УДК 004.056

Л.Ф. Єжова,
кандидат економічних наук, доцент

ЕКОНОМІЧНІ АСПЕКТИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Проаналізовано економічні аспекти інформаційної безпеки й запропоновано методики оцінювання ризиків для інформаційної системи в цілому, для окремих інформаційних процесів (сервісів), для окремих груп інформаційних активів.

Ключові слова: *ризики інформаційної безпеки, процесні ризики, методики оцінювання ризиків.*

В статье анализируются экономические аспекты информационной безопасности и предлагаются методики оценивания рисков для информационной системы в целом, для отдельных информационных процессов (сервисов), для отдельных групп информационных активов.

Ключевые слова: *риски информационной безопасности, процессные риски, методики оценивания рисков.*

In article economic aspects of information safety are analyzed and techniques of an estimation of risks for information system as a whole, for separate information processes (services), for separate groups of information actives are offered.

Keywords: *risks of information safety, process risks, techniques of an estimation of risks.*

Сучасний бізнес в Україні зазнає ризиків інформаційної безпеки, що динамічно змінюються. Для того, щоб зберегти конкурентоспроможність підприємства, необхідно впроваджувати економічно обґрунтовані заходи захисту цінних інформаційних активів. На стані інформаційної безпеки позначаються такі чинники як постійне збільшення кількості електронних злочинів, жорсткі й часто змінювані вимоги з боку держави та регуляторів, посилення залежності бізнесу від безперебійної роботи інформаційної системи підприємства.

Перед побудовою або модернізацією комплексної системи захисту інформації важливо оцінити можливі матеріальні збитки і можливість реалізації загроз безпеці інформації, для чого передовсім доцільно проаналізувати можливі інформаційні ризики.

Метою дослідження є розробка методик обчислення можливих втрат системи від реалізації загроз інформаційній безпеці та пошук шляхів удосконалення процесу управління ризиками.

Для досягнення поставленої мети необхідно виконати наступні *завдання:* проаналізувати існуючі методики аналізу ризиків, побудувати математичну модель оцінювання ризиків втрат системи, застосувати цей підхід до окремих інформаційних процесів (сервісів), до окремих груп інформаційних активів і визначити шляхи вдосконалення процесу управління ризиками.

Процес управління ризиками безпеки дозволяє поєднати максимальну економічну ефективність із прийнятним рівнем бізнес-ризику й надає користувачам зрозумілий метод організації та розстановки пріоритетів при обмежених ресурсах для реалізації управління ризиками. Це, у свою чергу, дозволяє організаціям здійснювати економічно ефективний контроль ризику з метою мінімізації матеріальних втрат в результаті несанкціонованого втручання. Процес управління ризиками залежить від особливостей організації, **рівня її зрілості, правильного вибору методики побудови систем та джерел інформації для аналізу. Тому** не існує універсального рішення та єдиної моделі управління ризиками.

Результати аналізу ризику актуальні лише протягом певного проміжку часу. Потім можуть змінитися склад системи, зовнішні умови тощо, і доведеться проводити новий аналіз. При цьому деякі фактори не враховувалися в минулому періоді, а деякі могли втратити актуальність.

При аналізі ризиків може виявитися, що деякі ризики залежать від виникнення інших ризиків, і тоді з певною ймовірністю може виникнути ланцюгова реакція. Тобто події, пов'язані з несанкціонованим втручанням в інформаційні процеси, не можна вважати цілком незалежними. Проте в межах нашого дослідження цей варіант не розглядається.

Оцінка ризиків організації є одним із основних факторів формування вимог до інформаційної безпеки. Через ідентифікацію загроз та оцінку ризиків їх здійснення оцінюється уразливість активів, визначається їх цінність для організації, а також можливий негативний вплив і наслідки при реалізації несанкціонованих дій.

Управління інформаційними ризиками включає такі етапи:

– аналіз та оцінку ризиків;

– вибір та оцінку рішень за результатами аналізу ризиків;

– створення та впровадження набору заходів та засобів для своєчасного зменшення рівня ризиків до припустимої величини згідно з міжнародними стандартами ISO;

– впровадження моніторингу, аудиту та контролю стану інформаційної безпеки для оцінки ефективності процесу управління ризиками.

Під час виконання оцінки ризиків здійснюється:

– інвентаризація й оцінка цінності інформаційних активів;

– ідентифікація відповідних вимог законодавства та нормативної бази;

– ідентифікація загроз і вразливостей інформаційної безпеки та оцінка ймовірності їх здійснення;

– детальний технічний аналіз уразливостей інформаційних систем організації щодо загроз та оцінка величини ідентифікованих загроз;

– визначення системи організаційних заходів із підтримки режиму інформаційної безпеки;

– визначення величини та ймовірності завдання шкоди в результаті здійснення загроз безпеки.

Процес управління ризиками безпеки поєднує елементи кількісного (більш детального) та якісного (більш простого) методів аналізу, що робить його ефективним, зручним у використанні та зрозумілим на кожному кроці оцінювання для всіх зацікавлених осіб. Якісний підхід зменшує протидію персоналу на етапах аналізу ризику та ухвалення рішень, дозволяє швидше знайти задовільне рішення та забезпечити його підтримку впродовж всього процесу. Якісний підхід

використовується, в першу чергу, в організаціях з найменшим рівнем зрілості.

При оцінці ризиків якісний підхід використовується для швидкого впорядковування переліку всіх ризиків безпеки, а кількісний підхід дозволяє надалі виконати детальний аналіз відносно невеликої кількості найбільш суттєвих ризиків, виявлених на цьому етапі. Аналіз ризиків може бути виконаний з різним ступенем деталізації залежно від критичності ресурсів інформаційного об'єкта, відомих уразливостей і попередніх інцидентів інформаційної безпеки [3].

Оскільки у процесі аналізу ризиків бере участь декілька підрозділів, то процес його проведення бажано автоматизувати, щоб забезпечити узгоджені дії адміністративного рівня в усіх підрозділах. Непоодинокими є випадки, коли заборона доступу чи його обмеження для працівника в одному підрозділі невідома в системі, або скінчився термін доступу до певних інформаційних ресурсів, а повноважень доступу ніхто не відмінив. Такі ситуації негативно впливають на рівень інформаційної безпеки організації, що є неприпустимим.

Практично на всіх етапах управління ризиками необхідно робити їх оцінку. Існують різні підходи і методи оцінки ризиків, запропоновані різними виробниками. Наведемо найбільш поширені методики.

Методика FRAP

Методика "Facilitated Risk Analysis Process (FRAP)", запропонована компанією Peltier and Associates, дозволяє компаніям віднайти баланс між витратами на засоби захисту й отримуваним ефектом.

Оцінка визначається за правилами, що задаються матрицею ризиків, яка виділяє чотири рівні ризиків:

– рівень A – дії, пов'язані з ризиком, повинні бути виконані обов'язково й негайно;

– рівень B – пов'язані з ризиком дії повинні бути виконані;

– рівень C – попередження, що потрібен моніторинг ситуації;

– рівень D – ніяких дій на цей час здійснювати не потрібно.

Методика RiskWatch

Компанія RiskWatch розробила методику аналізу ризиків для проведення різних видів аудиту безпеки і сімейство програмних засобів, які її реалізують.

У методі RiskWatch як критерії для оцінки і управління ризиками використовуються очікувані річні втрати і оцінка повернення інвестицій. RiskWatch орієнтована на точну кількісну оцінку співвідношення втрат від загроз безпеки і витрат на створення системи захисту. Для формули розрахунку ($M=p*v$, де M – математичне очікування, p – вірогідність виникнення загрози, v – вартість ресурсу) запропоновано деякі зміни, а саме вводиться також поправочний коефіцієнт q, який дозволяє врахувати, що в результаті реалізації загрози ресурс може бути знищений не повністю, а тільки частково. M – це оцінка очікуваних втрат для одного конкретного активу від реалізації однієї загрози.

Коли всі активи і дії ідентифіковані і зібрані разом, то з'являється можливість оцінити загальний ризик інформаційної системи як суму всіх окремих значень.

Методика CRAMM

В основу методу CRAMM покладено комплексний підхід до оцінки ризиків, що поєднує кількісні і якісні методи аналізу і проводиться у три стадії. Для кожного інформаційного процесу будується дерево зв'язків використовуваних ресурсів. Побудована модель дозволяє виділити критичні елементи. Цінність

фізичних ресурсів в CRAMM визначається вартістю їх відновлення в разі руйнування, дається оцінка збитків за шкалою зі значеннями від 1 до 10. При низькій оцінці за всіма використовуваними критеріями (3 бали і нижче) вважається, що дана система вимагає базового рівня захисту (без докладної оцінки загроз ІБ).

На другій стадії оцінюються залежність призначених для користувача сервісів від певних груп ресурсів і існуючий рівень загроз і вразливостей, обчислюються рівні ризиків і аналізуються результати. Ресурси групуються за типами загроз і вразливостей.

Програмне забезпечення CRAMM для кожної групи ресурсів і кожного типу загроз генерує список питань, що допускають однозначну відповідь. Рівень загроз оцінюється, залежно від відповідей, як дуже високий, високий, середній, низький і дуже низький. Рівень уразливості оцінюється, залежно від відповідей, як високий, середній і низький. На основі цієї інформації розраховуються рівні ризиків від 1 до 7.

Проте оцінка ризиків на якісному рівні не дозволяє однозначно порівняти витрати на забезпечення інформаційної безпеки і одержувану від них віддачу (у вигляді зниження сумарного ризику). Тому переважними є кількісні методики, а вони вимагають наявності оцінок імовірності виникнення для кожної загрози безпеки.

При постановці процесу управління ризиками застосовують методики, що враховують положення та вимоги міжнародних стандартів ISO / IEC 17799, ISO / IEC 27001 та CobiT (Control Objectives for Information and related Technology), а також рекомендації NIST (National Institute of Standards and Technology).

Використовуються також оригінальні методики, розроблені на основі власного досвіду, а також світової практики та міжнародних стандартів, спеціальні інструментальні засоби, засновані на структурних методах системного аналізу і проектування (SSADM – Structured Systems Analysis and Design).

Після вибору методики необхідно знайти оцінки гранично припусти-мого та існуючого ризику здійснення загрози протягом певного часу (наприклад, року). Значення ймовірності здійснення кожної із загроз протягом певного часу допомагає співвіднести оцінку можливих збитків із витратами на захист. На практиці більшість керівників обмежуються якісними оцінками загроз, оскільки складно отримати достовірні дані про ймовірність реалізації загрози.

Оцінка ризиків інформаційної безпеки складається з таких етапів:

– визначення переліку об'єктів, що потребують захисту, інформаційною службою підприємства;

– формування повної множини загроз інформації за методологією, запропонованою в [1];

– аналіз і вибір переліку загроз, з огляду на особливості функціонування підприємства;

– виявлення можливих джерел цих загроз;

– визначення імовірності здійснення потенційних загроз із використанням експертні оцінки;

– оцінка можливих збитків в разі здійснення ідентифікованих загроз.

Ці збитки будуть складатися з витрат на відновлення інформації, заміну чи ремонт устаткування, комунікацій та програмного забезпечення, на

впровадження нових структурних елементів, на навчання і перепідготовку персоналу, на відновлення позицій на ринку та іміджу підприємства тощо.

Нині розрахунок можливих втрат в інформаційній сфері базується на експертних оцінках, що є достатньо суб'єктивними, а тому не має необхідної вірогідності. Іноді кількісні величини, отримані від різних експертів, суттєво різняться. В інформаційній сфері ця різниця може виявитися ще більш значною через нематеріальні властивості основних активів. Додатково уточнити експертні оцінки фахівців із інформаційної безпеки щодо можливої шкоди можна за рахунок оцінок керівників бізнес-процесів, для чого вони мусять відповісти якомога точніше на низку питань.

1. Які ваші обов'язки щодо збереження конфіденційності та цілісності даних?
2. Чи може спотворення цих даних призвести до великих втрат?
3. Чи існує реальна можливість такої події?
4. Чи може несанкціонований доступ до цих даних спричинити втрати в майбутньому (втрачена можливість у бізнесі)?
5. Чи може цей ви випадок піти на користь вашим суперникам (конкурентам)? Які можливі втрати від цього? Втрата клієнтів?
6. Яким може бути психологічний ефект від втрат? Чи можливі ускладнення?
7. Яке значення доступу до цих даних для організації?
8. Чи можна відкласти обробку цих даних?
9. Чи можна ці обчислення виконати в іншій організації?
10. Скільки вам коштуватиме обробка цих даних в іншому місці?
11. Які проблеми можуть виникнути при втраті ваших даних?
12. Чи можна відновити втрачені дані? Скільки це буде коштувати ?

Більш висока вірогідність може бути отримана на основі статистики відповідних прецедентів та аналогів. Однак в Україні статистичні дані про правопорушення в інформаційній сфері, через низку причин (у першу чергу, небажання потерпілих оприлюднювати відомості про недостатній рівень захисту інформації), не мають високої вірогідності і докладної деталізації, що свідчить про недостатню увагу до цих аспектів економічної безпеки та про відсутність необхідної системної аналітичної роботи.

У країнах з розвиненою інформаційною інфраструктурою для оцінки ризиків використовуються статистичні показники, вивірені бухгалтерські стандарти і процедури, результати, отримані в рамках незалежного аудиту. Наприклад, у США збір і аналіз відповідної статистичної інформації здійснюють: правоохоронні органи (близько 40 суб'єктів), зокрема міністерство юстиції; торгово-промислова палата; компанії, що працюють у сфері високих технологій та інформаційної безпеки, а також інші державні органи і комерційні організації. Налагоджена інформаційно-аналітична система дозволяє з високим ступенем ймовірності визначати не тільки характер загроз, але і їх кількісні параметри (вагові коефіцієнти).

Побудова процесу управління інформаційними ризиками є одним з найважливіших елементів системи ІБ, в який інтегровані всі основні процеси організації.

Якщо в даний час в організації взаємодію менеджерів з безпеки з бізнес-підрозділами не організовано на належному рівні, то залучення всіх найваж-

ливіших підрозділів організації до процесу аналізу ризиків стане важливим етапом побудови комплексної системи інформаційної безпеки компанії.

Побудуємо математичну модель оцінки ризиків.

Нехай маємо:

ІТ-система, що складається з n структурних елементів

$i = 1, 2, \ldots, n$;

повна множина загроз щодо елементів системи має m складових

$j = 1, 2, \ldots, m$;

x_{ij} – втрати системи від здійснення j-ої загрози до і-го елемента;

p_{ij} – ймовірність здійснення j-ої загрози до і-го елемента.

Побудуємо матрицю поелементних втрат системи (табл. 1).

Таблиця 1

Матриця втрат системи

Загрози / Об'єкти	1	2	...	m	$\sum_{J=1}^{m}$
1	X_{11}	X_{12}	...	X_{1m}	X_1
2	X_{21}	X_{22}	...	X_{2m}	X_2
...	...	...	...	...	...
n	X_{n1}	X_{n2}	...	X_{nm}	X_n
$\sum_{i-1}^{n}$	Y_1	Y_2	...	Y_m	

$X_i = \sum_{J=1}^{m} X_{ij}$ – максимально можливі втрати і-го об'єкта від загроз;

$Y_j = \sum_{i=1}^{n} X_{ij}$ – максимально можливі втрати системи від j-ої загрози.

Матриця, звичайно, буде містити нульові клітини при побудові, а опісля аналізу втрат деякими з них можна нехтувати, якщо вони будуть меншими за певний припустимий рівень втрат, тобто для спрощення розрахунків їх теж можна прирівняти до нуля.

Витік різних документів конфіденційного характеру завжди має різні наслідки для компанії. Формально обидва документи можуть маги однаковий гриф, а збитки компанія від їх витоку понесе зовсім різні. В такому випадку можна оцінювати ризик за максимальною шкалою шкоди для всіх таких документів, однак при цьому рівень втрат буде перебільшений, неадекватний реальності.

Для оцінки можливих збитків побудуємо матрицю ймовірностей втрат системи від здійснення загроз.

Для початкового визначення p_{ij} можна застосувати якісну шкалу (мала ймовірність і т. д. аж до високої ймовірності на кшталт методики FRAP, яка пропонує чотири рівні безпеки A, B, C, D). Але для подальших обчислень треба використовувати числові значення (наприклад, обирають певний набір типових значень: 0,1, 0,3 та 0,5; 0,7; 0,9). Крім того, якщо є відповідна статистика здійснення загроз на підприємстві або на аналогічних підприємствах, можна знайти більш реальні значення цих показників. Можна також скористатися послугами експертів з інформаційної безпеки для визначення ймовірностей здійснення загроз.

При цьому подія, яка повинна обов'язково відбутися, не є ризиком, і дії, які необхідно в зв'язку з ним зробити, враховуються в рамках звичайного планування і управління, а не управління ризиками.

Таблиця 2

Матриця ймовірностей втрат системи

Загрози \ Об'єкти	1	2	. . .	m
1	P_{11}	P_{12}	. . .	P_{1m}
2	P_{21}	P_{22}	. . .	P_{2m}
. . .	. . .	. . .	. . .	. . .
n	P_{n1}	P_{n2}	. . .	P_{nm}

Математичне сподівання втрат і-го об'єкта

$$M(X_i) = \sum_{J=1}^{m} X_{ij}\, p_{ij}$$

$M(X_i)$ – середнє значення можливих втрат і-го об'єкта від здійснення всіх загроз.

Математичне сподівання втрат системи від j-ої загрози

$$M(Y_j) = \sum_{i=1}^{n} X_{ij}\, p_{ij}$$

$M(Y_j)$ – середнє значення сукупних втрат системи від j-ої загрози.

Можна розрахувати можливі втрати об'єкта від здійснення декількох загроз одночасно.

Наприклад, при здійсненні 5-ої, 6-ої та 10-ої загроз до 2-го об'єкта втрати S будуть

$$S = X_{2,5} + X_{2.6} + X_{2.10}$$

Ймовірність такої події (за умови незалежності загроз) буде дорівнювати

$$P = p_{2,5}\, p_{2.6}\, p_{2,10}$$

Математичне сподівання втрат від такої події буде такою

$$M(S) = S \cdot P$$

Отримані середні значення втрат можна використовувати для визначення найбільш вразливих місць, їх ранжирування та визначення черговості використання інвестицій у системі безпеки підприємства для підвищення рівня захисту інформації.

Для кожного інформаційного процесу, що має самостійне значення і є призначеним для користувача сервісом, можна побудувати дерево зв'язків використовуваних ресурсів або матрицю зв'язків.

Щоб побудувати матрицю можливих втрат для кожного сервісу, спочатку побудуємо матрицю зв'язків між сервісами та ресурсами (інформаційними активами, об'єктами), використовуваними даним сервісом (табл. 3). Ненульові значення в клітинах таблиці призначатимуться тільки для ресурсів, використовуваних даним сервісом. Нехай в організації здійснюється k інформаційних процесів (сервісів), кожний з яких використовує певні інформаційні ресурси.

Таблиця 3

Матриця зв'язків між сервісами та ресурсами

Сервіси \ Об'єкти	1	2	...	k
1	z_{11}	z_{12}	...	z_{1k}
2	z_{21}	z_{22}	...	z_{2k}
...	...	...	...	...
n	z_{n1}	z_{n2}	...	z_{nk}

Де

1, якщо pr-ий сервіс використовує i-ий ресурс,

$z_{i,pr} = 0$, якщо не використовує

i=1, ..., n;

pr = 1,..., k.

Побудуємо матрицю можливих втрат від загроз для сервісів наступним чином. Обчислимо vs_{prj} втрати pr-го сервісу від здійснення j-ої загрози

$$vs_{prj} = \sum_{i=1}^{n} x_{ij} z_{i,pr},$$

де

pr = 1, ..., k;

i = 1, ..., n;

j = 1, ..., m.

Тоді матриця можливих процесних втрат матиме вигляд, проілюстрований наведеною нижче таблицею.

Таблиця 4

Матриця можливих процесних втрат

Загрози / Сервіси	1	2	. . .	m
1	vs_{11}	vs_{12}	. . .	vs_{1m}
2	vs_{21}	vs_{22}	. . .	vs_{2m}
. . .	. . .	. . .	. . .	. . .
k	vs_{k1}	vs_{k2}	. . .	vs_{km}

Математичне сподівання втрат pr-го сервісу від здійснення j-ої загрози розраховуємо наступним чином:

$$M(vs_{pr,j}) = \sum_{i=i}^{n} vs_{pr,j}\, p_{ij};$$

$$M(vs_{pr}) = \sum_{j=1}^{m} \sum_{i=1}^{n} vs_{pr,j}\, p_{ij}$$

Побудована модель дозволяє виділити критичні елементи в кожному сервісі, а для решти загроз можна призначити базовий рівень захисту, для якого не вимагається докладної оцінки загроз інформаційної безпеки.

Крім того, можна провести ідентифікацію і оцінку рівнів загроз для груп ресурсів та їх вразливостей. Ресурси групуються за типами загроз і вразливостями. Наприклад, у разі існування загрози пожежі або крадіжки, до групи ресурсів доцільно включити всі ресурси, що знаходяться в одному місці (серверний зал, кімната засобів зв'язку і т. д.). Оцінка рівнів загроз і вразливостей для груп ресурсів можна провести за тією ж методикою, що і для сервісів та на основі дослідження непрямих чинників.

Ні в кого не викликає сумнівів той факт, що найбільшу загрозу для інформаційної безпеки становлять саме користувачі. Для формалізації залежностей між інформаційними ресурсами (активами) та користувачами необхідно побудувати матрицю доступів, що надаються користувачам до інформаційних об'єктів (табл. 5).

Нехай до інформаційних об'єктів системи мають доступ L користува-чів, кожний з яких має ідентифікатор суб'єкта (ідентифікатор користувача, мережну адресу комп'ютера тощо). Кожний об'єкт має свій список рівнів доступу. Наприклад, програмний файл припускає такі окремі дії стосовно нього:

"o" – дозвіл на передачу прав доступу іншим користувачам;
"r" – читання;
"w" – запис;
"e" – виконання;
"a" – додавання інформації.

Крім того, із файлом можуть виконуватись комбінації перерахованих дій: "rw", "orw" тощо. Усі ці дії можна ранжирувати, і тоді ранг визначить рівень доступу до такого інформаційного об'єкта, як програмний файл.

Для кожного суб'єкта буде свій рівень доступу до конкретного інформаційного об'єкта.

Позначимо множину рівнів доступу через RD=(1, 2, ..., D). Тоді елементами матриці доступу будуть $d_{li} \in RD$, l=1, 2, ..., L.

Таблиця 5

Матриця доступу користувачів до інформаційних об'єктів

Об'єкти / користувачі	1	2	...	n
1	d_{11}	d_{12}	...	d_{1n}
2	d_{21}	d_{22}	...	d_{2n}
...	...	...	...	...
L	d_{L1}	d_{L2}	...	d_{Ln}

Аналізуючи цю матрицю, можна здійснювати наступне:
– визначати сумарний рівень доступу до системи кожного користувача (суми за рядками матриці);
– контролювати рівні доступу кожного користувача до кожного інформаційного об'єкта при зміні його статусу в організації;
– визначати списки доступу;
– визначати сумарний рівень доступу до кожного інформаційного об'єкта системи (суми за стовпцями матриці);
– контролювати рівні доступу до кожного інформаційного об'єкта та залежність його рівня безпеки від кожного користувача і, у разі необхідності, змінювати окремі рівні доступу;
– при кожній зміні елементів матриці перераховувати залишковий ризик, щоб визначити рівень захисту інформаційної системи в цілому.

При великій кількості користувачів традиційні підсистеми керування доступом стають занадто складними для адміністрування. Зменшити складність керування можна за допомогою рольового керування. Його сутність полягає у наступному.

Проаналізуємо матрицю й об'єднаємо користувачів у групи з однаковим рівнем доступу до одних і тих самих ресурсів, тобто визначимо групи користувачів

з однаковою роллю в інформаційній системі. Побудуємо матрицю рольового доступу до інформаційних ресурсів (табл. 6).

Таблиця 6

Матриця рольового доступу до інформаційних ресурсів

Об'єкти \ Ролі	1	2	. . .	n
1	d_{11}	d_{12}	. . .	d_{1n}
2	d_{21}	d_{22}	. . .	d_{2n}
. . .	. . .	. . .	. . .	. . .
L_g	dL_{g1}	dL_{g2}	. . .	d_2L_g

Аналіз сумарного доступу за кожною групою дозволить визначити найбільшу залежність рівня безпеки інформаційної системи від рольової групи користувачів і вживати необхідні заходи для його підвищення.

Але кожному користувачеві одночасно може бути відведено кілька ролей, тобто він може належати до різних рольових груп. Тому рольовий доступ можна вважати певним каркасом чи оболонкою для розмежування доступу. І взагалі, матрицю доступу необов'язково зберігати в явному вигляді: можна для кожного конкретного завдання (процесу) обчислювати вміст відповідних клітинок.

Крім того, важливим є врахування операційних ризиків при побудові та функціонуванні систем захисту інформації. Сучасні підходи до оцінки операційних ризиків допускають використання як статистичних, так і нестатистичних методів. Більшість подій ІБ відбуваються нечасто, через що інформація про них рідко потрапляє до накопичувальної статистичної бази з операційних ризиківх, що ведеться в організації. Тому для оцінки ризиків інформаційної безпеки необхідно використовувати нестатистичні методи, наприклад метод аналізу сценаріїв на основі експертної оцінки, що припускає виділення подій, пов'язаних із порушенням конфіденційності, цілісності або доступності інформації, які могли б завдати шкоди інтересам компанії. Список сценаріїв формується на основі переліку критичних інформаційних ресурсів і інформаційних сервісів, визначених раніше. Для кожного сценарію зі списку здійснюється експертна оцінка ймовірності його реалізації і можливих втрат. З метою одержання достовірних і відтворюваних результатів експертам надається максимально можлива достовірна інформація й набір формальних критеріїв оцінювання, наприклад час недоступності інформаційного сервісу або фіксований перелік можливих наслідків сценарію.

Будь-який аналіз ризиків носить імовірнісний характер, тому в ряді випадків варто керуватися здоровим глуздом і більш тісно взаємодіяти з бізнесом для отримання реальних результатів.

Проблеми ризиків інформаційної безпеки і знаходження шляхів зниження шкоди постають з кожним роком все гостріше. Однак не всі власники і користувачі інформаційних ресурсів можуть самостійно забезпечити надійний захист інформації та гарантоване покриття можливих втрат від ризиків.

Можливі рішення з управління ризиками:

– застосування належних контролів для зниження ризиків;

– об'єктивне прийняття рішень щодо ризиків, які задовольняють політику організації та критерії оцінки ризиків;

– уникнення дій, які можуть спричинити виникнення ризиків;

– перерозподіл ризиків між іншими сторонами;

– страхування ризиків.

Для забезпечення їх поінформованості й зацікавленості необхідно чітко розподілити ролі й відповідальність у процесі керування ризиками, наприклад, відповідальність за контроль над ризиками ІБ, пов'язаними з бізнес-процесом, покласти на власника процесу. При цьому він здійснює оцінку можливих збитків у разі реалізації загрози й повідомляє про зміни, що відбуваються в бізнес-процесі.

Можна також розподілити ризик між страхувальниками або постачальниками шляхом створення дієвого страхового захисту – системи страхування ризиків інформаційної безпеки, яка є важливим і перспективним інструментом управління ризиками інформаційної безпеки організації, економічно вигідним методом компенсації збитків власникам інформаційних активів. Доцільно розглядати страхування ризиків інформаційної безпеки в комплексі зі страхуванням інформаційних і фінансових активів організації, ризиків, пов'язаних із комерційною діяльністю.

Результати аналізу ризиків повинні надаватися вищому керівництву в лаконічному та інформативному вигляді, відзначатися простотою й доступністю викладу. Більш складні та докладні документи повинні бути передані керівникам середньої ланки для опрацювання.

Проблеми безпеки необхідно вирішувати, але їм не завжди приділяється належна увага, оскільки забезпечення безпеки є витратною статтею в бюджеті організації. Необхідно постійно доводити керівництву та співробітникам організації, що безпека – важлива функція самого бізнесу, що відіграє важливу роль у переході на більш високий рівень зрілості процесів забезпечення інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Андреєв В.І.* Основи інформаційної безпеки / В.І. Андреєв, В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест ; за ред. проф. В.О. Хорошка. – 2-е вид., доп. і перероб. – К. : Вид. ДУІКТ, 2009. – 292 с.

2. *Юдін О.К.* Захист інформації в мережах передачі даних : Підручник / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович. – К. : Видавництво ТОВ НВП "ІНТЕРСЕРВІС", 2009. – 714 с., іл.

3. *Рішняк І.В.* Системний аналіз категорій ризику та невизначеності / І.В. Рішняк // Вісн. Нац. ун-ту "Львівська політехніка". – 2003. – № 489.

Отримано 10.10.2011