

Технічна та соціальна складові інформаційної безпеки

В сучасному суспільстві, в тому числі і в нашій країні, давно вже звикли до словосполучення «інформаційна безпека», яке зайняло своє місце серед інших видових щодо поняття «безпека» термінів (економічна, екологічна, психологічна, національна безпека тощо). Проте, незважаючи на достатньо міцне вкорінення терміну «інформаційна безпека» в суспільному дискурсі, далеко не всі з тих, хто до нього звертається, розуміють глибину та складність проблемної області, до якої він відноситься.

Пересічне уявлення про інформаційну безпеку формується під впливом того факту, що інформація в сучасному суспільстві усвідомлюється як важливий ресурс, який здатний принести його господарю певні прибутки, а тому цей ресурс потребує захисту від сторонніх посягань та випадкового ушкодження. Звідси й випливає проблема захисту інформації, що розуміється як забезпечення її основних властивостей: конфіденційності, цілісності та доступності.

Надамо коротку характеристику означених властивостей інформації.

Доступність – це можливість використання інформації щоразу, коли в цьому виникає необхідність. Інформація стає недоступною в разі її блокування або знищення.

Цілісність інформації (повнота і точність) порушується при фальсифікації, несанкціонованій модифікації, викривленні тощо.

Конфіденційність – властивість інформації не підлягати розголосу. Безпека конфіденційної інформації порушується внаслідок її несанкціонованого копіювання, викрадення або втрати.

Об'єктом захисту тут виступає інформація, механізми, організаційні структури і форми, в яких існують інформаційні потоки. Тобто у даному випадку ми маємо справу з безпекою інформації, тоді як поняття інформаційної безпеки цим змістом не вичерпується.

Поняття "безпека інформації" та "інформаційна безпека" безумовно пов'язані між собою. Оскільки зміст поняття "безпека" визначається вибором об'єкту захисту, то якщо цим об'єктом виступає власне інформація, то поняття "інформаційна безпека" і "безпека інформації" синонімічні. Але якщо в якості об'єкта / суб'єкта захисту розглядається деякий суб'єкт 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" є родовим по відношенню до поняття "безпека інформації", а їх взаємозамінність є неприпустимою.

У сучасних умовах поряд із задачею **захисту інформації** надзвичайно актуальною стає проблема **захисту від інформації**, яка фокусується на колі проблем, що гуртуються навколо людини та суспільства. Інформація циркулює в рамках соціо-технічної системи, найменш захищеними ланками якої виступають не механізми і технології, що забезпечують зберігання, розповсюдження та обробку інформації, а люди.

Таким чином, інформаційну безпеку ми визначаємо як стан захищеності свідомості і буття соціальних суб'єктів від інформаційних загроз, який визначається рівнем реальної чи потенційної шкоди, заподіяної внаслідок деструктивного інформаційного впливу або порушення безпеки інформації. Ще раз підкреслимо діалектичну сутність інформації: вона може виступати і об'єктом захисту, і засобом, інструментом впливу на свідомість та буття соціальних систем, причому цей вплив може носити як позитивний, так і негативний характер.

Отже, в загальному випадку серед загроз інформаційній безпеці можна виділити наступні:

а) порушення безпеки інформації, тобто загрози об'єктивній складовій інформаційного середовища;

б) порушення безпеки об'єкта / суб'єкта захисту внаслідок деструктивних інформаційних впливів, інформаційної дезорієнтації, тобто загрози суб'єктивній складовій інформаційного середовища.

Ці групи загроз інформаційній безпеці пов'язані між собою. Загрози об'єктивній складовій інформаційного середовища, що описані нами трохи вище, безумовно, впливають на суб'єктивну складову, адже людині набагато важче прийняти рішення, сформувані свою власну позицію, адекватну реальному стану речей, в умовах інформаційної нестачі, викривлення та фальсифікації інформації. Деструктивний інформаційний вплив на індивідуальну та суспільну свідомість здійснюється саме через канали розповсюдження і передачі інформації.

Постійне ускладнення суспільного життя, перевантаженість інформацією у поєднанні з розгортанням інформаційної нерівності сприяє формуванню у людей стереотипної, багато в чому міфологізованої свідомості, знижує здатність до адекватного сприйняття нової інформації.

З одного боку, існування феномену інформаційної нерівності у її первинному, технічному вияві – обмеженості деяких суб'єктів інформаційних відносин у доступі до сучасних інформаційно-комунікаційних технологій – дає змогу іншим суб'єктам, можливості яких в цьому плані більші, контролювати та відбирати інформацію, що надходить кінцевим споживачам.

Кожна людина в процесі свого розвитку отримує певні навички та знання, напрацьовує деякі поведінкові схеми та алгоритми, формує власні переконання, вподобання та пріоритети. Зрозуміло, що все це здійснюється на основі інформації, яка поступає до людини із зовнішнього світу. Отже, під впливом контрольованого потоку інформації у людини цілком можливо поступово сформувати так само контрольовану, наперед задану «інформаційними модераторами» свідомість, разом із відповідними навичками, знанням та вподобаннями.

З іншого боку, так само, як і всі інші вміння та навички, вміння працювати з інформацією, орієнтуватися в її безкінечному та суперечливому

різноманітні, оцінювати її достовірність, приймати на її основі рішення, – всі вони формуються на основі попереднього практичного досвіду. Традиційний, перевірений часом спосіб навчання полягає у поступовому переході від простого до складного, від базових, елементарних навичок до більш професійних та специфічних. І якщо людина не отримала елементарних знань, то більш складні знання та навички стають недосяжними для неї. Це дозволяє нам говорити про соціальну, ментальну складову інформаційної нерівності, яка впливає на відповідну складову інформаційної безпеки і полягає у нездатності людини самостійно орієнтуватися в інформаційному просторі, зокрема здійснювати пошук, верифікацію, аналіз отриманої інформації, а також приймати рішення на її основі та синтезувати нову інформацію.

Наостанок зазначимо, що для інформаційної безпеки людини та суспільства величезне значення має і той факт, що, крім відсутності обмеження у доступі до інформації та наявності відповідних інформаційних навичок, для адекватного її сприйняття необхідно докласти досить суттєвих зусиль, а бажання їх докласти виникає далеко не у всіх та далеко не завжди. Зорієнтуватися у безлічі інформаційних повідомлень, які представлені у різних видах та форматах, доповнюють або суперечать один одному дійсно складно – це потребує певних навичок, вільного часу та відповідного бажання. Саме тому забезпечення інформаційної безпеки не є виключною прерогативою державних інституцій, а частково лягає на плечі самих споживачів інформації.