

УДК 331.45 331.46

Шмирко В.І.¹, Ліпіліна О.С.²

¹ канд. техн. наук, доц. ЗНТУ

² студ. гр. М-214м ЗНТУ

ОСНОВНІ НАПРЯМКИ ДІЯЛЬНОСТІ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

З метою аналізу впливу інформації на особистість та оцінки ступеню небезпеки цього впливу проведено інформаційний пошук та проаналізовано матеріали, що представлені в Інтернеті. Для більш легкого, доступного і повного сприйняття проблеми інформація була систематизована та візуалізована у вигляді блок-схеми (рис.1). В основних напрямках забезпечення безпеки можна виділити три блока: основним є нормативно-правове забезпечення, також передбачається ряд організаційних та технічних заходів, система страхування ризиків.

Інформаційний захист регламентується нормативними документами: «Про Державну службу спеціального зв'язку та захисту інформації України», «Про основні засади забезпечення кібербезпеки України», Указом Президента України затверджено «Положення про Національний координаційний

центр кібербезпеки» та «Стратегію кібербезпеки України». З метою забезпечення протидії кіберзлочинності, завчасного інформування населення про появу нових кіберзлочинів, для систематизування та аналізу кіберінцидентів, здійснення оперативно-розшукової діяльності була створена Кіберполіція. Вона запобігає зламу баз даних, платіжних систем, поширенню вірусів та крадіжок інформації із, наприклад, держреєстрів з персональними даними громадян тощо. Також кіберполіція України створила сервіс для генерації паролів, які не зможуть зламати хакери.

Організаційно-технічне забезпечення (рис.1) спрямовано на захист інформаційних ресурсів, тобто не допускає витік, знищення даних, несанкціонований доступ до інформації та модифікації тощо. Режимне й оперативне забезпечення відкривають безпосередній доступ особам та організаціям до закритої захищеної інформації. За допомогою технічних засобів забезпечується захист від побічного електромагнітного випромінювання і наведень, захист від несанкціонованого доступу до інформації, криптографічний захист інформації. Організаційним забезпеченням є проведення єдиної державної політики захисту інформації.

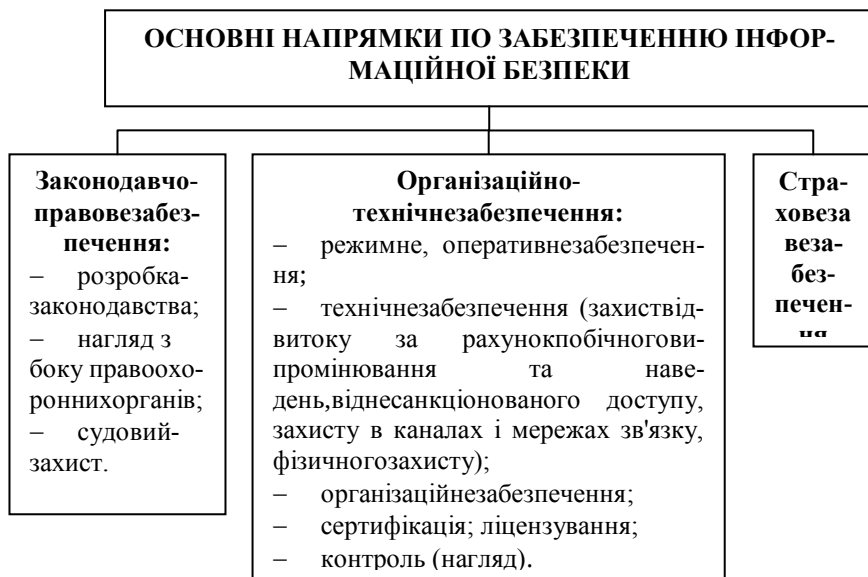


Рисунок 1 – Основні напрямки діяльності щодо забезпечення інформаційної безпеки.

Також держава контролює здійснення обов'язкової сертифікації та ліцензування діяльності в галузі захисту інформації, зокрема виробництва товарів та надання послуг у галузі технічного і криптографічного захисту інформації відповідно до ліцензійних умов провадження господарської діяльності з надання послуг у галузі технічного захисту.

Страхування інформаційних ризиків (рис.1) стосується лише недержавних установ. Це гостре та актуальне питання, яке нажаль, перебуває на низькому рівні, а його доцільність недооцінюється. Наприклад, страховий захист інформації дозволяє економічно стабілізувати ситуацію (матеріально компенсувати загублену інформацію), знизити психоемоційні навантаження на користувача в зв'язку з втратою важливої інформації.

Страхування також дає можливість стабілізувати розвиток суспільства, підприємства, організації, державних структур, страхових компаній. Залучення коштів страхових компаній дасть можливість розробляти більш захищене програмне забезпечення та практично підтримувати розробку технічних принципів забезпечення інформаційної безпеки та сприяти технічному прогресу.