

СЕКЦІЯ «БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ»

УДК 331.45 331.46

Шмирко В.І.¹, Бочарова А.О.²

¹ канд. техн. наук, доц. НУ «Запорізька політехніка»

² студ. гр. Ю-310м НУ «Запорізька політехніка»

ОСНОВНІ НАПРЯМКИ ПО ЗАБЕЗПЕЧЕННЮ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Останнім часом зазначається глобальне розповсюдження інформаційного середовища. Інформація швидко поширюється серед значної кількості людей, незалежно від країни, її рівня розвитку і економічно-матеріального рівня. Нова інформаційна реальність, з одного боку, розширює спектр можливостей людини як користувача інформації, з іншого – впливає на формування (або зміну) її світогляду, особистісних цінностей. Перенасиченість та непорядкованість інформаційного простору призводить до психічного та фізичного напруження користувачів інформації.

Зазначається широке різноманіття засобів доступу до інформації (інтернет, засоби масової інформації: телевізори, газети, книги, журнали, тощо). Прогресивним при цьому є свобода вибору джерела інформації та вільний доступ до світового інформаційного поля. Користувачі мають можливість самостійно оцінювати яка інформація і в якому об'ємі може бути корисною в розважальному або їх професійному розвитку. Крім того, інформація впливає на інтелектуальний стан людини, на її психо-емоційний стан, загальний стереотип поведінки, а також на взаємовідносини з іншими людьми.

Таке розповсюдження інформаційного поля, крім позитиву, нажаль, має і негативні моменти. В першу чергу, це пов'язано з тим, що інформація може бути і недостовірною, а сформована при цьому точка зору може кординально відрізняється від думки оточуючих. Це, в свою чергу, призводить до непорозуміння, конфліктів і сутичок в професійному колективі і, навіть, у сімейному колі. З розвитком електронної платіжної системи, збільшилась і кількість шахрайств, не добродійних дій з боку окремих осіб. Тому, засвоєння сталих навичок якісного аналізу різноманітної інформації має дуже велике значення для користувачів.

З метою аналізу впливу інформації на особистість та оцінки ступеню небезпеки цього впливу та більш легкого, доступного і повного сприйняття проблеми, інформацію систематизували у вигляді блок-схеми, що наведено в

таблиці 1. В основних напрямках забезпечення безпеки можна виділити три блока, основним із яких є нормативно-правове забезпечення. Інформаційний захист регламентується нормативними документами, наприклад, «Про Державну службу спеціального зв'язку та захисту інформації 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, діяльність якої відповідає вимогам нормативно-правових документів:

– «Про основні засади забезпечення кібербезпеки України»; Указом Президента України затверджено «Положення про Національний координаційний центр кібербезпеки» та «Стратегію кібербезпеки України».

Вона запобігає зламу баз даних, платіжних систем, поширенню вірусів та крадіжок інформації із, наприклад, держреєстрів з персональними даними громадян тощо.

Таблиця 1 – Основні напрямки діяльності щодо забезпечення інформаційної безпеки.

Основні напрямки діяльності щодо забезпечення інформаційної безпеки.		
Законодавчо-правове забезпечення	Організаційно-технічне забезпечення	Страхове забезпечення
Розробка законодавства та нагляд з боку правоохоронних органів	Режимне, оперативне забезпечення	
Судовий захист	Технічне забезпечення (захист від витоку за рахунок побічного випромінювання та наведень, від несанкціонованого доступу, захисту в каналах і мережах зв'язку, фізичного захисту)	
	Організаційне забезпечення	
	Сертифікація, ліцензування, контроль (нагляд)	

Також кіберполіція України створила сервіс для генерації паролів, які не зможуть зламати хакери

Організаційно-технічне забезпечення (табл.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.

Страхування 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.

Таким чином, небезпеки пов'язані з розповсюдженням інформаційного поля часто залишаються недооціненими, а їх узагальнення дозволить користувачеві краще орієнтуватись серед значної кількості загроз, їх швидко аналізувати, та розробляти ефективні методи профілактики.