УДК 004.04

ЗАСОБИ ЗАХИСТУ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Б. В. Дурняк, Т. М. Хомета

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

Розглянуто питання засобів захисту даних в інформаційних соціальних системах. Важливою умовою функціонування соціальної системи є економічна діяльність,завдяки якій можливі всі інші види діяльності членів соціальної системи, що ґрунтується на реалізації процесів формування та використання інформаційних засобів. Тому при реалізації відповідних інформаційних засобів захист даних здійснюється на основі інформації про те, які дані і якою мірою потрібно захищати.

Ключові слова: *інформаційно-соціальна система ICS, система захисту SBC, система доступу SD, небезпека NB, засоби захисту ZA_i, загроза SM, Fierwall, інтерпретація, атака, дебагер, аномалія.*

Постановка проблеми. Спільною особливістю інформаційних систем та методів організації засобів захисту даних у них є система захисту. Необхідність засобів захисту даних в інформаційних системах зумовлена наявністю небезпек, які існують стосовно даних, що передаються по цих системах, і систем загалом. Тому засоби захисту є сукупністю технічних рішень із захисту, кожен з яких орієнтований на певний тип відомих небезпек. Засоби захисту, що використовуються в інформаційних системах, формуються таким чином, щоб їх можливості протидії атакам були універсальними.

Мета статті — розглянути структуру системи захисту даних, яка містить засоби захисту, загрози, небезпеки, відбір інформації та інші компоненти, що використовуються для ініціації процесів виявлення атак та протидії атакам несанкціонованого доступу до ресурсів; показати інші види атак в інформаційних системах.

Виклад основного матеріалу дослідження. Соціальна система як об’єкт, для функціонування якого передбачено використання інформаційних засобів, повинна розглядатися з позиції мети функціонування такої системи. Однією з основних цілей є економічна діяльність, завдяки якій можливо реалізовувати всі інші види діяльності членів соціальної системи та соціальної системи загалом. Це означає, що насамперед необхідно розглянути використання інформаційних засобів у господарській діяльності. Найпопулярнішою господарською діяльністю вважається бізнесова діяльність. Основна характеристика або властивість, якою вона відрізняється від інших типів господарської діяльності, полягає у тому, що в цьому виді діяльності всі питання, пов’язані з функціонуванням окремого бізнесового об’єкта, розв’язуються в межах відповідної бізнесової структури. Зв’язок між такою бізнес-структурою та зовнішнім оточенням реалізується на основі зобов’язань, які виникають з необхідності оплати податків та інших зобов’язань, що регулюються державними органами в межах усієї соціальної системи. У зв’язку з цим проаналізуємо методи та засоби

інформаційного обслуговування, що реалізується в межах різних процесів, які відбуваються у соціальній системі і відображають її функціонування загалом. До них належать такі процеси:

– бізнесу;
– функціонування державних установ, які є загальними для всієї соціальної системи;
– навчання;
– медичного обслуговування;
– процеси, пов'язані з узагальненими змінами в соціальних системах, наприклад, процеси підвищення зайнятості населення, процеси міграції в межах соціальної системи та інші.

Оскільки одним з основних факторів, який зумовлює можливість ефективної роботи соціальної системи, є функціонування економіки, то передусім розглянемо особливості інформаційного обслуговування діяльності в цій галузі. У зв'язку з тим, що ця форма діяльності є досить різноманітною, опишемо деякі форми бізнесових процесів, які найбільше залежать від інформаційного обслуговування і часто ґрунтуються на реалізації процесів формування та використання інформаційних засобів у своїй діяльності. Виділимо такі форми діяльності, які безпосередньо пов'язані з інформаційними засобами:

– електронне проектування;
– електронно-інформаційні засоби комунікації;
– інформаційні засоби у виробництві;
– інформаційні засоби у торгівлі;
– інформаційні засоби у страховій діяльності;
– інформаційні засоби у транспорті та інші.

Розглянемо особливості задач захисту інформації в наведених формах діяльності. Захист інформації актуальний у таких випадках:

– коли існують відомості про існування інцидентів, пов'язаних з несанкціонованим використанням інформації в певних системах, що призводило до виникнення негативних факторів у організаціях, які їх застосовують;
– коли декларується необхідність захисту інформації в певній системі;
– коли захист інформації є природним розширенням функціональних можливостей систем.

Перший та другий випадок є тривіальними, а тому прокоментуємо третій випадок, що має кілька аспектів, а саме:

– юридичні аспекти;
– умови, які стосуються організації певного процесу, що виходять з природних закономірностей;
– вимоги, зумовлені фізичною природою реалізації відповідного процесу.

Перший аспект — це вимоги до документів, в яких регулюються питання, пов'язані із захистом даних. Прикладом такої ситуації можуть бути вимоги до захисту персональних і медичних даних та інші.

Оскільки інформаційні системи здебільшого використовують для автоматизації відомих процесів, то в таких процесах уже обумовлено ситуації, в яких необхідно захищати інформацію. Тому при реалізації відповідних інформаційних засобів потреба реалізації захисту даних здійснюється на основі інформації про те, які дані і наскільки їх потрібно захищати. Ці вимоги забезпечуються в системах і в тих випадках, коли вони не є автоматизованими. Тому захист інформації в системі, яка автоматизує такий процес, є природним розширенням засобів автоматизації. Наприклад, при автоматизації навчальних процесів до різних даних повинні мати доступ тільки ті учасники цього процесу, які мали певний доступ до них тоді, коли процес ще не був автоматизованим. Прикладом можуть бути оцінки студентів. У цьому випадку записувати оцінки мають повноваження тільки викладачі відповідних предметів і т. д. [1].

Третій аспект стосується інформаційних систем управління, які призначені для роботи з фізичними об'єктами або цілими технологічними процесами, які реалізуються на основі використання фізичних, хімічних чи інших процесів, що реалізуються відповідно до певних законів природи. Вони можуть мати певні обмеження до параметрів, що характеризують такий процес. Крім того, використання деякого фізичного процесу може мати подвійний характер з погляду свого призначення. У цьому разі захист інформації інтерпретується як захист процесу від можливого його переходу з одного режиму функціонування в інший. Він стосується можливості неуповноважених осіб приймати рішення про переключення режимів функціонування технологічного процесу, який здійснює управління відповідними фізичними процесами. Прикладом може бути управління атомною електростанцією [2].

Розглянемо наведені випадки з погляду розв'язання задач захисту, незалежно від причин, які зумовлюють необхідність реалізації захисту. В межах випадку, який характеризується тим, що захист необхідний у зв'язку з відомими випадками несанкціонованого використання даних, можна розглядати ряд інформаційних систем різного типу. Тому зупинимося, для прикладу, на деякій системі та методі організації засобів захисту у такій системі. Спільними функціями, що об'єднують різні системи, є:

– виявлення несанкціонованого впливу, переважно зі сторони довкілля, на об'єкт охорони;
– протидія виявленому фактору негативного впливу на систему, за яку приймемо інформаційну систему управління деяким об'єктом чи процесом;
– модифікація системи захисту таким чином, щоб відповідний фактор був не лише відразу розпізнаний, а й елімінований системою захисту;
– обчислення побіжного значення рівня безпеки системи;
– у разі потреби засоби захисту повинні керувати рівнем безпеки системи, що означає можливість зменшення чи збільшення цього рівня;
– прогнозування можливості виникнення негативного впливу щодо системи, яка охороняється, якщо відповідний негативний фактор належить до класу факторів, які є недопустимими;

– система захисту, яка забезпечує певний рівень безпеки інформаційної управлінської системи, повинна бути здатною розширювати свої функціональні можливості з розв'язання задач захисту.

У галузі захисту інформації для скорочення інтерпретаційних описів використовуються різні терміни. Розглянемо визначення тих термінів, які використовуватимуться. Оскільки певна термінологія орієнтована на системи різного типу, то її визначення може формулюватися таким чином, щоб останні враховували особливості тих систем, для яких відповідні терміни планується застосовувати. Це може стосуватися не всіх термінів, адже більшість із них визначена у відповідних стандартах, що не обмежує можливості їх використання в різних випадках, які визначаються особливостями системи, що є об'єктом захисту [3].

Визначення 1. Небезпекою будемо називати деякий зовнішній фактор, який може створити загрозу для об'єкта, який охороняється.

Небезпеку позначатимемо символами NB.

Визначення 2. Атакою називаємо послідовність подій, які реалізуються під дією небезпек NB та проявляються в середовищі об'єкта захисту.

Атаку будемо позначати:

$$A_i = f_i^a (a_{i1} * \ldots * a_{ik}) \quad (1)$$

де a_{ij} — окремі події, які проявляють дію атаки A_i,* — описує взаємозв'язок між окремими подіями, що відбуваються в об'єкті захисту.

Визначення 3. Об'єктом захисту є деяка інформаційна чи інформаційно-соціальна система, яку необхідно захищати від NB.

Позначатимемо символами ICS.

Визначення 4. Системою захисту називатимемо сукупність засобів захисту, які об'єднуються певною системою управління.

Таку систему будемо позначати символами SBC.

Визначення 5. Засоби захисту (ZA_i) являють собою окремі компоненти, кожен з яких орієнтований на протидію певному типу атаки.

Завдяки такій орієнтації виникає необхідність у розв'язуванні задачі розпізнавання типу атаки.

Визначення 6. Слабким місцем системи ICS називають такі фрагменти системи чи її елементи, використання яких небезпекою дозволяє активізувати відповідну атаку.

Таку характеристику фрагмента системи ICS позначатимемо символами SM. Досить часто SM називають загрозою, оскільки наявність в ICS відповідного фрагмента може призвести до того, що деяка NB використає відповідне SM для активізації атаки A_i. Оскільки довільна ICS може наразитися на певну атаку, то можна вважати, що не існує ICS, яка б не мала слабких місць. Це означає, що одним зі способів підвищення рівня безпеки, величину якої будемо позначати RB, є виявлення й усунення в ICS відповідних SM_i. Очевидно, що таке усунення реалізується шляхом розширення або розбудови відповідних фрагментів φ_i (ICS) таким чином, щоб виявлена атака не змогла б активізуватися на основі використання φ_i (ICS). Відповідно до наведених понять можна

стверджувати, що кожне SM_i існує в тому випадку, коли відома атака A_i, яка активізується за рахунок використання SM_i. Якщо прийняти, що деяке SM_i існує, то це означає, що відомою є деяка атака A_i, яка ініціюється безпосередньо NB_i.

У пропонованій праці розглядатимемо такі небезпеки, атаки, слабкі місця та засоби захисту, які реалізуються програмними засобами. Очевидно, що наведені визначення та відповідні поняття можна поширювати і на апаратурні засоби. У цьому випадку небезпека NB_i може являти собою деяку зовнішню систему, яка формує різні атаки у вигляді програмних засобів. Такі програмні засоби, відповідні NB_i передають у ICS через інформаційні канали, які практично використовуються ICS. Прикладом типових та відомих атак, що широко використовуються та передаються в ICS через канали зв'язку, є віруси [4]. Їх особливістю є те, що вони являють собою програмну реалізацію певних функцій, які зорієнтовані на здійснення обраної цілі в середовищі ICS, та їх реалізація враховує особливості програмних засобів ICS, на яку орієнтований певний вірус.

Засоби захисту, які використовують в інформаційних системах, формують таким чином, щоб їх можливості протидії атакам були, по змозі, універсальними. В деяких випадках створення одного типу захисту призводить до того, що він може протидіяти ряду атак. Це пов'язано з тим, що засоби захисту часто орієнтуються на елімінацію SM_i, а одне слабке місце може використовуватися безліччю атак, оскільки атаки класифікуються на основі відомостей про їхні функціональні можливості. Прикладом такого засобу захисту може слугувати Fierwall, який орієнтований на захист вхідного каналу від небажаних вхідних пакетів. У цьому випадку він розбудовується через розширення його можливостей у реалізації перевірки пакетів, які надходять на вхід системи. Мінімальною можливістю такого засобу є перевірка адреси приймача та надавача, яка полягає у визначенні, чи відповідні адреси є дозволеними для приймання пакетів від відповідних надавачів [5]. У зв'язку з цим Fierwall часто називають фільтром пакетів. Основною особливістю такого засобу захисту є те, що він функціонує на основі аналізу пакетів, які уже надійшли. Це означає, що коли атака здійснена, Fierwall розпізнає її як наявну. В цьому випадку вхідний пакет сприймається реалізацією атаки, якщо адреса надавача або приймача є забороненою для пропуску в систему. Оскільки внесення до списку заборонених адрес джерел пакетів є внутрішньою справою системи, то пакет із відповідного джерела не обов'язково формується як атака у джерелі, яке виступає в ролі небезпеки. Отже, можна стверджувати, що у багатьох випадках інтерпретація деякого вхідного пакета як результат дії деякої небезпеки NB_i відносно системи залежить від внутрішніх умов або обмежень, сформованих у відповідній системі. Це означає, що те саме джерело, яке породжує такий потік у вигляді послідовності пакетів, для іншої системи може не інтерпретуватися як атака.

Сьогодні існує тенденція до розширення функціональних можливостей одного засобу захисту для того, щоб він міг діяти щодо широкого класу типів

атак. Такий підхід не завжди є ефективним, оскільки використання складного засобу захисту не доцільне, коли типи атак, від яких треба захищатися — обмежені. У разі розширення типів атак відповідна система захисту може розширювати склад своїх компонентів через інсталяцію або активізацію в системах захисту. Це означає, що SBC повинна володіти бібліотекою різних засобів захисту, які можуть знадобитися в процесі її роботи. Розширення системи захисту новими засобами захисту реалізується на основі аналізу таких подій, які можуть виникати в ICS або в самій SBC:

– коли в ICS виявлено результат успішної атаки;
– коли виявлено лише факт виникнення атаки;
– коли виявлено зміну значень загальних параметрів, які характеризують ICS чи SBC.

Завдяки тому, що ICS відносно зовнішнього середовища є структуризованою, то атака може активізуватися тільки в межах системи доступу (SD). Це дає можливість розподілити процеси виявлення атак на класи:

– виявлення атак в (SD);
– виявлення аномалій в середовищі ICS;
– виявлення наслідків успішної атаки, які можуть проявлятися не тільки в ICS, а й в усій інформаційній системі, зокрема й включно з користувачами.

Виявлення атак в SD є найефективнішим з погляду убезпечення всієї системи, оскільки в цьому випадку атака ще не встигла здійснити заплановані негативні дії на об'єкт атаки. Це призводить до того, що більшість засобів захисту ZA_i орієнтовані на виявлення та елімінацію атак в компоненті SD. Прикладом цієї ситуації може бути система детекції інтрузій (IDS), яка на основі аналізу всіх негативних факторів, що виникають в оточенні системи, формує характеристики окремих фрагментів зовнішнього оточення мережі. Для цього використовуються різного типу сенсори, кожен з яких орієнтовано на виявлення певних типів відхилень та аномалій, а також втручань різних типів у систему [6].

Виявлення аномалій в середовищі інформаційних систем реалізується на основі таких підходів:

– моніторування всієї системи;
– реалізації діагностичних процедур;
– використання імітації дій негативних факторів на фрагменти, що орієнтовані на реалізацію функцій системи.

Моніторування реалізує певну процедуру перевірки окремих складових системи. Це означає, що функціонально — система структуризована відносно процесу, який реалізує ICS. Використання системи моніторингу для виявлення аномалій в ICS передбачає формування певної стратегії. Основною метою використання стратегії моніторування є оптимізація процесу функціонування системи SBC загалом. Очевидним є те, що ресурси обчислювальних засобів інформаційної системи повинні використовуватися системою SBC значно мен-

ше, ніж ресурси, які має використовувати система ICS для розв'язання прикладних задач. У відсотковому співвідношенні кількість ресурсів, яка може надаватися для SBC, визначається у кожному окремому випадку залежно від специфіки задач, які передбачено розв'язувати в інформаційній системі.

Результатом роботи системи моніторування є виявлення аномалії в середовищі ICS за винятком SD. Для того щоб можна було захищатися від негативного впливу атаки, необхідно розпізнати її. Для цього використовують процедури діагностування. Річ у тому, що аномалія може являти собою такі зміни в тексті програм, фрагментах даних чи в інших галузях пам'яті або середовища ICS, які ще не вказують однозначно на тип атаки та її поведінку. Наприклад, якщо аномалія є деяким програмним фрагментом, який не передбачений в системі, то необхідно визначити функціональні можливості відповідного фрагмента та інші дані про нього. Такі дані дають змогу визначити необхідну інформацію про атаку, яка сформувала відповідну аномалію.

Для аналізу виявленої аномалії використовують окремі засоби діагностування. Для цього методами, що подібні до тих, які використовує дебагер, встановлюється опис фрагмента на рівні машинної мови, наприклад, асемблера. В межах такого опису або образу визначаються загальні характеристики фрагмента, що полягає у:

– визначенні початку алгоритму, який реалізується фрагментом аномалії;
– визначенні типу вхідних даних, що використовуються у відповідній програмі;
– визначенні характеру результату функціонування відповідного фрагмента програми.

Наведені цілі функціонування засобів діагностики дають можливість визначити певну інформацію про атаку, яка створила відповідну аномалію.

Якщо з отриманих даних неможливо виявити необхідні характеристики типу атаки, то засоби SBC активізують засоби імітації дій можливих атак.

Засоби імітації копіюють підсистему або фрагмент системи в якому виявлено аномалії, та розміщають її в ділянці SBC, яка використовується як полігон для випробувань. Очевидно, що відповідний фрагмент системи повинен бути функціонально нероздільним, та мають бути відомими вимоги системи до відповідного фрагмента. У виділеній ділянці аномалія розміщається з реальним фрагментом. На основі використання опису модифікованого та опису відповідного реального фрагмента, які представлені у відповідних мовах програмування, реалізуються вибрані атаки та результат їхньої дії порівнюється із виявленою аномалією. Може трапитись, що жодна з відомих атак не приведе до ідентифікації виявленої аномалії очікуваної атаки. У цьому разі реалізується процес виведення відповідної аномалії. Він ґрунтується на таких даних: у фрагменті полігону в SBC активізується фрагмент, який вміщає аномалію. На основі аналізу вихідних даних та подій, до яких призводить активізація фрагмента з аномалією, формується опис цілі її існування. Якщо ціль встановлено, то на основі аналізу виводу з аномалії та функціональної різниці

між аномалією та оригінальним образом реалізується виведення подій, які можуть призвести до виникнення аномалії. З отриманої послідовності подій формують окремі фрагменти атаки, які на наступних циклах роботи ICS будуть використовуватися для приблизного визначення атак, що можуть виникати відносно ICS.

Виявлення наслідків успішних дій атак є одним із важливих випадків використання системи SBC. Особливо актуально це для систем, які призначені для функціонування з метою обслуговування завдань соціального характеру. Основою для підтримки або відновлення необхідного значення RB є використання аудиту. Оскільки кожна з ICS має власні специфічні задачі, що характерно при розв'язуванні соціальних задач, то в складі SBC повинна бути персональна система аудиту. Така система реалізує функції:

– в рамках класичних уявлень про аудит, система проводить аналіз даних про всі виконувані задачі;
– система збирає та аналізує всі звертання користувачів до системи з ціллю виявлення зауважень до процесу функціонування ICS;
– на основі даних аудиту відповідні засоби обчислюють узагальнений на період між аудитами рівень безпеки RB.

Висновки. Проведено аналіз використання захисту даних в інформаційних системах на основі небезпек, які переходять в атаки, що реалізуються програмними засобами. Знаходження та знешкодження дії атак важливо у використанні системи SBC, а також систем, які призначенні для обслуговування задач соціального характеру, зокрема персональної системи аудиту, що входить до складу системи SBC.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Сендж П. Пятая Дисциплина / П. Сендж. — Издательство «Дабли», 1990.
2. Ендренный Ж. Надежность моделирования в електросиловых системах / Ж. Ендренный. — Нью-Йорк. — Издательство «Вилли», 1978.
3. Общие критерии для оценки безопасности информационных технологий. — Ч. 1 : Введение и общая модель. — ISO/IEC SC27 N2161, 1998.
4. Козлов Д. А. Энциклопедия компьютерных вирусов / Д. А. Козлов, А. А. Парандовский, А. К. Парандовский. — М. : «Солон-1», 2001.
5. Польман Н. Архитектура брандмауеров для сетей предприятий / Н. Польман, Т. Кразес. — М. : Издательский дом «Вильямс», 2003.
6. Амороссо И. Исследование: Введение в интернет-изучения, соотношение, пастки, отслежывание и ответственность / И. Амороссо. — Издательство «AT&T», 1999.

MEANS OF DATA PROTECTION IN INFORMATION SYSTEMS

B. V. Durnyak, T. M. Khometa

Ukrainian Academy of Printing,
19, Pidholosko St., Lviv, 79020, Ukraine

The article presents the issue of means of data protection in the information social systems. An economic activity is an important function of social system

functioning which makes possible all types of other activity of members of the social system, which is based on realization of forming processes and use of information means. Therefore, during the realization of the proper information means, the data protection is carried out on the basis of information about what data and in what extent it is needed to protect them.

Keywords: *Information social system ICS, system of protection SBC, system of access o SD, danger NB, protection facilities of ZAi, threat SM, Firewall, interpretation, attack, debugger, anomaly.*

Стаття надійшла до редакції 12.03.2015.