному вигляді. В цьому випадку значення методу стандартизації мають загальний характер і окремі способи реалізації процесів захисту від тих чи інших атак можуть бути різними. Це зумовлено тим, що під стандартизацію потрапляє не так спосіб захисту, як можливість зберегти захист, який вимагається відповідно до стандарту [1].

Стандарти, розроблені для визначення норм та вимог до захисту, не можуть враховувати всі можливі випадки порушень безпеки окремої *ІТ* системи. Безпека окремої системи може залежати від різних факторів, які безпосередньо в системі стандартів можуть не наводитися. Прикладом таких факторів є певні особливості функціонування системи *ІТ*, параметри системи, які не мають безпосереднього стосунку до безпеки, та інші. Наприклад, важливим параметром *ІТ* системи є її розміри. Отже, використовувати засоби захисту для забезпечення необхідного рівня безпеки, які співрозмірні з самою системою, не доцільно. Іншим прикладом фактора може бути вимога до системи, яка полягає у тому, щоб система *ІТ* працювала в режимі реального часу функціонування процесу розв'язання прикладної задачі, для якої розроблена *ІТ*. Це означає, що використовувати засоби захисту, які призведуть до недопустимого зниження швидкості

функціонування *IT* системи, є неприйнятно. Отже, відомі, або стандартні, засоби захисту, які орієнтовані на протидію певним атакам — неприпустимі. Прикладом таких стандартних засобів можуть бути різні типи пакетних фільтрів, відомі під назвою *firewall.*

Оскільки стандарти безпеки *IT* повинні бути, з одного боку, достатньо загальними, а з другого — конструктивними, то як опис міри безпеки використовується не якийсь окремий параметр, а конструкція, яка залежно від повноти може відповідати різним значенням, наприклад, параметру безпеки. Однією з конструкцій, які використовують у системі стандартів, є уявлення про профіль безпеки. Опис профілю безпеки передбачає наявність ряду даних, які безпосередньо стосуються проблем захисту. Такими відомостями є опис вимог для забезпечення безпеки функціонування обраного об'єкта. Прикладом таких вимог є вимоги до функціональної безпеки, до адекватності, до середовища *IT* та інші. Найширше використовують вимоги до функціональної безпеки, оскільки вони належать до тих, які гарантують необхідний спосіб функціонування *IT*. Вимоги до адекватності передбачають необхідність використання певних типів засобів при реалізації системи *IT*. Це означає, що система *IT*, в якій закладалась певна операційна система (ОС), повинна працювати лише з цією системою, і недопустимо з погляду забезпечення певного рівня безпеки використовувати іншу операційну систему, незважаючи на те, що вона за основними параметрами може бути ідентичною до попередньої. Такі вимоги до системи *IT* називаються класами безпеки. Кожний з цих класів безпеки визначається методами реалізації, а стандарти безпеки в межах одного класу описують безліч засобів, які є описами процесів функціонування відповідного засобу. Наприклад: системи ідентифікації й аутентифікації доступу до системи — засіб, який забезпечує захист інформаційного каналу обміну, що реалізується в межах *IT*, від перехоплення даних, що по ньому передаються і т. д. [3–4].

З викладеного не зрозуміло, як забезпечувати повноту опису певного класу безпеки для окремої обраної системи. Для розв'язання цієї задачі в межах стандартів безпеки *IT* використовують профілі безпеки. Кожен тип *IT*, залежно від типу прикладної задачі, яка реалізується в системі, має свій тип профілю безпеки, який позначається Pr_i. Кожен профіль містить певні класи безпеки, а кожен клас безпеки відповідного профілю — описи певних вимог до засобів захисту. Наприклад, для профілю Pr_i клас функціональної безпеки може містити засоби ідентифікації та не містити засобів аутентифікації (профіль *IT* системи, зорієнтованої на обслуговування бібліотеки). Клас адекватності *IT* системи у відповідному Pr_i може не містити вимог щодо використання лише певної версії ОС, а це означає, що у такій системі *IT* можна переходити від Windows-7 до Windows-10 і т. д.

Використання стандартів безпеки *IT* системи є обов'язковими для довільної системи промислового значення. Це означає, що будь-яка інформаційна керівна система має проектуватися із дотриманням вимог безпеки. Такі вимоги

полягають у необхідності розроблення проекту безпеки відповідної системи. Основним елементом проекту безпеки є профіль безпеки. Ці вимоги не означають, що треба щоразу формувати окремий профіль для системи, яка проектується. Профіль безпеки можна вибрати з бібліотеки профілів безпеки, які уже були розроблені для системи відповідного типу та підтвердили на практиці здатність забезпечувати певний рівень безпеки. Зрозуміло, що в кожному окремому випадку профіль безпеки може модифікуватися у зв'язку з потребою враховувати певні особливості конкретної системи, які визначаються відповідною предметною галуззю, в якій розв'язують задачу. Наприклад, для *IT* системи, яка обслуговує бібліотеку раритетних видань, профіль безпеки повинен містити багаторівневу систему аутентифікації порівняно з відповідним профілем безпеки *IT*, що обслуговує студентську бібліотеку і т. д.

Стандарти безпеки *IT* систем, які формуються у вигляді міжнародних документів, орієнтовані на виконання насамперед окремих завдань:

– стандартизації систем захисту, які використовуються для забезпечення безпеки функціонування інформаційних систем різного типу;
– усунення необхідності щоразу будувати систему безпеки, проектувати засоби захисту, які були б аналогічними до вже наявних;
– розвитку окремих засобів захисту, що забезпечує збільшення рівня безпеки щодо атак, на які їх орієнтовано;
– завдання юридичного характеру, тобто призначення осіб, відповідальних за безпеку *IT* у разі виникнення раніше невідомих атак.

Використання стандартів безпеки інформаційних систем для забезпечення потрібного рівня безпеки системи *IT* не достатньо. У більшості випадків необхідно використовувати нові можливості захисту *IT* систем в межах вимог, сформульованих у стандартах безпеки *IT*, апелюючи тільки до індивідуальних вимог кожної системи. Така потреба зумовлена низкою чинників, а саме:

– особливостями функціонування інформаційної системи управління, що зумовлено специфікою відповідних технологічних процесів;
– специфікою небезпек, які існують щодо окремого технологічного процесу і полягають у тому, що кожна небезпека може активізувати атаки, на протидію яким не орієнтовано засоби захисту;
– об'єктивними можливостями, які визначають реалізацію засобів захисту та способи реалізації технологічного процесу загалом.

Очевидно, що можливості певного технологічного процесу значною мірою впливають на можливості побудови системи управління. Особливо це характерно для поліграфічних технологічних процесів, в яких можуть використовуватися окремі технологічні установки з різним рівнем можливостей їх автоматизації та об'єднання окремих установок в єдину автоматизовану технологічну лінію виробництва, зумовлену тим, що реалізація друкарського технологічного процесу передбачає наявність фрагментів, які значно відрізняються, а саме:

– складністю реалізації окремого фрагмента технологічного поліграфічного процесу;
– мірою впливу на параметри кінцевого продукту різних фрагментів технологічного процесу;
– суттєвою різницею у вартості окремих фрагментів технологічного процесу.

Прикладом першого випадку може бути порівняння друкарської машини з установками брошурування, обрізки та формування блоку книжки, якщо остання є продуктом, який виробляється в межах усього технологічного процесу. Очевидно, що параметри продукції, які забезпечуються складнішими фрагментами технологічного процесу, більше впливають на кінцеві параметри продукту порівняно з параметрами, які забезпечуються менш складними технологічними процесами. Прикладом може бути складний фрагмент друкарської машини та різальна машина. Зрозуміло, що ключовим параметром є параметр друку, а не лише якість нарізання листів чи блоків книг. Якщо порівнювати вартість друкарської машини з пристроями друкарської підготовки, то, очевидно, є різниця у вартості відповідних пристроїв. Наведені приклади визначають особливості, які впливають на організацію та проектування інформаційної системи керування. Якщо друкарська машина може бути повністю автоматизованою, зокрема підготованою до реалізації друку, то машина формування блоку, якщо вона не забезпечує можливості автоматизувати свої процеси, для об'єднання її в єдиний технологічний процес з друкарською машиною потребує залучення до технологічного процесу персоналу обслуги. Це не впливає на реалізацію загальної керівної системи не тільки з погляду автоматизації процесу, а й з погляду забезпечення певного рівня безпеки інформаційної системи керування технологічним процесом.

Наведений фактор можна використати для ілюстрації особливостей або специфіки небезпек, які виникають щодо інформаційної керівної системи. Така небезпека являє собою людський фактор і може активізуватися безпосередньо працівником.

Ще один випадок, що зумовлює специфічну небезпеку, полягає у тому, що простіші технологічні засоби автоматизації, наприклад механічні, значно складніше поєднати з електродинамічними засобами керування іншої установки. Прикладом може слугувати використання механічного перемикача в одному пристрої з електронним перемикачем — в іншому.

Один з головних підходів до забезпечення заданого рівня безпеки системи *IT* полягає у декларуванні певного рівня безпеки на основі використання деякої оцінки та методів реалізації, що можуть забезпечити відповідний рівень. За допомогою цього підходу розв'язують такі задачі:

– вибір типу оцінки рівня безпеки, яка повинна бути обґрунтованою для системи;
– вибір засобів захисту системи від можливих атак, що передбачає необхідність аналізувати небезпеки, загрози та можливі типи атак;

– встановлення зв'язку між засобами захисту нформаційної системи та оцінкою рівня її безпеки, яка була вибрана на першому етапі;
– розробка та дослідження методів визначення рівня безпеки, що залежить від відповідних засобів захисту.

Перш ніж розглядати окреслені задачі, зауважимо, що всі вони можуть бути узгоджені з вимогами та нормами стандартів безпеки, про які йшлося. Вибір засобів захисту й оцінка вкладу кожного з них може пов'язуватися з особливостями та вимогами предметної галузі, що в ній реалізується технологічний процес, для якого будується відповідна керівна інформаційна система.

Відомими інтегральними оцінками, які використовують для визначення рівня безпеки функціонування *IT*, є такі уявлення про безпеку, кожне з яких має власну інтерпретацію:

– рівень захищеності *IT*;
– рівень безпеки *IT*;
– рівень ризику функціонування *IT* та інші.

Рівень захищеності, який будемо позначати *RZ*, має власну інтерпретацію, яка полягає у тому, що поняття захищеності пов'язане з атаками на *IT*, від яких *IT* повинна захищатися системою безпеки *SB*. Це означає, що *R(IT)* ґрунтується на даних про відомі атаки A_i, які можуть активізуватися щодо *IT*. У цьому випадку за допомогою відомих атак визначаються методи протидії, а на основі їх аналізу вибираються або формуються необхідні засоби захисту. Розв'язання такої задачі ґрунтується на:

– виборі однакових фрагментів послідовності реалізації різного типу атак;
– елімінації загроз, які використовують декілька атак і при їх впровадженні в середовище *IT*, що здійснюється за допомогою активізації атак відповідними небезпеками;
– скеруванні атак на об'єкти, які моделюють об'єкт атаки і протидіють негативному впливу на атакований об'єкт.

Оскільки кожна атака At_i складається з низки подій, які відбуваються в середовищі *IT*, то може виникнути ситуація, коли дві різні атаки At_i і At_j мають однакові фрагменти, або:

$$At_i \cap At_j = \{(at_{ik} = at_{jr})*(at_{i(k+1)} = at_{j,(k+1)})*...*(at_{j,(k+1)}) = at_{j,(r+q)}\}.$$

У цьому випадку необхідно реалізувати протидію виділеним фрагментам, що призведе до дезактивації атак At_i і At_j.

Відомо, що будь-яка атака, щоб активізуватися в середовищі *IT*, повинна використовувати слабке місце в *IT*, або загрозу, що існує в *IT*, за допомогою якої атака може здійснити проникнення в *IT* і реалізувати свої функції. Відомо, що тією самою загрозою можуть скористатись інші атаки, а тому в разі ліквідації загрози засобами *SB* є можливість їм протидіяти.

Скеровування активізованих атак на моделі об'єктів, які, очевидно, моделюють об'єкт тільки частково або моделюють *IT* лише в межах поточних даних про об'єкт, які відомі атакам, являє собою окремий напрям, що стосується створення примарних об'єктів *IT* в системі *SB*.

Для реалізації описаних підходів здійснення протидії атакам необхідно розв'язати такі задачі в межах *SB*:

– виявлення факту виникнення атаки At_i;
– розпізнавання типу атаки At_i;
– вибір засобу захисту, що відповідає розпізнаній атаці, та його активізація;
– визначення результатів засобу захисту на атаку.

Виявлення факту виникнення атаки може ґрунтуватися на аналізі змін у *IT*, зумовлених атакою At_i, або на основі аналізу моніторингу небезпек, які мають місце в *IT*. При проектуванні довільної системи *IT* інформація про загрози Zg_i або слабкі місця здебільшого є доступною. Це можливо тому, що Zg_i — свідомо залишені в *IT* як фрагменти, які з різних причин не могли бути усунені. Найпоширенішою причиною виникнення в *IT* загроз Zg_i є необхідність мінімізувати можливі надмірності в IT_i. Оскільки, згідно з визначенням, відомими є можливі атаки, то існує можливість визначитися з алгоритмом взаємодії відповідного процесу активізації атаки із загрозою Zg_i. Якщо Zg_i, виходячи з можливостей фрагмента реалізації *IT*, який вміщує *Zg*, може взаємодіяти з рядом At_i, то при проектуванні *IT* такого типу Zg_i елімінується. Якщо наведена умова не виконується, то відповідна Zg_i залишається в межах *IT*. Очевидно, що фрагмент *IT* може ідентифікуватися як окрема Zg_i тільки в тому випадку, коли на етапі проектування *IT* є відомими атаки At_i, які використовуватимуть відповідну загрозу. Такий підхід дає можливість розв'язувати задачу розпізнавання факту активізації атаки At_i за допомогою моніторування відомих Zg_i в *IT* з метою виявлення в Zg_i змін або аномалій, зумовлених атакою At_i. Оскільки загроза Zg_i може використовуватися атаками At_i,..., At_{in}, то залишиться задача розпізнавання атак.

Розпізнавання атак здійснюється кількома етапами:

– розпізнавання групи атак, що використовують ту саму загрозу Zg_i;
– розпізнавання підгрупи атак $\{At_{ik}, At_{i(k+1),} At_{i(k+r)}\}$ із групи атак, які використовують ту саму небезпеку;
– кінцева ідентифікація атаки.

Для розв'язання іншої задачі аналізують розвиток аномалії, яка виникає у результаті дії At_i в оточенні фрагмента реалізації Zg_i. У цьому випадку опис атаки At_i наводиться у вигляді послідовності подій, виникнення яких вона спричиняє. Як тільки зміна аномалій в IT_i починає відповідати образу однієї атаки, це означає, що атака розпізнана. З цього випливає, що процес розпізнання атаки полягає у порівнянні чергової зміни виявленої аномалії в Zg_i з черговим елементом атак $\{At_i, At_{i1} ..., At_{ik}\}$. Якщо на наступному кроці зміни Zg_i виявиться, що поточна зміна відповідає поточному фрагменту тільки однієї атаки At_{iq}, то вважається, що розпізнана атака At_{ig} з множини атак $\{At_{i1},..., At_{ik}\}$. Необхідність повного розпізнавання атаки зумовлена тим, що протидіяти атаці засобами захисту Zg_i. можна лише тим змінам, які атака ще не здійснила, оскільки блокування уже здійсненого етапу функціонування атаки не зможе завадити реалізації наступного кроку атаки.

Якщо атака At_i розпізнана й описується змінами, які вона реалізує у відповідному фрагменті Zg_i, то відомий наступний крок її реалізації для протидії відповідній атаці. Отже, засобам захисту не потрібно протидіяти всім проявам атаки, а тільки тим, які ще не реалізовані. Це дає змогу спростити процес функціонування відповідних засобів захисту Za_i.

Важливою задачею є визначення наслідків впливу деякої атаки At_i на *IT* навіть у тому випадку, коли атака реалізувала лише частину етапів свого функціонування. Цей етап важливий з огляду на такі фактори:

– зміни у фрагменті Zg_i, які встигла реалізувати атака At_i, можуть бути використані іншими атаками At_j;
– зміни або модифікації фрагмента Zg_i можуть вплинути на окремі функціональні можливості *IT*;
– якщо перший та другий випадки неможливі, то модифікації в *IT*, після впливу певної кількості атак, накопичуються і можуть створити нову загрозу, яка є невизначеною на етапі прогнозування *IT*, а тому може виникнути нова атака, яка цією загрозою може скористатися. Для виключення цієї можливості та для забезпечення вимог стандарту безпеки адекватності *IT*, відповідні модифікації фрагментів Zg_i з *IT* повинні бути усунені. Ця задача розв'язується засобами системи безпеки незалежно від того, чи виникають атаки, чи ні. Якщо розглядати *IT* як програмне середовище, то відповідні модифікації фрагмента $Zg_i \in IT$ можуть полягати у зміні адреси в командах тіла програм, зміні окремих команд програми чи даних, які можуть бути у цих фрагментах. Такі відновлення здійснюються на основі використання описів відомих атак, що знаходяться у *SB,* які, як зазначалось вище, є описами модифікацій, що здійснюються в *IT* під дією At_i.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Столлинг В. Основы защиты сетей. Приложения и стандарты / В. Столлинг. — М. : Издательский дом «Вильямс», 2002.
2. Олгтри Т. Firewalls. Практическое применение серевых екранов / Т. Олгтри. — М. : ДМК Пресс, 2001.
3. Зегжда Д. П. Как построить защищенную информационную систему / Д. П. Зегжда, А. М. Ивашко. — Ч.1. — СПб. : Мир и семья, 1997.
4. Зима В. М. Защита компьютерных ресурсов от несанкционированых действий пользователей / В. М. Зима, А. А. Молдоваян, Н. А. Молдовян. — СПб. : типография Военной Академии связи, 1997.
5. Сенькивский В. Н. Автоматизация фотонаборных процессов / В. Н. Сенькивский. — Л. : Выща школа, 1987.
6. Волкова Л. А. Издательско-полиграфическая техника и технология / Л. А. Волкова. — М. : МГУП «Мир книги», 1999.

MEANS OF PROTECTION OF COMPUTER NETWORKS

B. V. Durnyak, T. M. Maiba
Ukrainian Academy of Printing
19, Pidholosko St., Lviv, 79020, Ukraine

The means of protection of computer networks have been reviewed according to: protection standards of information systems, selected requirements to ensure the functioning and ensuring a certain level of IT protection, which is defined as an integral parameter. The impact of technological processes at the possibility of management system design as an example of printing technological processes has been shown.

Keywords: *standards of safety of informative systems, means of protection, attack, danger.*

Стаття надійшла до редакції 08.07.2015.