УДК: 351/354: 004.6

Архипова Є.О.
Національний технічний університет України
«Київський політехнічний інститут»

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ: МЕТОДИЧНІ АСПЕКТИ

Визначені основні характеристики інформаційної безпеки та безпеки інформації, показані їх відмінності та спільні риси. Наведена характеристика основних властивостей інформації як суб'єкту захисту. Акцентовано увагу на неприпустимості зведення інформаційної безпеки д о безпеки інформації. Показані наслідки негативного інформаційного впливу на свідомість людини.

ВСТУП

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). Питання інформаційної безпеки розробляються у різних площинах: як складова державної (національної) безпеки (О. Андрєєва, І. Арістова, В. Горбулін, О. Данільян, О. Дзьобань, В. Конах, , М. Кормич, О. Ніколаєв, Г. Ситник та ін..), як одна з умов успішної реалізації демократичних реформ, становлення громадянського суспільства та гуманізації державної влади (С. Алексєєв, М. Богданова, Л. Євдоченко,Д. А. Керімов, А. Колодій, Н. Оніщенко та інші). Психологічні аспекти інформаційної безпеки вивчалися Г. Грачовим, Е.Доценком, К. Каландаровим, С. Кара-Мурзою, С. Некляєвим, В. Остроуховим, В. Полевим, Г. Почепцовим та іншими.

Можна відзначити, що дискусії стосовно проблем інформаційної безпеки давно вже вийшли за межі кабінетів науковців, спеціалістів із захисту інформації та ведення інформаційних операцій, перетворившись на одну із популярних тем у засобах масової інформації, що безумовно засвідчує її актуальність. 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. З огляду на це видається корисним розкрити сутнісні характеристики інформаційної безпеки та провести певну демаркаційну лінію між поняттями «захист інформації» та «інформаційна безпека».

ОСНОВНІ РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Пересічне уявлення про інформаційну безпеку формується під впливом того факту, що інформація в сучасному суспільстві усвідомлюється як важливий ресурс, здатний принести його господарю певні прибутки, а тому цей ресурс потребує захисту від сторонніх посягань та випадкового ушкодження. Звідси й випливає проблема захисту інформації – специфічного ресурсу, який може втратити свою цінність, не лише від пошкодження, знищення чи викрадення, але і від копіювання чи розмноження. При цьому інформаційна безпека редукується до безпеки інформації.

В сучасній науковій та професійній літературі, а також в нормативно-правових джерелах під захистом інформації розуміється забезпечення її основних властивостей:

цілісності, доступності та конфіденційності. 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) передбачає захищеність від будь-яких «несанкціонованих дій щодо інформації в *[інформаційно-телекомунікаційній]* системі, внаслідок яких змінюється її вміст» [1, Ст.1]. Таким чином, цілісність інформації може порушуватися внаслідок фальсифікації, несанкціонованої модифікації, викривлення, підміни тощо.

Конфіденційність – властивість інформації, доступ до якої на законних підставах обмежено фізичною або юридичною особою, не підлягати розголосу. Конфіденційність інформації порушується внаслідок її несанкціонованого копіювання, розголосу, викрадення або втрати.

Використання сукупності методів і засобів захисту інформації, що забезпечують її цілісність, конфіденційність та доступність, дозволяють досягти прийнятного рівня безпеки інформації. До речі, більшість визначень самого терміну «захист інформації» (від англійського «data protection») чітко вказує на те, що мова йде не про всю інформацію, що циркулює в соціумі, а лише про ту, що зберігається та обробляється в інформаційно-телекомунікаційних системах [2; 6-8].

Об'єктом захисту у цьому випадку виступає саме інформація (дані), що циркулюють в ІТС, механізми, організаційні структури і форми, в яких існують інформаційні потоки. Якщо розглядати проблему безпеки інформації в широкому плані, на рівні соціуму, а не ІТС, то стане зрозуміло, що інформація циркулює в рамках соціально-технічної системи: всі ІТС функціонують для виконання певних задач, визначених володільцями інформації, від яких зазвичай залежить і порядок доступу до інформації, і перелік користувачів, яким він буде наданий, і їх повноваження щодо інформації в системі [1]. Володільці, користувачі, власники ІТС мають доступ до інформації в системі, а, як відомо, вплив соціальних факторів на систему є найменш передбачуваним та прогнозованим. З огляду на це ми вважаємо, що найменш вразливою ланкою соціально-технічної системи виступають не механізми і технології, що забезпечують зберігання, розповсюдження та обробку інформації, а людина.

Беручи до уваги зазначене вище, можна стверджувати, що методика вирішення проблем захисту інформації в установах та організаціях має передбачати впровадження організаційних заходів захисту, в тому числі встановлення правил розмежування доступу та розробку корпоративної політики безпеки з обов'язковим доведенням їх до відома співробітників та регулярними перевірками дотримання встановлених правил. Звичайно, методика захисту інформації передбачає використання й технічних (наприклад, антивіруси, фаєрволи, маршрутизатори тощо), інженерних (пожежна та охоронна сигналізації, сейфи, інші фізичні обмеження доступу) та криптографічних (шифрування, використання електронного цифрового підпису) засобів. Тим не менше розробка та впровадження організаційних заходів у поєднанні із розвитком загальної інформаційної культури співробітників, на наш погляд, є визначальною, адже жодне шифрування та фаєрволи не допоможуть, якщо, наприклад, паролі доступу до персональних комп'ютерів подібні до «123zxc», відомі всім співробітникам відділу та/або зберігаються на клаптику паперу під клавіатурою, а флешки з важливою інформацією вільно передаються іншим особам.

Тепер зупинимося на трактуванні поняття «інформаційна безпека». Як вже зазначалося [4], часто інформаційну безпеку неправомірно редукують до безпеки інформації:

приклади таких визначень можна побачити в навчально-методичних посібниках з даного профілю, в науковій та монографічній літературі, різних інформаційних ресурсах. Візьмемо для прикладу одне з типових визначень наведене, зокрема, у Вікіпедії: «Інформаційна безпека – це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення». Далі слідує примітка, в якій вказано, що поняття «інформаційна безпека» не обмежується безпекою технічних інформаційних систем чи безпекою інформації у чисельному чи електронному вигляді, а стосується усіх аспектів захисту даних чи інформації незалежно від форми, у якій вони перебувають.

Тобто, за логікою авторів, захищати від інформаційної небезпеки слід не лише інформацію в інформаційно-комп'ютерних мережах, але й, наприклад, паперові бази даних, листівки, роздруківки, картотеки, інформація на магнітних носіях, оптичних дисках тощо. Заувага цілком слушна, але тим не менше, автор даної статті під об'єктом захисту розуміє виключно інформацію та/або дані, тобто звужує поняття інформаційної безпеки до безпеки інформації. Він не вбачає неповноти своїх суджень, коли в тій самій статті наводить визначення інформаційної безпеки, взяте із законодавчої бази України [2], де зазначається. що забезпечення інформаційної безпеки передбачає, серед іншого, запобігання «нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив».

Поняття "безпека інформації" та "інформаційна безпека" безумовно пов'язані між собою. Зауважимо, що 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, як це часто буває, 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'єкту / суб'єкту 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.

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 на людину або через 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;

б) порушення безпеки об'єкта/суб'єкта захисту внаслідок деструктивних інформаційних впливів, інформаційної дезорієнтації.

Ці групи загроз інформаційній безпеці пов'язані між собою. Загрози природного або штучного характеру, внаслідок реалізації яких відбувається знищення, модифікація, викрадення, блокування інформації в ІТС, безумовно, впливають і на людину, адже врешті-решт вона є користувачем (принаймні – потенційним), власником чи розпорядником цієї інформації, а тому несанкціоновані дії з інформацією наносять їй певну шкоду.

З іншого боку, негативні інформаційні впливи, що діють безпосередньо на людину, здатні призвести до зміни її свідомості, поведінки та навіть об'єктивних умов її існування. Все це за певних обставин може спричинити свідоме чи несвідоме викривлення інформації, представленої в засобах масової інформації, інтернет-просторі та ІТС.

Виявити ознаки інформаційної агресії в інформаційному просторі дозволяє застосування контент-аналізу – методу якісно-кількісного дослідження змісту текстів різної природи, що дозволяє виявити або зафіксувати зміну фактів та тенденцій, які відображені в цьому тексті. Контент-аналіз дозволяє врахувати соціальний контекст представленої інформації, що є суттєвою перевагою цього методу під час спроби виявити або зафіксувати факти інформаційної агресії.

Деструктивний інформаційний вплив може здійснюватися цілеспрямовано, або ж виявитися випадковим наслідком включення людини у несприятливе інформаційне середовище. Як правило, наслідки випадкового негативного інформаційний впливу мають менш виражений характер та не так сильно травмують свідомість людини, ніж цілеспрямований вплив, але тривале перебування в несприятливих інформаційних умовах також здатне нанести людині досить серйозну травму. Так, перевантаження людини будь-якою, в тому числі позитивною інформацією чи емоціями може викликати загальмованість сприйняття, уповільнення реакції, погану концентрацію уваги, провали в пам'яті тощо. Все більше науковців відзначають, що активне поширення ІКТ в суспільстві супроводжується накопиченням надлишкової інформації, яка перевантажує інформаційних простір, ускладнює пошук потрібної, своєчасної та якісної інформації, створює невідповідність попиту і пропозиції інформації [3; 5; 8]. У зв'язку з цим доречно згадати таке поняття, як «гіпертрофована інформація», яке визначається як «надмірна кількість інформації, що вбиває інформацію, надмірна кількість комунікації, що вбиває комунікацію» [5].

Якщо ж негативний інформаційний вплив здійснюється свідомо, то його наслідки можуть спостерігатися значно швидше та у більш вираженій формі. 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. Людині набагато важче прийняти рішення, сформувати 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, тому недаремно контроль над ЗМІ був і є одним із основних факторів успішності будь-якої військової, політичної, економічної чи соціальної кампанії.

Концентрація засобів масової інформації у власності окремих суб'єктів інформаційних відносин загострює проблему інформаційної нерівності. 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 різноманітті, 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. І 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.

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

Підсумовуючи викладене вище 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 докладати 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, часу та відповідного бажання. Держава не в силах повністю контролювати власний інформаційний простір, тим більше, що такий тотальний контроль матиме явні ознаки інформаційної монополії та диктатури Саме тому забезпечення інформаційної безпеки не є прерогативою державних інституцій, а частково має бути покладено на плечі самих споживачів інформації, які повинні усвідомлювати зону своєї відповідальності та знати та використовувати способи захисту від негативних інформаційних впливів.

Список використаних джерел

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Електронний ресурс]. Чинний від 05.07.94; в редакції від 19.04.2014 / Офіційний портал Верховної Ради України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

2. Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки». Чинний від 9.01.2007. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/537-16

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. 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: Материалы

международной научной конференции ИТБ-2014. – К.: ИПРИ НАН Украины, 2014. – С.18-30.

5. Даниленко С. Тенденції розвитку електронних ЗМІ // Нові медіа. – К. : СПД Рудницька А., 2009. – С. 38–41.

6. Захист інформації [Ел.ресурс] // Матеріали сайту ТОВ «Софтлайн-ІТ». – Режим доступу: http://www.softline.kiev.ua/ua/our-services-ua/192-information-security.html

7. Woulds J. A Practical Guide to the Data Protection Act. London, The Constitution Unit, 2004. – 32 p.

8. The Guide to Data Protection. Version 2.1. – 6 February 2015; Information Commissioner's Office. – 2015. Available at: https://ico.org.uk/media/for-organisations/documents/1607/the_guide_to_data_protection.pdf

References

1. On protection of information in telecommunication systems, Ofitsiinyi portal Verkhovnoi Rady Ukrainy, 1994. Available at: http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (In Ukrainian).

2. On the General Principles of Information Society Development in Ukraine for 2007-2015, Ofitsiinyi portal Verkhovnoi Rady Ukrainy, 2007. Available at: http://zakon4.rada.gov.ua/laws/show/537-16 (In Ukrainian).

3. Arhipova E.A. Social'naja sostavljajushhaja informacionnoj bezopasnosti [The social component of information security], Bezpeka informacii, 2012, vol. 18, no.2, pp. 28-32.

4. Arkhypov O.Ye., Arkhypova Ye.O. Osoblyvosti rozuminnia poniat «informatsiina bezpeka» ta «bezpeka informatsii» [Features an understanding of the concepts of «information security» and «safety of information»], Ynformatsyonnыe tekhnolohyy y bezopasnost: osnovы obespechenyia ynformatsyonnoi bezopasnosty: Materyalы mezhdunarodnoi nauchnoi konferentsyy YTB-2014, 2014, pp 18-30.

5. Danylenko S. Tendentsii rozvytku elektronnykh ZMI [Trends in electronic media], New media,, 2009, pp.38-41.

6. Information security. Portal of Softline-IT. Available at: http://www.softline.kiev.ua/ua/our-services-ua/192-information-security.html. (In Ukrainian).

7. Woulds J. A Practical Guide to the Data Protection Act. London, The Constitution Unit, 2004. 32 p.

8. The Guide to Data Protection. Version 2.1. – 6 February 2015; Information Commissioner's Office, 2015. Available at: https://ico.org.uk/media/for-organisations/documents/1607/ the_guide_to_data_protection.pdf

Архипова Е.А. Обеспечение информационной безопасности и защиты информации: методические аспекты

В статье раскрываются сущностные характеристики информационной безопасности, проводится демаркационная линия между понятиями «защита информации», «безопасность информации» и «информационная безопасность». Раскрыты некоторые методические аспекты обеспечения информационной безопасности и защиты информации.

Показан генезис формирования понятия «информационная безопасность». Раскрыты основные свойства информации как объекта защиты: доступность, целостность, конфиденциальность. Проанализировано определение термина «защита информации».

Очерчены некоторые способы решения проблем защиты информации в учреждениях и организациях, в частности рекомендовано предусмотреть внедрение организационных мер защиты информации, в том числе установление правил разграничения доступа и разработку корпоративной политики безопасности с обязательным доведением их до сведения сотрудников и регулярными проверками соблюдения установленных правил.

Акцентировано внимание на недопустимости сведения информационной безопасности к безопасности информации. Подчеркнуто, что обеспечение информационной безопасности включает в себя безопасность информации и защиту от негативных информационных воздействий.

Указано, что контент-анализ как метод качественно-количественного анализа текстов позволяет выявить признаки информационной агрессии в информационном пространстве. Перечислены последствия негативного информационного влияния на сознание человека.

Ключевые слова: информационная безопасность, защита информации, безопасность информации, методы обеспечения информационной безопасности.

Arkhypova Ye.O. Ensuring of information security and protection of information: methodological aspects

The article describes the essential characteristics of information security, carried out the line of demarcation between the concepts of “Protection of information”, “Data Protection” and “Information security”. Discloses certain methodological aspects of information security and information protection.

Showed genesis of the formation of the concept of “information security”. Outlined the main properties of information as an object of protection: the availability, integrity and confidentiality. Analyzed the definition of “Data Protection.”

Outlined some ways to solve the problems of information security in institutions and organizations, in particular recommended to provide for the implementation of organizational measures of information security, including the establishment of access control rules and the development of corporate security policy with compulsory bringing them to the attention of employees and regular checks of compliance.

Accentuated the inadmissibility of simplify the information security to the security of information. It was stressed that information security includes security of information and protection from adverse effects of information.

It is indicated that the content analysis as a method of qualitative and quantitative analysis of the texts reveals signs of aggression information in the information space. Listed impact of negative information effect on human consciousness.

Keywords: information security, information security, information security, information security practices.