- 29% підприємств малого та середнього бізнесу використовували стандартні засоби упередження витоку інформації у 2017 році, що навіть менше за 2016 рік і становить 39%;
- середній період, упродовж якого хакери діють непоміченими (сплячими) у мережі до моменту їх виявлення, складає понад 200 днів;
- близько 70% кібератак використовують комбінацію так званих тактик «фішінгу» та «хакінгу», а також ураження не лише безпосередніх жертв, а й опосередкованих;
- близько 74% керівників служб інформаційної безпеки мали справу з викраденням персональних даних щодо працівників підприємств, установ чи компаній;
- 38% підприємств впевнені, що справді готові до захисту проти кібератак підвищеного рівня складності;
- більше 81% опитаних жертв витоку даних заявили, що ні система, ні служба з управління інформаційною безпекою не є самодостатніми з точки зору можливості виявлення інформаційного витоку. Натомість вони є залежними від третіх (зовнішніх щодо підприємства чи компанії) осіб. І це незважаючи на загальновідомий факт, згідно з яким внутрішнє виявлення витоків займає в середньому 14,5 днів, тоді як зовнішнє виявлення сягає в середньому 154 днів.

З урахуванням наявних та потенційних загроз національній інформаційній безпеці, у *Доктрині інформаційної безпеки* України визначені пріоритети державної політики в інформаційній сфері за такими напрямами: забезпечення інформаційної безпеки; забезпечення захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію; відкритість та прозорість держави перед громадянами; формування позитивного міжнародного іміджу України. Важливою перевагою нової Доктрини є представлений у ній механізм практичної реалізації, відповідно до якого Рада національної безпеки і оборони згідно з Конституцією України та у встановленому законом порядку має здійснювати координацію діяльності органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері [3]. При цьому чітко розподілено функції Кабінету Міністрів України, міністерств, інших органів виконавчої влади відповідно до їх компетенції у цій сфері.

Через те, що в законодавстві України поняття національної інформаційної безпеки використовується досить широко, а проблема його точного визначення так і не вирішена, ускладнюється створення цілісної системи нормативно-правового забезпечення цієї надважливої сфери національної безпеки в цілому. Узагальнюючи вище викладене, можна зробити висновок, що нині нормативно-правові засади національної інформаційної безпеки в цілому мають досить розвинутий характер, прийняті законодавчі та нормативні акти загалом відповідають міжнародним стандартам і принципам. Водночас вони потребують подальшого вдосконалення для усунення суперечностей та заповнення прогалин, у тому числі відображення місця і завдань державної статистики як важливої складової системи національної інформаційної безпеки підприємств.

1. Cisco 2016. Annual Security Report. (2016). Cisco. Retrieved from http://signalpartners.fi /wp-content/uploads/2016/01/Cisco-securityreport-2016.pdf 2. 2015 Global Cybersecurity Status Repor. (2015, January). ISACA International. Retrieved from https://www.isaca.org/cyber/ Documents/2015-Global-Cybersecurity-Status-Report-Data-Sheet_ mkt_Eng_0115.pdf 3. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII, станом на 01.01.2017 р. URL: http://zakon5.rada.gov.ua/laws/show/ 2657-12 (дата звернення: 17.06.2017).

Хухра Юрій
Науковий керівник – д.е.н., проф. Я.Я. Пушак

УПРАВЛІННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЮ ДІЯЛЬНІСТЮ ОРГАНІВ ПУБЛІЧНОГО УПРАВЛІННЯ

Сьогодні в усьому світі відбувається інформаційно-технологічна революція. Серед основних тенденцій розвитку суспільства на сучасному етапі слід відзначити процес глобалізації щодо інформатизації практично всіх сфер діяльності. При цьому особливо важливим є запровадження інформаційного забезпечення в державному управлінні, і, зокрема, розробка та впровадження наукового підходу до нього.

Інформаційне забезпечення – це динамічна система одержання, оцінки, зберігання та переробки даних, створена з метою вироблення управлінських рішень [1]. Його можна розглядати і як процес забезпечення інформацією, і як сукупність форм документів, нормативної бази та реалізованих рішень щодо обсягів, розміщення та форм існування інформації, яка використовується в інформаційній системі у процесі її функціонування.

Зміст інформаційного забезпечення складають наступні етапи: постановка завдань відповідних інформаційних зв'язків і цілей інформування; створення фонду відомостей, банку даних; обробка інформації, її систематизація, внаслідок чого відомості стають придатними для подальшого використання; визначення найоптимальнішого режиму використання усіх форм і засобів поширення (обміну) інформації, застосування найраціональніших з них; надання (поширення) інформації за допомогою спеціальних форм і засобів (повідомлення засобів масової інформації, публічні виступи, оприлюднення правових актів та ін.).

На сьогодні, в процесі інформаційного забезпечення органів державної влади продовжують широко використовуватись традиційні джерела інтелектуальної інформації.

Це стосується, наприклад, розвитку системи електронного урядування, яка виступає засобом, що забезпечує інформаційну взаємодію органів виконавчої влади між собою, з громадянами та юридичними особами на основі сучасних інформаційних технологій. Ця інформаційна взаємодія включає надання інформаційних та адміністративних послуг і на неї покладається сприяння ефективності державного управління шляхом інноваційних перетворень в сфері інформаційного забезпечення органів державної влади [2]. Останнє передбачає: 1. налагодження інформаційних комунікацій між суб'єктами державної влади всіх рівнів, створення централізованих баз даних з технологіями розподіленої обробки даних для забезпечення електронного документообігу в усіх державних органах та установах; 2. забезпечення надання державними органами повного спектру інформаційних послуг електронними засобами всім категоріям громадян у доступній та зручній формі, без часових та просторових обмежень; 3. сприяння розвитку електронного ринку товарів і послуг для забезпечення державних замовлень, організації тендерів, ефективності управління виробництвом та реалізацією товарів і послуг з метою підвищення конкурентоспроможності вітчизняних виробників на міжнародному ринку; 4. впровадження електронної демократії як форми забезпечення прозорості, довіри у відносинах між державою і громадянами, приватним бізнесом, громадськими організаціями та інституціями; 5. відкритості державного управління для громадського й суспільного обговорення, контролю та ініціатив; 6. підвищення якості життя громадян через удосконалення надання соціальних послуг, системи охорони здоров'я, забезпечення гарантій правової, екологічної та особистої безпеки, розширення можливостей для освіти; 7. Впровадження системи електронного голосування як форми забезпечення прозорості виборчого процесу, зворотного зв'язку відносин виборець-депутат та контролю за діяльністю депутатів з боку виборців.

В контексті цього, основною вимогою до системи інформаційного забезпечення органів державної влади, особливо в умовах упровадження електронного урядування, є те, що вона повинна мати відкритий характер і забезпечувати інтерактивну взаємодію між підрозділами всередині окремої державної установи, між органами державної влади та місцевого самоврядування по вертикалі й по горизонталі, між органами влади та громадянами й підприємствами.

Інтегрована інформаційна система має забезпечити ефективну роботу органів державної влади завдяки удосконаленню їх інформаційно-аналітичних систем та використанню компонентів, що реалізують інтеграцію їх діяльності, а саме: телекомунікаційне середовище, інтегровану систему електронного документообігу, інтегровану систему управління інформаційними ресурсами, систему управління розподіленими технологіями аналітичних обчислень тощо.

1. Чубенко Л.М. Аналіз підходів до побудови інформаційного забезпечення [Електронний ресурс]. – Режим доступу: http://khnu.km.ua/root/kaf/ksm/Chubenko.doc 2. Про схвалення Концепції розвитку електронного урядування в Україні: Розпорядження Кабінету Міністрів України від 13.12.2010 № 2250-р [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2250-2010-р

Цапулич Анастасія
Науковий керівник – д.е.н., проф. О. О. Другов

ВИРІШАЛЬНЕ ЗНАЧЕННЯ ЛІДЕРСТВА ДЛЯ ФОРМУВАННЯ ТА РЕАЛІЗАЦІЇ СТРАТЕГІЇ УКРАЇНИ В ГАЛУЗІ БУДІВНИЦТВА

Лідерство відіграє важливу роль у формулюванні та реалізації стратегій держави, воно розглядається як зв'язок, який пов'язує процес стратегічного управління з баченням країни [1]. Проект Стратегії сталого розвитку України до 2030 року визначає стратегічні напрями довгострокового розвитку України. Стратегічне бачення сталого розвитку України ґрунтується на забезпеченні національних інтересів. Операційна ціль 4.3. включає в себе завдання, яке передбачає поліпшення до 2030 року житлових умов всіх громадян України, зокрема молодих сімей, багатодітних сімей, фахівців з дефіцитними професіями.

Вирішальне значення лідерських ролей для формування та реалізації стратегії, спрямованої на створення інклюзивних, безпечних, життєстійких та збалансованих населених пунктів мають наступні риси:

1. Лідер повинен забезпечувати впровадження інновацій у процесі стратегічного управління будівництвом.

2. Лідерство передбачає людину-аналітика: у процесі стратегічного управління відповідальність лідера полягає у аналізі ситуації, знаходженні розривів між поточним та бажаним станом.

3. Лідер повинен дбати про кожен аспект, який забезпечує ефективність в будівельній галузі.

4. Відповідальність лідера полягає у наданні всіх необхідних ресурсів для ефективної роботи будівельної галузі.

5. Лідер як аналітик ризиків: лідери сканують середовище в якому працюють, для того, щоб виявити ключові можливості, ризики та зміни.

Отже, лідером у даній ситуації може виступати очільник області, району, міста, громади або Держархбудінспекції.