УДК 35.078.3+340.68

Положення про інформаційну безпеку в міжнародних стандартах

Серед проблемних питань в галузі інформаційної безпеки чи не найбільш актуальним є визначення самого поняття “інформаційна безпека”, бо відсутність цієї ключової дефініції обумовлює певну методологічну невизначеність ряду інших положень та термінів означеної галузі.

Можна було б сподіватися, що ситуація дещо зміниться з прийняттям у січні 2007 р. Закону України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки”, у третьому розділі якого визначено: “**інформаційна безпека** – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [7]. На жаль, поява цього офіційного визначення не зменшила кількості дискусій щодо з’ясування ряду положень нормативно-правової бази інформаційної безпеки. Це, зокрема, яскраво ілюструє зміст статей першого номеру журналу „Інформаційна безпека людини, суспільства, держави” [5].

Додаткової гостроти окресленій ситуації надає той факт, що в галузі знань 1701 „Інформаційна безпека” започатковано підготовку фахівців за напрямом 6.170103 „Управління інформаційною безпекою”. Це обумовлює необхідність в обмежений термін узгодити розуміння принципових термінологічних та методичних положень у сфері інформаційної безпеки. З цих позицій видається корисним розгляд і опрацювання матеріалів, в яких акумульовано світовий досвід управління інформаційною безпекою. Мова йде про чинні міжнародні стандарти з інформаційної безпеки, зокрема ті розділи, де здійснюється аналіз та дослідження підходів, понять, визначень, які ще не мають єдиного усталеного сприйняття у вітчизняному нормативно-правовому та навчально-методичному забезпеченні галузі інформаційної безпеки, насамперед в сфері управління інформаційною безпекою.

Таким чином, *метою* статті є дослідження певних суперечливих термінологічних і методологічних положень у сфері інформаційної безпеки, *завданням* – аналіз змісту цих положень в контексті чинних міжнародних стандартів у цій галузі.

В першу чергу до цих стандартів належать британський національний стандарт BS 7799, який було затверджено в 2000 році як перший міжнародний стандарт з управління інформаційною безпекою, серія стандартів ISO/IEC 13335, які у 2003 – 2005 р.р. отримали статус державних стандартів України з управління інформаційною безпекою [2, 3, 4], та новітня серія стандартів з менеджменту інформаційної безпеки ISO/IEC 27000, зокрема стандарт [13] цієї серії.

Перш за все з'ясуємо, який зміст вкладається в термін „інформаційна безпека" у міжнародних стандартах. Так в ISO/IEC 17799 інформаційна безпека визначається як забезпечення конфіденційності, цілісності та доступності інформації. В стандартах ISO/IEC 13335-1 та ISO/IEC 27001 визначення цього терміну більш широке: додається забезпечення таких властивостей інформації як обліковість, достовірність, невідмовність та надійність, а головне, підкреслюється, що стан інформаційної безпеки – це змінна у часі величина, що інтегрує у собі всі наведені вище властивості інформації та залежить від рівнів цих властивостей на даний момент часу. Зміна рівнів обумовлюється непостійністю характеристик та варіюванням кількості діючих зовнішніх і внутрішніх загроз: чим більша кількість загроз і вища їх інтенсивність, тим нижчий (гірший) рівень інформаційної безпеки. Для забезпечення належного рівня інформаційної безпеки створюється система захисту – система інформаційної безпеки (СІБ), найважливішим елементом якої є система управління інформаційною безпекою (СУІБ). Головна задача СУІБ – забезпечити своєчасне та адекватне реагування на інформаційні загрози. Для цього необхідно:

а) контролювати процеси виникнення та розвитку загроз;

б) неперервно оцінювати значущість, суттєвість кожної загрози;

в) трансформувати часткові оцінки значущості та суттєвості загроз в інтегральний показник стану інформаційної безпеки;

г) керуючись інформацією, отриманою за п. а), формувати в складі СІБ сукупність механізмів захисту (методів, процедур, програмно-апаратних засобів);

д) спираючись на поточні дані, отримані за пп. б), в), забезпечувати оптимізацію стану інформаційної безпеки шляхом узгодженого оперативного управління механізмами безпеки.

Розв’язання наведених вище завдань потребує вирішення однієї принципової проблеми – вимірювання рівня значущості (важливості, суттєвості) загроз інформації. При цьому слід враховувати, що хоч загрози можуть бути спрямовані на різні властивості інформації (конфіденційність, цілісність, доступність, надійність тощо), необхідно якимсь чином забезпечити можливість співставлення та порівняння значущості цих загроз, а також обрахування інтегральної оцінки рівня значущості сукупної дії всієї множини загроз. Міжнародні стандарти у якості показника значущості загроз, оцінювання рівня якого забезпечить виконання всіх перелічених вище вимог, рекомендують використовувати ризик загроз, під яким розуміють ймовірну шкоду, що виникає внаслідок реалізації часткової загрози або усієї множини загроз [10]. Саме орієнтація ризику не на фіксацію змін певної властивості інформації, на яку спрямована загроза, а на кінцевий результат, наслідок дії загрози (сукупності загроз) забезпечує застосування ризику як універсального показника рівня небезпеки.

За своєю структурою ризик є добутком ймовірності реалізації загрози та кількісної оцінки шкоди, обумовленої реалізацією цієї загрози [4, 10, 12]. Така структура ризику виключає можливість його прямого вимірювання, тому в деяких стандартах наводяться методики опосередкованого оцінювання ризику, які містять і описи процедур визначення обох структурних складових ризику: ймовірності та шкоди. В процесі оцінювання останньої стикаємося з необхідністю вирішення ще одного принципового питання: в яких межах слід аналізувати і визначати можливі наслідки впливу загроз (тобто шкоду, обумовлену реалізацією загроз). Відповідь на це питання дозволяє виявити різницю між поняттями „інформаційна безпека” та „безпека інформації”.

Останнім двом термінам відповідає ситуація, коли оцінювання шкоди засновано на чисто формальному вимірі рівня змін у блоці інформації, які виникли внаслідок дії загроз. Можна вважати, що цей прийом базується на підході, прийнятому в математичній теорії зв’язку, де втрати інформації внаслідок впливу шумових збурень (загроза) в каналі зв’язку оцінюються шляхом співставлення форми вихідного

повідомлення та повідомлення, отриманого на прийомі (із застосуванням певної кількісної міри виявлених розбіжностей) [9]. Зокрема, при представленні інформації двійковим кодом у разі порушення цілісності інформації внаслідок дії загроз рівень шкоди може бути виміряний кількістю невірно прочитаних бітів інформації. Кількість бітів, не сприйнятих через порушення умов доступу до інформації, визначатиме розмір шкоди, спричиненої внаслідок недостатньої доступності інформації. У разі порушення конфіденційності інформації показником шкоди можна вважати кількість правильно сприйнятих бітів за умов відсутності у отримувача прав санкціонованого доступу до блоку інформації.

У всіх наведених вище прикладах шкода від реалізації загроз визначається шляхом формального обчислення втрат інформації (внаслідок її знищення, спотворення або несанкціонованого отримання), яке ніяк не враховує важливість змісту втраченої інформації та обумовлені цим наслідки (збитки) в соціальній, політичній, економічній, виробничій та інших сферах людської діяльності. Тому побудована в цих випадках система інформаційної безпеки спрямована на захист сприймаємих чисто формально властивостей інформації. Певним підтвердженням цього є наведений в Постанові Кабінету Міністрів України від 20.01.1997 р. № 40 „Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи" термін „безпека інформації", яка визначається як захищеність інформації від несанкціонованих дій (випадкових чи навмисних), що призводять до модифікації, розкриття чи руйнування даних.

На відміну від наведеного формального підходу до оцінювання шкоди, обумовленої реалізацією загроз інформації, в міжнародних стандартах [10, 12, 13] шкода визначається в значно більш широкому розумінні. Так у вступній частині стандарту ISO/IEC 17799 завданням інформаційної безпеки визнається захист інформації „від широкого спектру загроз з метою забезпечення неперервності бізнесу, мінімізації шкоди, максимізації прибутку... і створення сприятливих можливостей бізнесу" [10]. При цьому термін бізнес (англ.„business"), як це зазначається в Примітці 1 пункту *1.1. Загальні положення* стандарту ISO/IEC 27001, слід інтерпретувати як „види діяльності, що є основними для існування організації" [13]. Ще детальніше це аналізується в стандарті ISO/IEC 13335-1 [12]. Тобто українською мовою зазначений

термін business доцільно перекладати як „основна діяльність організації” або словом „справа” (із тим змістом, яке вкладається у нього в словосполученні „власна справа”). Для того, щоб оцінити, як діяльність організації залежить від інформації, а точніше від інформаційно-телекомунікаційних технологій (ІТТ), де використовується ця інформація, слід розглянути наступні питання [12]:

„- які важливі складові діяльності організації не можуть існувати без ІТТ;

- які завдання можуть бути розв’язані тільки за допомогою ІТТ;

- які важливі рішення залежать від конфіденційності, цілісності, доступності, невідмовності, обліковості та аутентичності інформації, що зберігається або обробляється із застосуванням ІТТ, або від того, наскільки ця інформація актуальна;

- яка саме інформація із загального масиву інформації, що зберігається або обробляється, має бути захищеною;

- які наслідки для організації матиме виникнення інциденту безпеки?”.

Відповіді на ці питання дозволяють встановити межі аналізу можливих наслідків від реалізації загроз інформації, підрахувати ризики за окремими загрозами і, врешті-решт, оцінити сукупний ризик від можливої реалізації всієї множини загроз інформації, існуючих для певної конкретної організації. Знайдене кількісне значення сукупного ризику становитиме характеристику рівня інформаційної безпеки даної організації. У разі створення в організації системи захисту (СІБ організації) дієвість цієї системи об’єктивно характеризується різницею сукупних ризиків, оцінених до і після введення захисту, а ефективність захисту – віднесенням цієї різниці до суми загальних витрат на проектування та реалізацію СІБ. Таким чином стає можливою оптимізація СІБ за складністю та вартістю при заданому значенні рівня інформаційної безпеки організації, тобто стає реальним свідоме керування станом захищеності організації в інформаційній сфері.

Слід зазначити, що навіть виокремлення галузі застосування стандартів [2-4, 10, 12, 13] – ІТТ – призводить до появи певних обмежень в сфері аналізу наслідків реалізації інформаційних загроз. Дійсно, за стандартом [12] ІТТ включає в себе інформацію (дані), технічні засоби, програмне забезпечення, систему зв’язку та персонал. Відповідно, саме на ці складові мають бути спрямовані інформаційні

загрози, наслідки яких детально вивчаються та досліджуються на предмет визначення можливої шкоди та ризиків. Однак очевидно, що до складу цих загроз не входять негативні інформаційні впливи, наприклад наклеп чи обмова, які реалізуються через чутки, засоби масової інформації і т.п., бо цілями цих впливів є зовнішні по відношенню до ІТТ об'єкти. Через це наслідки дії таких загроз можуть залишитися поза межами аналізу. Прикладом подібної ситуації є компрометація продукції якої-небудь фірми. Кінцевим результатом цієї компрометації може стати зменшення збуту продукції фірми, що обумовить фінансові збитки, імовірне зменшення інвестицій й т.п..

При цьому інформація, що обробляється на фірмі засобами ІТТ, може зберігати абсолютну недоторканість, а традиційні загрози цілісності, доступності, конфіденційності та іншим властивостям інформації будуть відсутні. Тобто формально не виникає навіть приводу для оцінювання якоїсь шкоди.

Крім того, слід зазначити, що в наведеному вище прикладі негативним інформаційним впливом на діяльність фірми може бути оприлюднення навіть правдивої інформації. Так, якщо фірма використовує технології, що призводять до забруднення оточуючого середовища, то оприлюднення такої інформації призведе до погіршення іміджу фірми і, можливо, інших втрат, в тому числі фінансових, хоча, з точки зору суспільних інтересів, ця інформація має бути відома громадськості. Тобто для фірми в цьому випадку поява правдивої інформації щодо її діяльності буде негативним інформаційним впливом.

Тому при повному аналізі інформаційної безпеки організації треба виходити за межі інформаційної безпеки ІТТ та аналізувати усі можливі інформаційні загрози бізнесу. В цьому випадку фактично єдиним ефективним методом оцінювання можливої шкоди від інформаційних загроз стає ситуаційний аналіз, який дозволяє досліджувати ймовірні наслідки реалізації інформаційних загроз будь-якого походження [1], зокрема без їх прив'язки до ІТТ.

Після викладеного вище варто повернутися до початку статті, де наведено законодавче визначення поняття інформаційної безпеки [7], і зробити спробу його розширеної інтерпретації, виходячи з контексту міжнародних стандартів [2-4, 9, 10, 12, 13]. Для цього перш за все проаналізуємо зміст словосполучення „стан захищеності".

Іменник „захищеність” утворений від дієслова „захистити” (праслов’янське „щитити” – прикрити щитом [8]) і означає огородити від ворожих дій, удару, загрози. Тобто захищеність – це убезпеченість чого-, кого-небудь від загроз. Іменником „стан” визначається ситуація, зумовлена певними обставинами; це характеристика предмета, явища відповідно до певних вимог щодо якості, ступеня готовності [6]. Отже, словосполучення „стан захищеності” слід сприймати як кількісну або якісну ознаку (параметр) рівня захищеності кого-, чого-небудь. Так, для якісної оцінки можливі характеристики захищеності на зразок: мінімальна, задовільна, низька, достатня, абсолютна тощо. Зокрема, згідно зі стандартом Information Security Technology Evaluation Criteria (так звані „Європейські критерії” [11]) маємо три рівні безпеки: базовий, середній, високий; в стандартах [2, 3, 4] використовується поняття базового рівня захисту. Зважаючи, що стан захищеності – це змінна у часі величина, яка залежить від інтенсивності та значущості інформаційних загроз, а також дієвості та ефективності системи захисту, вираз „базовий рівень захисту” означає, що поточний рівень захищеності за умов нормального функціонування систем захисту не повинний бути нижче заданого порогу.

Наступне словосполучення з визначення інформаційної безпеки [7], яке слід інтерпретувати, – це „важливі інтереси людини, суспільства та держави”. В статті 1 Закону України „Про основи національної безпеки України” визначено поняття „національні інтереси” – це „життєво важливі матеріальні, інтелектуальні і духовні цінності українського народу..., визначальні потреби суспільства і держави...”. В стандартах [2-4, 9, 10, 12, 13] використовується поняття „активи”, яке за своїм змістом наближене до поняття „важливі інтереси”. Зокрема, в ДСТУ ISO/IEC 13335-1 визначається: „активи організації – усе, що має цінність для організації”. За аналогією, до активів (взагалі, а не лише організації) можна віднести все, що має цінність для особистості, суспільства, держави. Якщо хтось (щось) потерпає від інформаційних загроз, то саме через ступінь оцінки ушкодженості активів, обумовленої реалізацією загроз, визначається рівень сукупної шкоди та обчислюється сукупний ризик загроз. Відкритим залишається питання: що саме віднести до активів? Відповідь на нього залежить від того, хто (що) становить об’єкт інформаційних загроз (ОІЗ): конкретна особистість, її існування, виробнича та суспільна діяльність; підприємство з системою

ресурсів та технологій, спрямованих на забезпечення певного виду діяльності; будь-які інші організації і т.п. Зауважимо, що встановлення переліку активів не є самоціллю, а лише засобом, елементом процедури визначення рівня шкоди, заподіяної реалізацією інформаційної загрози. В принципі шкоду можна визначити і у інший спосіб, наприклад шляхом прямого експертного оцінювання.

Останнім елементом в інтерпретованому визначенні інформаційної безпеки є перелік можливих інформаційних загроз, який містить два класи загроз: загрози, орієнтовані безпосередньо на інформацію, інформаційні ресурси та складові інформаційної інфраструктури об'єкту захисту (для протидії цим загрозам створюється система захисту інформації, що має гарантувати безпеку інформації на ОІЗ), та інформаційні загрози більш загального характеру, які, зокрема, впливають на елементи середовища, що оточує об'єкт захисту. Для визначення можливої шкоди від загроз другого класу необхідне проведення глибокого аналізу семантики цих загроз, співставлення його результатів із задачами та метою діяльності ОІЗ та визначення найбільш суттєвих наслідків реалізації загроз. Потрібний рівень інформаційної безпеки в цьому випадку забезпечується створенням СІБ.

Отже, в контексті стандартів [2-4, 9, 10, 12, 13] наведене в Законі [7] визначення інформаційної безпеки можна дещо переформулювати: **інформаційна безпека** – це поточний стан захищеності об'єкта від інформаційних загроз, який визначається рівнем шкоди, що може бути заподіяна існуванню, функціонуванню чи діяльності об'єкта в разі реалізації цих загроз. В даному визначенні основний наголос робиться не на захисті життєво важливих інтересів (категорії достатньо аморфної і суб'єктивної через відсутність чіткого законодавчого визначення), а на забезпеченні (збереженні) умов, необхідних для нормального існування, життєдіяльності, функціонування об'єкту захисту, причому загальноприйняті вимоги щодо цих умов визначаються та регулюються низкою документів, зокрема Загальною декларацією прав людини, Конституцією України, Господарським кодексом України тощо.

СПИСОК ЛІТЕРАТУРИ

1. **Архипов О.Є.**, Касперський І.П. Застосування методології передбачення для оцінювання шкоди, заподіяної витоком секретної інформації // Правове,

нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2007. – Вип. 2(15). – С. 13-19.

2. **ДСТУ** ISO/IEC TR 13335-1-2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 1. Концепції й моделі безпеки IT (ISO/IEC TR 13335-1:1996, IDT)
3. **ДСТУ** ISO/IEC TR 13335-2-2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 2. Керування та планування безпеки IT (ISO/IEC TR 13335-2:1997, IDT)
4. **ДСТУ** ISO/IEC TR 13335-3-2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 3. Методи керування захистом IT (ISO/IEC TR 13335-3:1998, IDT)
5. **Інформаційна** безпека людини, суспільства, держави. – 2009. – №1(1). – с.106.
6. **Новий** тлумачний словник української мови. – Т.3 / Укладачі: В.В. Яремко, О.М. Сліпушко. – К.: Аконіт, 2007. – 862 с.
7. **Про** Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки. Закон України від 9 січня 2007 року № 537-V // Відомості Верховної Ради України. – 2007. – № 12. – Ст.102.
8. **Цыганенко Г.П.** Этимологический словарь русского языка. – К.: Рад. шк., 1989. – 511 с.
9. **Шеннон К.** Работы по теории информации и кибернетики. – М.: Изд-во иностр. литер-ры, 1963. – 830 с.
10. **BS** ISO/IEC 17799:2005. Information technology – Security techniques – Code for practice for information security management.
11. **Information** Security Technology Evaluation Criteria. Harmonized Criteria of France – Germany – Netherlands – United Kingdom. – Department of Trade and Industry. London. 1991.
12. **ISO/IEC** 13335-1:2004 Information technology – Security techniques –Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management
13. **ISO/IEC** 27001:2005 Information technology – Security techniques – Information security management systems – Requirements.

Анотація

Про деякі аспекти розуміння сутності інформаційної безпеки
В статті здійснена спроба визначення суті деяких термінологічних і методологічних аспектів інформаційної безпеки, які неоднозначно трактуються у вітчизняних джерелах, шляхом аналізу їх інтерпретації у міжнародних стандартах з керування інформаційною безпекою.
Ключові слова: інформаційна безпека, інформаційні загрози, збитки організації, ризик, безпека інформації.

Про некоторые аспекты понимания сущности информационной безопасности
В статье предпринята попытка определения сути некоторых неоднозначно трактуемых в отечественных источниках терминологических и методологических аспектов информационной безопасности путем анализа их интерпретации в международных стандартах по управлению информационной безопасностью.
Ключевые слова: информационная безопасность, информационные угрозы, ущерб организации, риск, безопасность информации.

About some aspects of the understanding of the information security essence
The authors of the article make an attempt of definition of some terminological and methodological aspects of information security which are ambiguously determined in domestic sources. It was made by the analysis of this aspects interpretation in the international standards of information security management.
Key words: information security, information threats, harm to the organization, risk, information defense.