

ДОСЛІДЖЕННЯ ОЦІНКИ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Стаття присвячена дослідженню та оцінці основних загроз інформаційної безпеці об'єктів інформаційної діяльності, а також засадам забезпечення інформаційної безпеки організації. В статті узагальнено існуючі наукові підходи до визначення сутності загроз та джерел, уразливостей, розглянуто класифікації можливих загроз та напрями забезпечення інформаційної безпеки організації.

Ключові слова: загрози, інформаційна безпека, забезпечення інформаційної безпеки, забезпечення інформаційної безпеки організації, оцінка загроз.

Постановка проблеми

Суспільна трансформація та загальна нестійкість, заплановані біфуркації та неочікувані переміни сторіччями несуть з собою превентивну функцію підготовки до зустрічі з несподівано складними емерджентними проблемами, ставлячи у тому числі задачі пошуку нових підходів до оцінки загроз інформаційної безпеки (ІБ) об'єктам інформаційної діяльності (ОІД). В умовах бурхливого розвитку інформаційних технологій (ІТ), коли вони стали основою для формування глобального інформаційного суспільства, у свою чергу ІБ стає життєво необхідною умовою забезпечення інтересів людини, суспільства та держави і найважливішою ланкою всієї системи національної безпеки країни.

Стан інформаційної безпеки України істотно залежить від загроз, прояв яких може завдати непоправної шкоди як державному так і комерційному секторам національної економіки [1]. Саме тому дослідження основних загроз та засад щодо оцінки ІБ ОІД для побудови ефективних систем захисту інформації (ЗІ) є актуальним.

Аналіз останніх досліджень і публікацій

ІБ в Україні вже набула обрису нового державно-громадського інституту, становленню якого, як і в інших країнах світу, притаманна низка проблем. Так наприклад, у взятому Україною курсі на входження у європейський простір (підкріплений Указом Президента України Про Стратегію кібербезпеки України від 27 січня 2016 року [2]) акцентується увага на посиленні значення та ролі ІБ, як складової національної безпеки України. Одним із пріоритетів забезпечення ІБ визначено при цьому створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них. Дослідженню цих питань присвячено роботи: В.Л. Бурячка, Ю.В. Богдановича, П.О. Балашова, С.В. Кавуна, С.В. Казмірчук, О.Г. Корченко, В.О. Хорошко тощо. Використання різних методик з метою оцінювання захисту інформації в організаціях розглядали у своїх роботах: В.В. Бут, О.В. Гребенюк, В.В. Домарєв, М.О. Живко, І.Р. Конєв, В.В. Микитенко, А.А. Садердинов, О. А. Сороківська, М. Ю. Танцюра, В. С. Цимбалюк.

Метою статі є дослідження сучасних вітчизняних та зарубіжних підходів у визначенні оцінки основних загроз щодо об'єктів інформаційної діяльності.

Викладення основного матеріалу

Інформаційна безпека – це, як відомо [3], «стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій». Основу ІБ становлять політика ІБ, законодавча, нормативно-правова та наукова база ІБ, структура органів, які здійснюють захист інформації, а також методи, способи і засоби, які вони для цього застосовують. Напрями ІБ та етапи її формування подано на рис.1. Зважаючи, що заходи забезпечення ІБ в організації спрямовуються головним чином на те, щоб не допустити збитків від втрати інформації, правомірно перш за все сконцентрувати увагу на визначенні загроз – сукупності умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства та держави в цілому в інформаційній сфері. Передумовою появи загроз ІБ є як об'єктивні (недосконалість засобів захисту), так і суб'єктивні фактори (промислове шпигунство, карні елементи, несумлінні співробітники тощо).

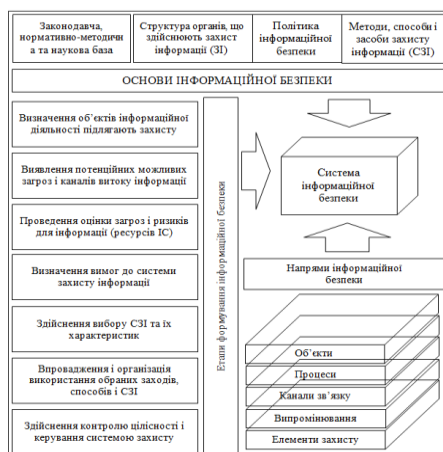


Рис. 1. Основи, етапи та напрями формування ІБ

Природа походження загроз ІБ може бути при цьому випадковою (збої, помилки, побічні впливи тощо), або навмисною (злочинні дії соціуму), табл.1.

Таблиця 1.

Типи загроз інформаційній безпеці в інформаційних системах

ТИП ЗАГРОЗИ		Причини або спонукальні мотиви
Навмисні загрози	Ненавмисні загрози	
Розкрадання носіїв інформації	—	Прагнення використовувати конфіденційну інформацію (КІ) у своїх цілях
Застосування програмних пасток	—	Недостатня кваліфікація обслуговуючого персоналу, застосування несертифікованих технічних засобів
—	Несправність апаратури, що може ініціювати несанкціоноване зчитування ІР	Завдання збитків шляхом НСД в інформаційну систему (ІС)
Використання програм «троянський кінь»	—	Завдання збитків шляхом внесення програмних закладок у процесі розробки програмних систем
Помилки в програмах обробки інформації	—	Руйнування ІС з метою завдання збитків
Впровадження комп'ютерного вірусу	—	Застосування несертифікованого програмного продукту
—	Помилки в програмах обробки інформації	Недотримання персоналом вимог ІБ, порушення технологічної послідовності роботи з ІС
—	—	З метою створення каналу для витоку КІ
Помилкова комутація в мережі ЕОМ	—	НКВ обслуговуючого персоналу
—	Помилкова комутація в мережі ЕОМ	Недостатнє урахування вимог безпеки на етапі проектування ІС або її створення
—	Паразитне електромагнітне випромінювання (ЕМВ)	Вивід з ладу ІС з метою завдання збитків
Примусове ЕМВ	—	Одержання конфіденційної інформації
Використання акустичних випромінювань	—	Несанкціоноване втручання в роботу системи в злочинних цілях
Копіювання за допомогою візуального і слухового контролю	—	Недостатня кваліфікація, застосування несертифікованого ПЗ
Маскування під користувача, підбір паролів	—	Використання недостатнього захисту
—	Помилка в роботі оператора	З метою добування особистої вигоди або завдання збитків
—	Помилки користувача	—
Помилки програміста: опис, переключування програмного захисту, розкриття кодів, паролів	—	Недостатня кваліфікація обслуговуючого персоналу, порушення технології
Помилки технічного персоналу: опис і переключування схем захисту, помилкова комутація	—	—
—	Помилки персоналу: переключування схем захисту, помилкова комутація	—

Засобами реалізації загроз як правило є: шкідливе та потенційно небезпечне ПЗ (computer virus; worm; trojan horse; rootkit; spyware тощо), Internet-шахрайство (phishing, carding, pharming, sms phishing тощо), несанкціонований доступ (НСД) до ІР та ІС (hacking, deface), DoS та DDoS-атаки тощо. За наслідками своєї дії загрози ІБ спрямовані на порушення *конфіденційності, цілісності та доступності до інформації* (рис.2). Оцінку можливих

актуальних загроз ІБ в організації доцільно починати з аналізу джерел загроз, обумовлених різними факторами.

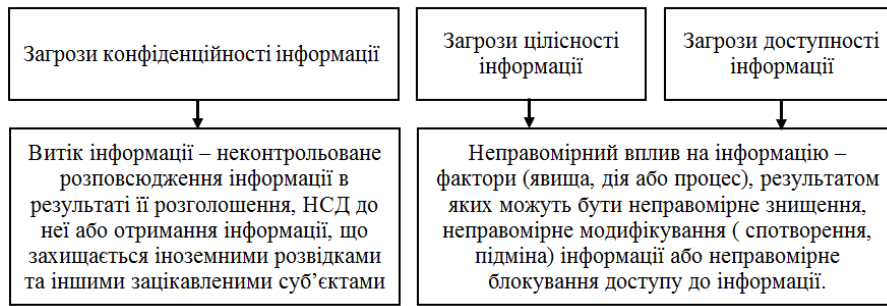


Рис. 2. Ознаки загроз конфіденційності, цілісності та доступності інформації

Джерелами загроз можуть виступати: людина, технічні пристрої, моделі, алгоритми, програми; технологічні схеми обробки; зовнішнє середовище. Прикладом цьому можуть слугувати статистичні дані, оприлюднені аналітичним центром компанії InfoWatch. Фахівці компанії стверджують, що останнім часом більше половини інцидентів, зафіксованих в компаніях, а саме біля 65,4%, пов'язані з внутрішніми порушниками. При цьому витік інформації відбувається з їх вини або по необережності. Причиною більше 32% витоку інформації на ОІД стають зовнішні зловмисники. У 51,2% випадків винуватцями витоків інформації були нинішні та колишні робітники – 48,9% і 2,3% відповідно. Тобто, як видно, нині саме людський фактор є одним з основних чинників ризику з точки зору ІБ організації. Наступний крок має полягати в проведенні аналізу факторів, які можуть вплинути на реалізацію певної загрози та визначенні низки актуальних загроз (рис.3).

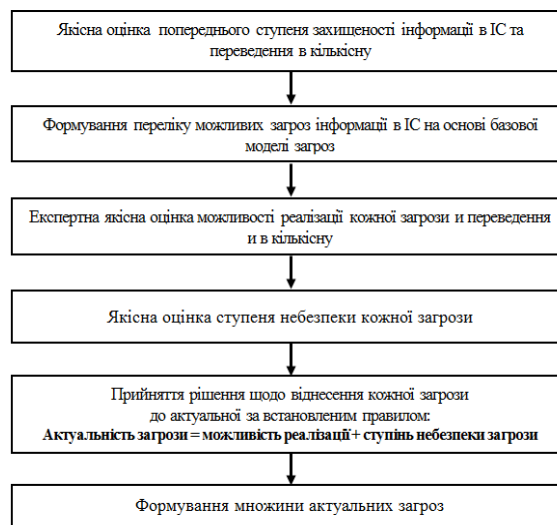


Рис. 3. Загальний порядок визначення актуальних загроз

Одним із найважливіших етапів цього процесу є проведення якісно-кількісної оцінки можливості реалізації кожної загрози. Більшість відомих підходів до оцінювання ймовірності реалізації загрози ґрунтуються на апостеріорних, апріорних та експертних методах (рис.4).

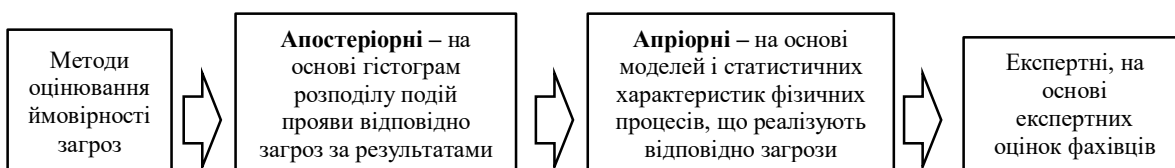


Рис. 4. Методи визначення ймовірності реалізації загроз

В контексті ситуаційного підходу процедуру оцінювання ймовірної реалізації загроз доцільно починати з актуальних загроз із ряду відомих класифікацій загроз [4 – 9] щодо вибраної організації (рис.5).

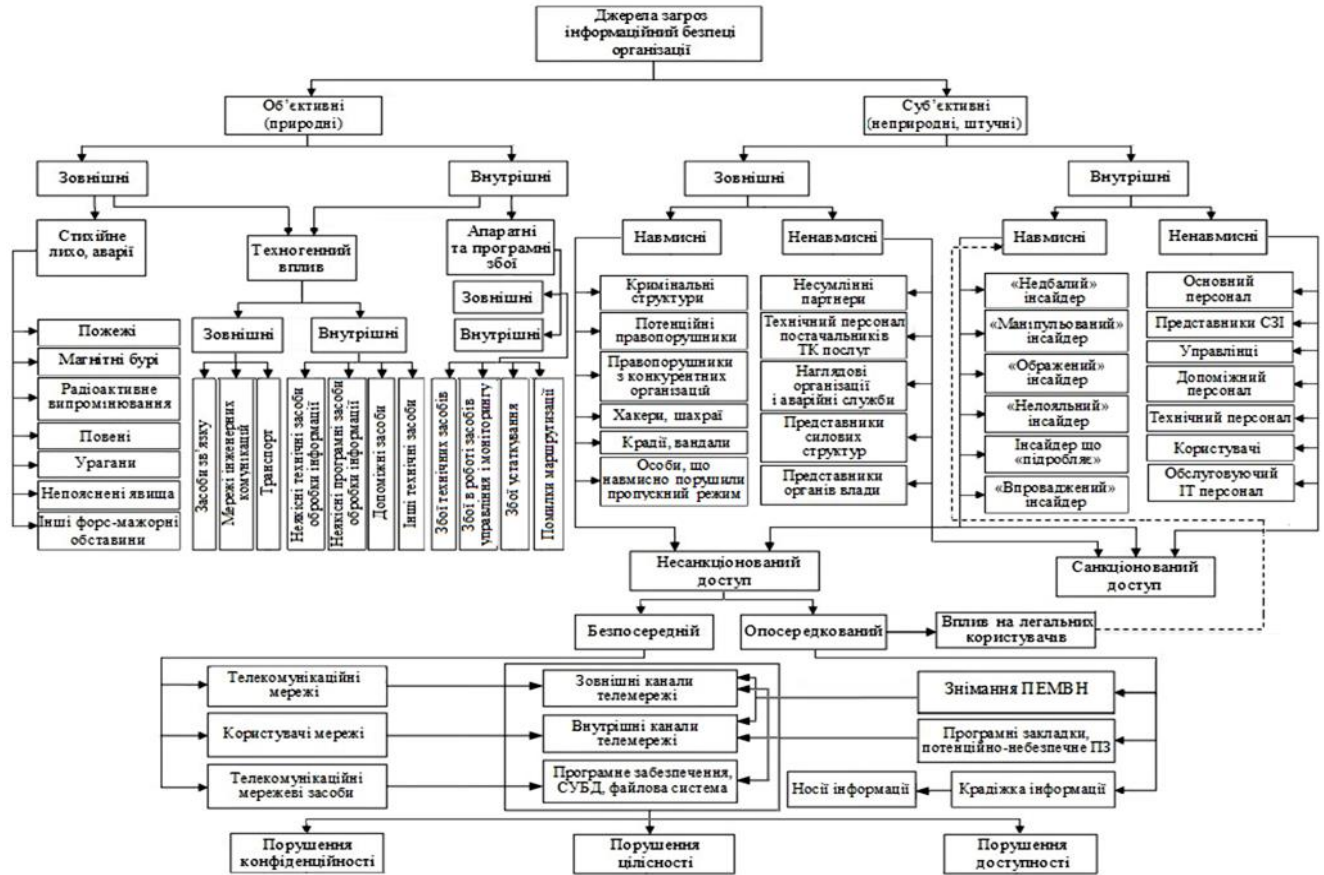


Рис. 5. Класифікація загроз за видами ознак та можливі цілі їх прояву

Враховуючи таке та з урахуванням пропозицій авторів [10] ймовірність реалізації кожної i -ої загрози по відношенню до j -го активу визначатимемо, використовуючи рівняння (1):

$$d_{rj} = 1 - p_{ri} \times \prod_{i=1}^m (1 - p_{rji}), \quad (1)$$

де n – кількість загроз;
 m – кількість активів;
 p_{ri} – можливість здійснення i -ої загрози;
 d_{rj} – можливість реалізації хоча б однієї загрози j -му активу.

При цьому:
$$p_{ri} = p_{ti} \times p_{vi}$$

де p_{ti} – можливість появи i -ої загрози;
 p_{vi} – можливість появи уразливості щодо реалізації i -ої загрози.

Наступним етапом буде обчислювання ціни ризику R_j для кожного j -го активу:

$$R_j = d_{rj} \times p_j, \quad (2)$$

Ціна повного ризику дорівнює сумі цін ризику для всіх активів за формулою:

$$R_{\text{повн}} = \sum_{j=1}^n R_j, \quad (3)$$

При визначенні коефіцієнта нейтралізації загроз вибирається система захисту інформації (СЗІ). При вирішенні щодо доцільності використання прийнятої СЗІ організації, наприклад, якщо $0,8 \leq \text{КНЗ} - \text{СЗІ}$ рекомендується використовувати як основну [10].

Відповідно до іншого підходу, сценарії реалізації загроз об'єкту захисту можуть бути представлені байесовськими мережами довіри (БСД) [11]:

$$BN_{O_3} = \langle A, Tab_{O_3} \rangle, \quad (4)$$

де $A = \{a_i\}_{i=1}^{N_A}$ множина дій порушників;

N_A – кількість всіх дій порушників;

Tab_{O3} – множина таблиць ймовірностей кожного з дій a_i з «батьківськими» діями $parents(a_i)$.

Такий підхід дозволяє з більшою точністю визначати ймовірність реалізації. Вузлами БСД в цьому випадку будуть атакуючі дії порушників.

Таблиці умовних ймовірностей описуються наступним чином:

$$Tab_{O3} = \{P(A_1|parents(A_1)), \dots, P(A_n|parents(A_n))\} \quad (5)$$

З дії A_i порушник починає реалізацію загрози. Використовується безумовна ймовірність $P(A_i)$. Компонент моделі загроз об'єкта захисту, що представляє дії порушника, в загальному вигляді включає в себе:

$A = \{a_i\}_{i=1}^{N_A}$ – множина дій порушників, N_A – число всіх дій порушників; F^{YDH} – множина функцій даного компонента.

Дії порушника представляємо таким чином:

$$a_i = \langle aid_i, pur_i, T_{ra}, Y_{max_i}, P_i^B, RE_i \rangle \forall i \in N_A, i \leq N_A, \quad (6)$$

де aid_i – ідентифікатор дії порушника;

$pur_i \in Pur$ – мета реалізації дії порушника;

T_{ra} – час для успішної реалізації дії;

Y_{max_i} – ймовірний збиток системі;

P_i^B – ймовірність виконання порушником даної дії;

$RE_i = \{re_i\}_{i=1}^{N_{re}}$ – рекомендації щодо виявлення, затримки і реагування СЗІ;

N_{re} – число рекомендацій відомих системі.

Ймовірність реалізації загрози ($P(B)$) обчислюється за формулою повної ймовірності події. Це дає більш точні значення показників ймовірності реалізації загрози за певним сценарієм. Сумарний збиток (Y) від реалізації сценарію визначається як сума збитків всіх дій з даного сценарію. Тоді, з урахуванням виразу $R = YP$, ризик від [11]:

$$R = YP(B), \quad (7)$$

Відносна оцінка втрат у разі реалізації i -ої загрози – d_i . Для кожної загрози визначається рівень значимості, що дорівнює добутку можливості реалізації на відносну оцінку утрат:

$$z_i = p_{ri} \times d_i, \quad (8)$$

де z_i – рівень значущості загрози.

Висновки

У зв'язку із зростаючою роллю інформаційних технологій у житті сучасного суспільства, а також через реальності численних загроз з точки зору їх захищеності проблема ІБ вимагає до себе все більшої уваги. Системний характер впливу на ІБ великої сукупності різних обставин призводять до необхідності комплексного підходу щодо вирішення даної проблеми. Особливої уваги в цих умовах потребує оцінка загроз ІБ як необхідна складова комплексного підходу до забезпечення інформаційної безпеки організації.

Зважаючи на те, що прояв загроз ІБ може завдати шкоди будь-яким державним або комерційним структурам. Дослідження загроз ІБ організації доцільно проводити за напрямками, які складаються з трьох блоків: *дії до атаки, під час атаки так і після неї*. При цьому головну увагу слід зосереджувати як на повному переліку загроз, так і передусім на множині актуальних внутрішніх та навмисних загроз ОІД. Оперування низкою притаманних загрозам параметрів дасть можливість визначити ймовірність реалізації кожної загрози, отримати повне уявлення про варіанти її деструктивного впливу та їх наслідки.

Література

1. Хмелевський Р.М. Тези. «Інформаційна безпека, як одна з основ забезпечення ефективності роботи державного управління». Матеріали міжнародної науково-технічної конференції «Сучасні інформаційно-телекомунікаційні технології» Том IV «Сучасні технології інформаційної безпеки» Київ, ДУТ. 17–20 листопада 2015 р. – С.155–158.
2. «Про Стратегію кібербезпеки України». Указ Президента України №96 / 2016 від 27 січня 2016 року. – [Електронний ресурс]. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/287/2015>
3. Кавун С.В. Інформаційна безпека. Навчальний посібник. Ч.1 / С.В. Кавун, В.В. Носов, О.В. Мажай. – Харків: Вид. ХНЕУ, 2008. – 352 с.
4. Вихорев С.В., Кобцев Р.Ю. Как узнать – откуда напасть или откуда исходит угроза безопасности информации // Защита информации. Конфидент, № 2, 2002. С.44–49.
5. Касперский Е. Основные классы угроз в компьютерном сообществе 2003 года, их причины и способы устранения // Информационный бюллетень «Jet Info». № 12 (127)/2003.
6. Классификация угроз Digital Security (Digital Security Classification of Threats). – [Електронний ресурс]. – Режим доступа: <http://www.dsec.ru/products/grif/fulldesc/classification>
7. Кузнецов И.Н. Учебник по информационно-аналитической работе. Информация: сбор, защита, анализ. М.: Изд. Яуза, 2001.
8. Расторгуев С. П. Философия информационной войны. – М.: Вузовская книга, 2001. – 468 с.
9. Christopher Alberts, Audrey Dorofee «OCTAVE Threat Profiles»; Software Engineering Institute, Carnegie Mellon University.
10. Нурдинов Р.А., Батова Т.Н. Подходы и методы обоснования целесообразности выбора средств защиты информации // Современные проблемы науки и образования. – 2013. – № 2.
11. Аверченков В.И. Автоматизация проектирования комплексных систем защиты информации: монография / В.И. Аверченков, М.Ю. Рытов, О.М. Голембиовская – Брянск: БГТУ, 2012. – 139 с.

Надійшла 04.12.2016 р.

Рецензент: д.т.н., проф. Толубко В.Б.