3) недостатній сукупний попит;

4) інфляція викликає скорочення капітальних вкладень, зниження реальних доходів населення, що викликає збільшення пропозиції зі зменшенням попиту на робочу силу;

5) співвідношення цін на фактори виробництва, яке веде до переважання працездатних технологій;

6) сезонні коливання виробництва, що викликають зміни у попиті на робочу силу;

7) науково-технічний прогрес, що збільшує диспропорції між попитом і пропозицією робочої сили [1].

Рівень безробіття – кількісний показник, який визначається як відношення кількості безробітних до загальної чисельності економічно активного працездатного населення країни (регіону, соціальної групи), та вимірюється у відсотках.

Аналізуючи представлений графік ми можемо бачити, що відсоткове відношення рівня безробіття уже на протязі декількох років не змінюється.

Виникнення безробіття тягне за собою такі наслідки: посилення соціальної напруги; зростання кількості психічних захворювань; посилення соціальної диференціації; загострення криміногенної ситуації; падіння трудової активності; скорочення податкових надходжень; зменшення ВНП; падіння життєвого рівня населення; зростання витрат на допомоги безробітнім.

Потрібно відмітити загрозливу тенденцію того, що у зв'язку з погіршенням економічної ситуації в країні з роботи звільняються в першу чергу жінки і ті працівники, у яких низький рівень кваліфікації та недостатній рівень практичної роботи. Саме вони в останню чергу і приймаються на роботу. Гостро стоїть питання про безробіття серед молоді: близько третини безробітних – це молоді люди у віці до 30 років.

Зважаючи на вищевикладене можна зазначити, що пріоритетними напрямами діяльності керівництва держави повинно бути розробка заходів щодо розвитку економіки, а отже і зменшенню безробіття.

1. Ярорва Л.Г. Аналіз рівня безробіття в Україні та напрямки його подолання // Глобальні та національні проблеми економіки. Миколаївський національний університет імені В.О.Сухомлинського. Електронне наукове фахове видання. № 10, 2016. С. 752–755.

2. Жиляк Н.В. Деякі аспекти самовизначення безробітних у процесі профпереорієнтації. Актуальні проблеми розвитку організаційної та економічної психології в Україні. Кам'янець-Подільський: Національний університет імені І. Огієнка, 2015. С. 86–87.

Степан Марія Дмитрівна
курсант факультету
економіко-правової безпеки

Науковий керівник:
Паршин Юрій Іванович
професор кафедри
фінансово-економічної безпеки
Дніпропетровського державного
університету внутрішніх справ,
доктор економічних наук, доцент

ПРОБЛЕМИ ОЦІНКИ СУЧАСНОГО РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

Інформаційна безпека (IS) призначена для захисту конфіденційності, цілісності та доступності даних комп'ютерної системи від осіб із шкідливими намірами. Конфіденційність, цілісність та доступність іноді називають Тріадою безпеки інформації ЦРУ. Ця тріада перетворилася на те, що прийнято називати гексадом Паркера, що включає конфіденційність, володіння (або контроль), цілісність, справжність, доступність та корисність.

Інформаційна безпека обробляє управління ризиками. Все, що може бути ризиком або загрозою для тієї ж самої інформаційної безпеки. Слід зберігати конфіденційну інформацію - її не можна змінювати, змінювати чи передавати без дозволу. Наприклад, повідомлення може бути змінено під час передачі тим, хто перехоплює його до того, як воно дійде до призначеного одержувача. Хороші інструменти криптографії можуть допомогти

пом'якшити цю загрозу безпеці.

Цифрові підписи, які нещодавно були запроваджені нашою державою, можуть покращити інформаційну безпеку за рахунок посилення процесів автентичності та спонукання осіб до підтвердження своєї особи, перш ніж вони можуть отримати доступ до комп'ютерних даних.

На сьогодні у сучасному суспільстві інформація стає найбільш важливою цінністю, а індустрія отримання, обробки і захисту інформації – провідною галуззю діяльності, куди з кожним роком вкладають все більш значні капітали. Вже найближчим часом саме розвиток інформаційної сфери, рівень інформаційної безпеки будуть визначати політичну й економічну роль окремих держав на світовій арені[1].

Взагалі аналітики зазначають, що стратегія національної безпеки України актуальними загрозами національній безпеці України в інформаційній сфері визначає ведення інформаційної війни проти України та відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства. Основними напрями державної політики щодо забезпечення інформаційної безпеки зазначає забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії; створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них; протидія інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства; розробка і реалізація скоординованої інформаційної політики органів державної влади та ін. [2].

Встановлення кібернетичної безпеки не може покладатися лише на технічні засоби. Належна увага повинна приділятися також кінцевим користувачам та адміністраторам систем ІКТ, працівникам з розробки, підрядникам державних контрактів, аудиторам та менеджерам. Недостатня інформація про безпеку систем ІКТ створює серйозні ризики. Відсутність кваліфікованого та обізнаного персоналу та подальша освіта підвищують вразливість та збитки.

Взагалі, щоб бути корисною політика безпеки повинна не лише визначати потребу в безпеці (наприклад, для конфіденційності дані повинні бути розкриті лише уповноваженим особам), але й вирішувати коло обставин, за яких цю потребу необхідно задовольнити, та пов'язані з ними експлуатаційні стандарти. Без другої частини політика безпеки настільки загальна, що є марною (хоча друга частина може бути реалізована через процедури та стандарти, встановлені для реалізації політики). У будь-яких конкретних обставинах деякі загрози є більш імовірними, ніж інші, і розсудливий розробник політики безпеки повинен оцінити загрози, призначити рівень занепокоєння для кожної людини та викласти політику, щодо якої можна протистояти загрозам. Наприклад, до недавнього часу більшість політик щодо безпеки не вимагали задоволення потреб безпеки в умовах вірусної атаки, тому що ця форма нападу була рідкісною і не була широко вивчена. Оскільки віруси переросли від гіпотетичної до звичайної загрози, виникла необхідність переосмислити таку політику щодо методів розповсюдження та придбання програмного забезпечення. Наслідком цього процесу є вибір керівництвом рівня залишкового ризику, з яким він буде жити, такого рівня, який залежить від організацій.

Тобто для того щоб мінімізувати атаки на інформаційну безпеку потрібно бездоганно відпрацювати стратегію щодо її забезпечення .та збереження конфіденційності інформації, щоб при цьому унеможливити її витік

---

1. Про рішення Ради національної безпеки і оборони України від 29.12.2016 «Про Доктрину інформаційної безпеки України»: Указ Президента України 25.02.2017 № 47/2017 // База даних «Законодавство України/ ВР України. URL: http://zakon2.rada.gov.ua/laws/show/47/2017 (дата звернення 01.03.18).

2. Про рішення Ради національної безпеки і оборони України від 06.05.2015 «Про Стратегію національної безпеки України»: Указ Президента України від 26.05.2015 р. № 287/2015 // База даних «Законодавство України/ ВР України. URL: http://zakon5.rada.gov.ua/laws/show/287/2015 (дата звернення 01.03.18).