УДК 004.73056.5 (045)

С. А. Яремко
канд. техн. наук
Вінницький торговельно-економічний інститут КНТЕУ

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ КОРПОРАТИВНИХ СИСТЕМ НА ОСНОВІ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Вступ. Новітні інформаційні технології є на даний час одним із рушійних факторів розвитку усіх сфер життєдіяльності людини: економіки, техніки, науки та освіти. Так, завдяки використанню телекомунікаційних засобів мережі Internet, стало можливим здійснення централізованого управління великими корпораціями, структурні підрозділи яких знаходяться у різних регіонах країни та за кордоном. Це дозволяє вирішувати проблеми забезпечення належної швидкості передачі інформації та обміну повідомленнями, здійснення бізнес-транзакцій та укладення електронних угод.

Постановка завдання досліджень. Проте, поряд з перевагами, які надають телекомунікаційні засоби для обміну повідомленнями та фінансовими даними, постає проблема захисту конфіденційної інформації від несанкціонованого доступу та пошкоджень. Так, згідно зі статистикою, наведеною в [1], до центру координації CERT університету Карнегі Меллон (США) кожного дня надходить біля 225 повідомлень про порушення безпеки в інформаційних системах компаній. Разом з тим, будь-яке стороннє втручання може вплинути на достовірність інформації та, у підсумку, спричинити загрозу фінансової стабільності корпорації. Тому управління інформаційною безпекою в корпоративних системах на основі розроблених норм, правил і практичних прийомів політики безпеки (ПБ), які регулюють управління, захист і розподіл цінної інформації, є актуальною задачею досліджень.

Аналіз останніх досліджень і публікацій. Основні поняття теорії захисту інформації, правила та положення політики безпеки, їх реалізацію на основі інформаційних систем і технологій обґрунтували в своїх наукових роботах такі вчені як: Бармен С., Грушо А. А., Тимоніна Е. Е., Баричев С. Г., Гончаров В. В., Сєров Р. Е., Щербаков А. Ю. та ін. Їх праці є основою для створення і реалізації нових напрямів та методів у сфері захисту інформації.

Метою статті є розробка положень політики безпеки (далі ПБ) в корпоративних інформаційних системах, що дозолить забезпечити конфіденційність інформації, а також її доступність та захист від сторонніх втручань.

Основна частина. На даний час роль комп'ютерної безпеки невпинно зростає. Компанії запрошують адміністраторів, розробників та інженерів, щоб забезпечити надійність своїх систем, служб та інформації протягом всієї доби. Адже стати жертвою зловмисних користувачів, програм або скоординованих атак є прямою загрозою успішної діяльності будь-якої компанії. Разом з тим, процес розробки норм та правил ПБ може бути досить складним і потребує врахування базових принципів захисту інформації, а також особливостей конкретної системи. Так, зокрема ПБ у різних корпоративних інформаційних системах може змінюватись в залежності від набору інформаційних компонентів, обраної шкали цінностей, виявлених загроз безпеці інформації, а також наявних у корпорації апаратних та програмних ресурсів для захисту інформації.

В загальному випадку, побудова ПБ для інформаційних систем включає наступну послідовність дій [2, 3]:

— створення структури цінностей;

— проведення аналізу загроз безпеці інформації;

— визначення правил для будь-якого процесу користування даним видом доступу до елементів інформації, що мають дану шкалу цінностей.

Розробимо базові положення ПБ для корпоративної інформаційної системи «1С-Підприємство», яка є найбільш розповсюдженою на теренах України і використовується на середніх та великих підприємствах і корпораціях.

З огляду на те, що забезпечення цілісності, доступності та конфіденційності інформації є особливо важливим у галузі медицини, розробимо правила ПБ при роботі із інформацією для мережі аптек ПП «Конекс», де використовується корпоративна інформаційна система «1С-Підприємство». Нехай дана корпоративна система мережі аптек включає наступні компоненти:

— повідомлення, які передаються від структурних підрозділів по інформаційному каналу мережі Internet на Web-сервер головного офісу корпорації;

— базу даних персоналу корпорації;

— базу даних, в якій зберігається інформація про діяльність структурних підрозділів;

— базу даних, в якій містяться зведені показники облікової та фінансової діяльності корпорації;

— модуль обробки даних, що надійшли від структурних підрозділів;

— модуль прийняття управлінських рішень щодо діяльності корпорації;

— управлінські вказівки, які передаються у зворотньому напрямку по інформаційному каналу до структурних підрозділів корпорації.

Для визначення цінності кожного інформаційного компонента застосуємо порядкову шкалу, яка використовується при оцінці секретної інформації в державних структурах [2]: «*несекретна*» (*НС*), «*для службового використання*» (*ДСВ*), «*секретна*» (*С*), «*цілком таємно*» (*ЦТ*). Дані рівні секретності утворюють множину $R = \{НС, ДСВ, С, ЦТ\}$, яка є лінійно впорядкованою: $НС < ДСВ < С < ЦТ$. При цьому вищий рівень має більшу цінність і тому вимоги для його захисту від несанкціонованого доступу є теж більш високими. Враховуючи наведене вище, присвоїмо відповідні рівні секретності інформаційним компонентам корпоративної системи: повідомленням, що передаються від структурних підрозділів на Web-сервер головного офісу корпорації — рівень *С*; базі даних персоналу корпорації — *ДСВ;* базі даних, в якій зберігається інформація про діяльність структурних підрозділів — *ДСВ;* базі даних, в якій містяться зведені показники діяльності корпорації — *ДСВ*; модулю обробки даних, що надійшли від структурних підрозділів — *С;* модулю прийняття управлінських рішень — *ЦТ*; управлінським вказівкам, які передаються у зворотному напрямку до структурних підрозділів — *С*. В результаті здійсненої ідентифікації, компоненти системи, кожний із яких має певний рівень секретності, утворюють множину:

$$M = \{K_{ir}, \ldots, K_{nr}\}, \qquad (1)$$

де $i = 1, 2, \ldots, n$ — інформаційні компоненти системи; *r* — рівень секретності інформаційної компоненти, $r \in R$. Згідно [3] множину (1) можна вважати лінійною решіткою цінностей. Тоді для елементів з множини *M*, які мають різні секртності $K_{iДСВ}, K_{iС}, K_{iЦТ}$, будуть справедливими відношення:

$$K_{iДСВ} < K_{iC}, K_{iC} < K_{iЦТ} \Rightarrow K_{iДСВ} < K_{iЦТ}.$$

Із наведених властивостей випливають наступні визначення:

Визначення 1: для $K_{iДСВ}, K_{iC} \in M$ елемент $K_{iЦТ} = K_{iДСВ} \oplus K_{iC} \in M$ є верхньою межею, якщо:

1. $K_{iДСВ} < K_{iC}, K_{iC} < K_{iЦТ}$;
2. $K_{iДСВ} < K_{iДСВ} \oplus K_{iC}, K_{iC} < K_{iДСВ} \oplus K_{iC} \Rightarrow K_{iЦТ} < K_{iДСВ} \oplus K_{iC}$ для всіх $K_{iДСВ} \oplus K_{iC} \in M$.

Таким чином, верхньою межею решітки є елемент, рівень якого має найбільшу цінність, що передбачає самий високий ступінь захисту.

Для $K_{iДСВ}, K_{iC} \in K_{iЦТ}$ елемент $K_{iНС} = K_{iДСВ} \otimes K_{iC} \in M$ є нижньою межею, якщо:

1. $K_{iНС} < K_{iДСВ}, K_{iНС} < K_{iC}$;
2. $K_{iДСВ} \otimes K_{iC} < K_{iДСВ}, K_{iДСВ} \otimes K_{iC} < K_{iC} \Rightarrow K_{iДСВ} \otimes K_{iC} < K_{iНС} < ДСВ$, для всіх $K_{iДСВ} \otimes K_{iC} \in M$.

Нижньою межею решітки є елемент, який має найменшу цінність і характеризується найменшим ступенем захисту.

Визначення 3: множина M є решіткою, якщо для будь-яких $K_{iДСВ}, K_{iC} \in M$ існують $K_{iДСВ} \oplus K_{iC} \in M$ та $K_{iДСВ} \otimes K_{iC} \in M$.

На основі наведеного вище можна зробити висновок, що для всіх елементів M решітки цінностей існує верхній елемент $High = \oplus M$ та нижній елемент $Low = \otimes M$. В даному випадку верхнім елементом решітки *High* буде $K_{iЦТ}$, а нижнім елементом — $Low - K_{iНС}$.

Після визначення цінностей інформаційних компонент згідно обраної порядкової шкали, для даної корпоративної інформаційної системи наступним етапом побудови ПБ є визначення загроз безпеці інформації та проведення їх аналізу. Під загрозами будемо розуміти дії або чинники, що можуть привести до порушення секретності, цілісності та доступності інформації в корпоративних інформаційних системах. Так, до втрати секретності інформації згідно [4–6] можуть привести наступні загрози: ненадійні працівники, ворожа розвідка, неякісна політика інформаційної безпеки, непомітне зняття інформації, передача конфіденційної інформації, розпізнавання інформації та підключення до каналів зв'язку. До порушення цілісності інформації, тобто її знищення або модифікації можуть привести наступні чинники: помилки персоналу, людський фактор, доступ до заземлення, пожежі, стихійні лиха, а також різноманітні вірусні атаки. До втрати доступності інформації, тобто неможливості її отримання, приводять різноманітні збої, а також розрив каналу передачі інформації.

Головними подіями, на основі наведеного розгляду загроз, будемо вважати розсекречення інформації, порушення її цілісності та доступності, а подіями, що їх зумовлюють — відповідні чинники цих подій.

При умові незалежності загроз, ймовірності появи головних подій будемо знаходити наступним чином [7]:

— у випадку появи головної події за умови логічного множення подій, що її спричиняють:

$$P = \prod_{i=1}^{k} P_i;$$

— у випадку появи головної події за умови логічного додавання усіх подій, що її спричиняють:

$$P = 1 - \prod_{i=1}^{k} (1 - P_i),$$

де P_i — ймовірність *i*-ої події, яка серед інших зумовлює появу даної головної події; k — загальна кількість подій, які спричиняють появу головної події.

Розглянувши загрози або події, які призводять до втрати безпеки інформації в корпоративних інформаційних системах, та визначивши головні та зумовлюючі події, відобразимо їх у вигляді ієрархічної моделі дерева ризику-відмов (рис. 1) [8].

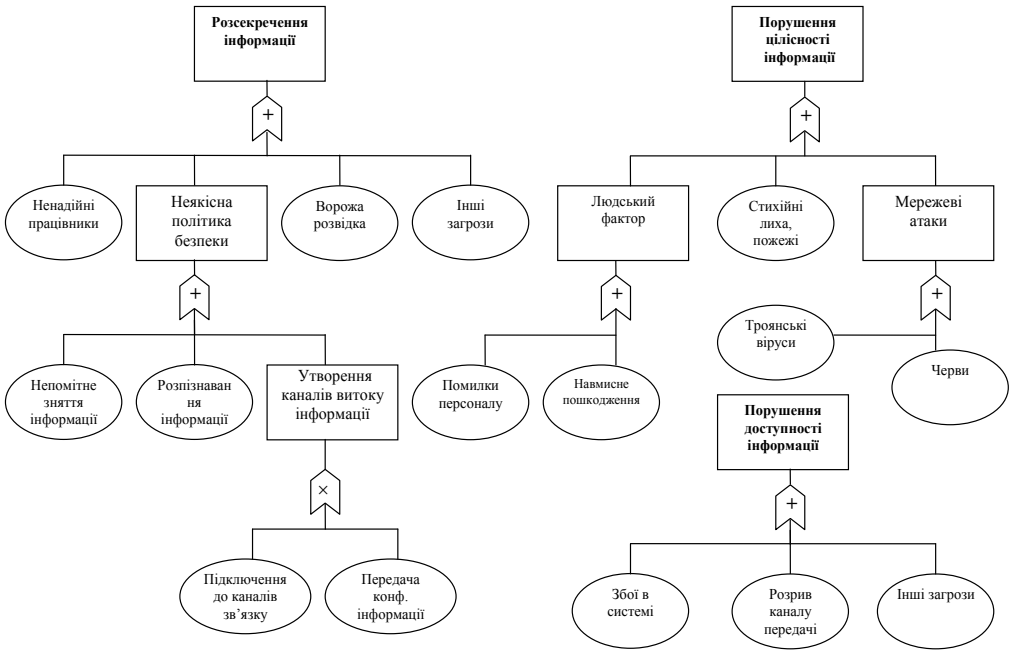

Рис. 1. Ієрархічні моделі загроз безпеці інформації в корпоративних інформаційних системах

На основі наведених моделей загроз визначимо їх ранги. Це дасть змогу виявити значущість даних загроз для загальної безпеки інформації в корпоративних інформаційних системах. Визначення рангів подій будемо здійснювати згідно методики, запропонованої у [8]. Вона передбачає обчислення різниці між ймовірністю появи головної події P та P^i — ймовірністю у випадку вилучення i-ої події, ранг якої розраховується, що відповідає виразу:

$$\Delta P_i = P - P^i$$

На основі наведених ймовірностей подій у [8] будемо здійснювати обчислення різниці між ймовірністю появи головних подій та ймовірністю за вилученням даної події.

Розташувавши обчислені різниці ΔP_i в порядку зростання, ми отримаємо ранги загроз безпеці інформації. Зведемо результати розрахунків ΔP_i та отримані ранги у табл.

Таблиця 1

Результати розрахунків ΔP_i та отримані ранги подій

№ події	Назва події	Різниця ймовірностей	Ранги подій
Розсекречення інформації			
1	Ненадійні працівники	0,45	1
2	Ворожа розвідка	0,1	3
3	Непомітне зняття інформації	0,05	4
4	Передача конфіденційної інформації	0,05	4
5	Розпізнавання інформації	0,15	2
6	Підключення до каналів зв'язку	0,15	2
7	Інші загрози	0,05	4
Порушення цілісності інформації			
1	Людський фактор	0,75	1
2	Стихійні лиха	0,03	5
3	Пожежі	0,07	3
4	Мережеві атаки	0,09	2
5	Інші загрози	0,06	4
Порушення доступності інформації			
1	Збої в системі	0,5	1
2	Розрив каналу передачі інформації	0,45	2
3	Інші загрози	0,05	3

Як видно з табл.1, найвищий ранг мають загрози, пов'язані з людським фактором: ненадійності працівників, допущення ними помилок та навмисних дій щодо пошкодження інформації, що свідчить про їх значущий вплив на безпеку інформації в корпоративних інформаційних системах.

Враховуючи визначені цінності інформаційних компонент, які потрібно захищати, та розраховані ранги погроз, які впливають на загальну безпеку інформації, сформуємо на основі [2, 3] базові положення ПБ для корпоративної інформаційної системи «1С-Підприємство», що використовується на даному підприємстві.

Визначення правил доступу. Це необхідно для того, щоб особи, які не мають відповідного для допущеного персоналу діапазону повноважень, не змогли отримати доступ до конфіденційних даних стосовно діяльності структурних підрозділів та корпорації в цілому; повідомлень від структурних підроздів, які передаються на Web-сервер корпорації; управлінських вказівок, які передаються у зворотньому напрямку тощо. Визначення правил доступу здійснюється за допомогою мандатного контролю, який дає можливість проводити контроль усіх звернень до інформаційних компонентів системи. Бажано також передбачити у системі безпеки можливість отримання доступу до даних службовому персоналу, якщо в цьому є необхідність і відповідна санкція керівництва.

Ідентифікація інформаційних об'єктів системи. Для того, щоб здійснювати управління доступом до інформації у відповідності до мандатного контролю, необхідно здійснити маркування кожного інформаційного компонента системи, що дасть змогу однозначно ідентифікувати об'єкт. Це може бути визначена цінність компонента або режими допуску, надані тим суб'єктам, які можуть запитувати цінну інформацію.

Контроль запитів цінної інформації. Для уникнення несанкціонованого доступу до інформації, необхідно здійснювати контроль за тим, на які класи цінної інформації дозволений доступ певним особам.

Контроль ризиків безпеки інформації. Необхідно здійснювати реєстрування подій, які мають відношення до безпеки системи, що надасть змогу забезпечити ефективний аналіз ризиків безпеки інформації.

На основі наведених правил та вимог для забезпечення секретності, цілісності та доступності інформації, розглянемо шляхи реалізації ПБ. Як було зазначено вище, контроль доступу до цінної інформації можна здійснювати за допомогою мандатної політики. Вона виконується підсистемою захисту на найнижчому апаратно-програмному рівні, що дозволяє ефективно будувати захищене середовище для механізму мандатного контролю. Пристрій мандатного контролю, що виконує крім зазначених, інші додаткові функції, називається монітором звернень. Мандатний контроль ще називають обов'язковим, оскільки його проходить кожне звернення суб'єкта до об'єкту, якщо суб'єкт і об'єкт знаходяться під захистом системи безпеки. Розглянемо спосіб організації мандатного контролю в корпоративній інформаційній системі «1С-Підприємство». Кожний інформаційний компонент K_{ir} отримує мітку про клас (цінність) $C(K_{ir})$. Кожний суб'єкт S також має мітку, що містить інформацію про те, який клас доступу $C(S)$ він має. Мандатний контроль порівнює мітки і задовольняє запит суб'єкта S до об'єкту K_{ir} на читання, якщо $C(S) > C(K_{ir})$, і задовольняє запит на запис, якщо $C(S) < C(K_{ir})$. Якщо в системі реалізований мандатний контроль, при зверненні користувача U_i до бази даних на читання дозволяється формувати «огляд» тільки такої інформації, клас якої $< C(U_i) < C(U)$. Аналогічно, мандатний контроль і правила декомпозиції дозволяють підтримувати в потрібному напрямі інформаційні потоки в процесі функціонування бази даних. Отже, за наявності мандатної політики, реляційна багаторівнева база даних буде захищена шляхом розмежування доступу до цінної інформації.

Наступним шляхом реалізації ПБ є вибір режимів та класу системи захисту безпеки інформації. Для обґрунтованого вибору режимів та класу системи захисту розрахуємо індекс ризику безпеки інформації в корпоративній інформаційній системі «1С-

Підприємство». Серед присвоєних рівнів секретності інформаційних компонентів системи мінімальним рівнем допуску користувача R_{min} в системі є ДСВ, а максимальним R_{max} — ЦТ. Так як в порядковій шкалі цінностей ДСВ = 2, а ЦТ = 4, тоді індекс ризику згідно [7] буде становити: $Risk\ Index = R_{max} - R_{min}$.

Визначеному індексу ризику, згідно [4, 5, 7], відповідають наступні режими захисту:

— c — багаторівневий режим, який дозволяє системі обробку інформації двох або більше рівнів секретності. При цьому не всі користувачі мають допуск до всіх рівнів інформації, що обробляється;

— d — контролюючий режим: багаторівневий режим обробки інформації, при якому немає повної гарантії захищеності, що накладає обмеження на допустимі класи цінної інформації, що обробляється;

— e — режим ізольованої безпеки: режим дозволяє ізольовано обробляти інформацію різних класів, що дає змогу забезпечити захист тільки певного класу інформації.

Ще однією важливою складовою інформаційної безпеки є клас системи захисту. Мінімальним класом, що вимагається для захисту інформації, є В3. Даний клас реалізує концепцію монітора звернень, що дає змогу здійснювати захист від несанкціонованих змін, псування та підробки. Цей клас захисту передбачає введення адміністратора безпеки системи. Згідно зазначених вище вимог створеної ПБ, механізми контролю в даному класі дозволяють забезпечити обов'язкове повідомлення про можливі порушення правил безпеки. Обов'язковими також є процедури, що забезпечують відновлення працездатності системи. Таким чином, вибір системи даного класу дає можливість забезпечити стійкість до різноманітних спроб втручання.

Обраними методами захисту інформації є резервування, архівація та знищення інформації. Для нейтралізації каналів витоку інформації, слід здійснювати контроль інформаційних потоків, а також шифрування інформації криптографічними методами.

Висновки. В роботі вирішено задачу розробки правил ПБ для корпоративних інформаційних систем, а також наведено напрямки їх реалізації, що дає змогу забезпечити конфіденційність інформації, а також її доступність та захист від сторонніх втручань. З цією метою було визначено рівні секретності інформаційних компонентів системи та проаналізовано загрози безпеки інформації, що дало змогу обґрунтувати вимоги ПБ для конкретної корпоративної інформаційної системи «1С-Підприємство» та обчислити індекс ризику, на основі якого було обрано відповідні засоби захисту.

Література

1. Кунченко-Харченко В. І. Документалістика / В. І. Кунченко-Харченко. — Черкаси : ЧДТУ, 2006. — 147 с.
2. Грушо А. А. Теоретические основы защиты информации / А. А. Грушо, Е. Е. Тимонина. — М. : Издательство агентства «Яхтсмен», 2001. — 76 с.
3. Бармен С. Разработка правил информационной безопасности / С. Бармен ; пер. с анл. — Н. : «Вильямс», 2002. — 208 с.
4. Плескач В. Л. Інформаційні технології та системи : підруч. для студ. екон. спец. / В. Л. Плескач, Ю. В. Рогушина, Н. П. Кустова. — К. : «Книга», 2004. — 520 с.
5. Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности / А. Ю. Щербаков. — М. : Нолидж, 2001. — 150 с.
6. Главатый В. Методы защиты информации / В. Главатый // Корпоративные системы. — 2005. — № 4. — С. 65–69.
7. Баричев С. Г. Основы современной криптологии / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. — М. : Горячая линия. — Телеком, 2001. — 180 с.
8. Дудатьєв А. В. Розробка уніфікованих моделей системного проектування оптимальних систем захисту інформаційних ресурсів / А. В. Дудатьєв // Вісник ЧДТУ. — 2008. — № 1. — С. 3–8.