Архипов О.Є., Архипова Є.О. Особливості розуміння понять «інформаційна безпека» та «безпека інформації» / О.Є. Архипов, Є.О. Архипова // Информационные технологии и безопасность: основы обеспечения информационной безопасности (ИТБ-2014): Материалы XIV международной научно-практической конференции. – К.: ИПРИ НАН Украины, 2014. – С.18-30.

УДК 340.13

Олександр Архипов, доктор технічних наук, професор, НТУУ «КПІ»
Євгенія Архипова, кандидат філософських наук, доцент, НТУУ «КПІ»

ОСОБЛИВОСТІ РОЗУМІННЯ ПОНЯТЬ «ІНФОРМАЦІЙНА БЕЗПЕКА» ТА «БЕЗПЕКА ІНФОРМАЦІЇ»

Анотація. Уточнено зміст поняття «інформаційна безпека», визначено його співвідношення із поняттям «безпека інформації».
Ключові слова: інформаційна безпека, безпека інформації, стандарти з інформаційної безпеки, загрози інформації, шкода від інформаційних загроз.

Аннотация. Уточнено содержание понятия «информационная безопасность», определено его соотношение с понятием «безопасность информации».
Ключевые слова: информационная безопасность, безопасность информации, стандарты по информационной безопасности, угрозы информации, ущерб от информационных угроз.

Summary. Clarified the concept of «information security», defined its relationship to the concept of «information security».
Keywords: information security, information security standards, information threats, harm from information threats.

Постановка проблеми. Цілком закономірним є те, що в сучасному суспільстві, яке часто називають інформаційним, питання, що лежать у площині інформаційної безпеки, викликають підвищену увагу в наукових та професійних колах, а також серед широкої громадськості. Терміни «інформаційна безпека», «безпека інформації», «кібербезпека», «захист інформації» тощо вже досить давно увійшли в широкий обіг, а визначення деяких із них закріплені у міжнародних та вітчизняних нормативно-правових актах. Проте, на жаль, аналіз наукових та правових джерел демонструє відсутність одностайного трактування термінів в сфері інформаційної безпеки, а їх визначення на законодавчому рівні потребує уточнення та ретельного узгодження.

Тому одним із пріоритетних завдань в галузі інформаційної безпеки наразі, на наш погляд, є визначення самого поняття “інформаційна безпека”, бо відсутність однозначного розуміння суспільством цієї ключової дефініції обумовлює методологічну невизначеність ряду інших положень та термінів означеної галузі.

Таким чином, **метою** даної статті є уточнення сутності поняття інформаційної безпеки та з’ясування його співвідношення з терміном «безпека інформації».

Виклад основних положень. У третьому розділі Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки» визначено, що «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» [10].

Але не дивлячись на існування офіційного визначення інформаційної безпеки, а також на досить високий професійний рівень її вивчення, на поточний момент з визначенням поняття " інформаційна безпека " склалася парадоксальна ситуація. З одного боку, термін "

інформаційна безпека" давно відомий і широко використовується в публікаціях, навчальній літературі та законодавчих документах різного рівня, а з іншого боку, в це поняття досі вкладається різний зміст. Так, в навчальному посібнику Шаньгіна В.І. [11, 10] наведено гранично звужене поняття інформаційної безпеки:«захищеність інформації від незаконного ознайомлення, перетворення і знищення, а також захищеність інформаційних ресурсів від впливів, спрямованих на порушення їх працездатності». Тобто в даному випадку під інформаційною безпекою розуміється лише технічна її складова, а діалектично пов'язана з нею соціальна, суб'єктивна складова – захист від негативних інформаційних впливів на свідомість людини – ігнорується.

Зрізом розвитку проблеми інформаційної безпеки в суспільстві можна вважати спеціалізовані конференції та виставки: переважна більшість їх учасників – це компанії, які займаються технічними аспектами інформаційної безпеки, а саме захистом від комп'ютерних вірусів, різноманітними програмно-апаратними рішеннями, комплексними Security-рішеннями.

Часто поняття безпеки інформації та інформаційної безпеки ототожнюються, або ж в одне і те саме поняття в різних джерелах, в тому числі у правових, вкладається різний зміст, що порушує основоположні принципи теорії систем та ускладнює подальший розвиток практичних та теоретичних досліджень в цій сфері.

Певною мірою така термінологічна невизначеність пояснюється тим, що проблематика інформаційної безпеки є дуже складною і багатоаспектною. Надмірна увага до проблем захисту інформації та нехтування іншими аспектами інформаційної безпеки обумовлена процесом збільшення цінності інформації в усіх її проявах, темпи якого невпинно зростають починаючи зсередини XX століття. Дуже швидко у свідомості людей вкоренилося розуміння того, що основним ресурсом сучасного глобалізованого суспільства є інформація, а створені на її основі інформаційні продукти є умовою ефективного функціонування та комфортного існування в даному соціумі. Здатність отримувати, обробляти і використовувати інформацію багато в чому детермінує рівень успішності людини в інформаційному суспільстві, адже інформація сьогодні виступає і специфічним ресурсом, і важливим фактором влади, і основою організації та управління.

У суспільній свідомості інформація почала сприйматися як товар, а тому виникла потреба у його (товару)захисті від неправомірних та/або небажаних посягань. Основними властивостями інформації як об'єкта захисту прийнято вважати доступність, цілісність та конфіденційність. Розширюючи цей перелік, до нього додають такі характеристики, як невідмовність, достовірність, адекватність, актуальність, точність, повнота тощо.

Крім того, часто вітчизняні та російські дослідники запозичують основний зміст визначення терміну «інформаційна безпека» з міжнародних стандартів ISO / IEC з управління та менеджменту інформаційної безпеки, не враховуючи, що словосполучення «Information Security» може перекладатися з англійської як «інформаційна безпека», так і як «безпека інформації». Але оскільки дані стандарти належать до сфери безпеки інформаційних технологій, то і об'єкт захисту в них звужений: це не людина, суспільство чи держава, а інформація та інформаційна інфраструктура.

Таке фрагментарне запозичення ключових термінів з іншомовних джерел без урахування загального контексту документів є, на наш погляд, основною причиною термінологічної плутанини.

З цих позицій видається корисним ґрунтовне опрацювання чинних міжнародних стандартів, в яких акумульовано світовий досвід управління інформаційною безпекою, 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.

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 рр. отримали

статус державних стандартів України з управління інформаційною безпекою [4-6], та серія стандартів з менеджменту інформаційної безпеки ISO/IEC 27000, зокрема стандарт [16] цієї серії.

Перш за все з'ясуємо, який зміст вкладається в термін «Information Security" у міжнародних стандартах. Так в ISO/IEC 17799 цим терміном визначається 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 «Information Security» – 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) стан «Information Security».

Для побудови ефективної системи інформаційної безпеки необхідно виміряти рівень 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 всієї множини загроз. Міжнародні стандарти у якості показника значущості загроз рекомендують використовувати ризик загроз, під яким розуміють ймовірну шкоду, що виникає внаслідок реалізації часткової загрози або усієї множини загроз [13]. Орієнтація ризику на кінцевий результат, наслідок дії загрози (сукупності загроз), а не на фіксацію змін певної властивості інформації, на яку спрямована загроза, забезпечує використання ризику як універсального показника рівня небезпеки.

За своєю структурою ризик є добутком ймовірності реалізації загрози та кількісної оцінки шкоди, обумовленої реалізацією цієї загрози [6; 13; 15]. В процесі оцінювання шкоди стикаємося з необхідністю вирішення ще одного принципового питання: в яких межах слід аналізувати і визначати можливі наслідки впливу загроз? Відповідь на це питання дозволяє виявити різницю між поняттями «інформаційна безпека» та «безпека інформації».

Зокрема терміну «безпека інформації» відповідає ситуація, коли оцінювання шкоди засновано на чисто формальному обрахуванні змін у блоці інформації, які виникли внаслідок реалізації 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 кількісного співставлення форми вихідного повідомлення та повідомлення, отриманого на прийомі [12]. Зокрема, при представленні інформації двійковим кодом у разі порушення цілісності інформації 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 порушення цілісності 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 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. У цьому випадку маємо справу із порушенням «стану інформації, у якому забезпечується збереження визначених політикою безпеки властивостей інформації», тобто із **безпекою інформації**, як вона зафіксована у [7].

На відміну від наведеного формального підходу до оцінювання шкоди, обумовленої реалізацією загроз інформації, в міжнародних стандартах [13; 15; 16] шкода визначається значно ширше. 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» [13]. При цьому термін бізнес (англ. «business») слід інтерпретувати як «види діяльності, що є основними для існування організації» [16]. Після з'ясування того, яким чином діяльність організації залежить від використовуваних нею інформаційно-телекомунікаційних технологій, можна 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 для певної організації [1]. Знайдене кількісне значення сукупного ризику становитиме характеристику рівня інформаційної безпеки даної організації. У разі створення в організації системи інформаційної безпеки (СІБ), дієвість цієї системи об'єктивно характеризується різницею сукупних ризиків, оцінених до і після введення захисту від інформаційних загроз, 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 [4-6; 13; 15; 16] – інформаційно-телекомунікаційні технології (ІТТ), – призводить до появи певних обмежень в сфері аналізу наслідків реалізації інформаційних загроз. Дійсно, за стандартом [15] 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 [2], зокрема без їх прив'язки до ІТТ.

Після викладеного вище варто повернутися до початку статті, де наведено законодавче визначення поняття інформаційної безпеки [10], і зробити спробу його розширеної інтерпретації, виходячи з контексту міжнародних стандартів [4-6; 13; 15; 16]. Для цього перш за все проаналізуємо зміст словосполучення «стан захищеності». Захищеність – це убезпеченість чого-, кого-небудь від загроз. Іменник «стан» визначає характеристику 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» [14]) маємо три рівні безпеки: базовий, середній, високий; в стандартах [4-6] 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 [10], яке слід інтерпретувати, – це «важливі інтереси людини, суспільства та держави». В статті 1 Закону України «Про основи національної безпеки України» [9] визначено поняття «національні інтереси» – це «життєво важливі матеріальні, інтелектуальні і духовні цінності українського народу..., визначальні потреби суспільства і держави...». В стандартах [4-6; 13; 15; 16] 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 [4-6; 13; 15; 16] наведене в Законі [10] 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 через:

а) використання неповної , несвоєчасної і недостовірної інформації;

б)здійснення негативного інформаційного впливу;

в) протиправного застосування інформаційних технологій;

г) несанкціонованого розповсюдження і використання інформації , порушення її цілісності, конфіденційності та доступності.

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.

Висновки. У підсумку зазначимо, що поняття «безпека інформації» та «інформаційна безпека» безумовно пов'язані між собою. Оскільки зміст поняття «безпека» визначається вибором об'єкта захисту, то якщо цим об'єктом виступає власне інформація , тоді поняття «інформаційна безпека» і «безпека інформації» синонімічні. Але якщо в якості об'єкта / суб'єкта захисту розглядається деякий учасник інформаційних відносин, то слово «інформаційна» в даному терміні вказує на напрямок діяльності, яка може заподіяти шкоду об'єкту / суб'єкту захисту. У цьому випадку поняття «інформаційна безпека» слід трактувати як стан захищеності деякого об'єкта / суб'єкта від загроз інформаційного характеру. Таким чином, поняття «інформаційна безпека» слід вважати родовим по відношенню до поняття «безпека інформації», а їх взаємозамінність є неприпустимою.

На жаль, в Україні коло питань інформаційної безпеки практично звужено до проблем безпеки інформації, і основна увага громадськості сконцентрована переважно на проблемі захисту інформації.

У той же час в умовах надмірної насиченості інформаційного середовища вкрай гостро стоїть проблема захисту людини від деструктивного інформаційного впливу, який здатний призвести до формування викривленої моделі сприйняття інформації, віртуалізації оточуючого середовища, порушення механізмів культурної та соціальної ідентичності, деформації суб’єктності [3].

Дослідження питань захисту від негативних інформаційних впливів представлені в основному або описами окремих ситуацій і сценаріїв, або у вигляді вельми абстрагованої узагальненої теорії. З огляду на це, актуальними напрямками подальших досліджень в галузі інформаційної безпеки є наукова розробка загальнотеоретичних, правових та методологічних аспектів цієї проблеми, у тому числі вироблення світоглядної інтерпретації філософської концепції інформаційної безпеки.

Використана література

1. Архипов А.Е. Практические аспекты оценивания рисков реализации угроз в информационных системах // Інтелектуальні системи прийняття рішень і проблеми обчислювального інтелекту (ISDMCI’2014, Залізний порт, 28 – 31 травня 2014 р.): Матеріали міжнародної наукової конференції. – Херсон: ХНТУ, 2014. – С.194-196.
2. 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.
3. Архипова Е.А. Социальная составляющая информационной безопасности / Е.А. Архипова // Безпека інформації: Наук.-практ. журнал. – 2012. – Том 18, № 2 (2012) – С.28-32.
4. ДСТУ ISO/IEC TR 13335-1-2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 1. Концепції й моделі безпеки ІТ (ISO/IEC TR 13335-1:1996, IDT).
5. ДСТУ ISO/IEC TR 13335-2-2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 2. Керування та планування безпеки ІТ (ISO/IEC TR 13335-2:1997, IDT).
6. ДСТУ ISO/IEC TR 13335-3-2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Частина 3. Методи керування захистом ІТ (ISO/IEC TR 13335-3:1998, IDT).
7. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. – (Чинний від 1999.04.28). – К.: ДСТСЗІ СБУ, 1999. – №22.

8. Новий тлумачний словник української мови. – Т.3 / Укладачі: В.В. Яремко, О.М. Сліпушко. – К.: Аконіт, 2007. – 862 с.
9. Про основи національної безпеки: Закон України від 19.06.03 р. № 537-V // Відомості Верховної Ради України. – 2003. – N 39. – Ст.351).
10. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.07 р. № 537-V // Відомості Верховної Ради України. – 2007. – № 12. – Ст.102.
11. Шаньгин В.И. Информационная безопасность компьютерных систем и сетей: Учеб.пособие / В.И. Шаньгин. – М.: ИД "Форум": ИНФРА-М, 2008. – 416 с.
12. Шеннон К. Работы по теории информации и кибернетики. – М.: Изд-во иностр. литер-ры, 1963. – 830 с.
13. BS ISO/IEC 17799:2005. Information technology – Security techniques – Code for practice for information security management.
14. Information Security Technology Evaluation Criteria. Harmonized Criteria of France – Germany – Netherlands – United Kingdom. – Department of Trade and Industry. London. 1991.
15. 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.
16. ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements.