Тлумак Ольга
Науковий керівник – к.е.н., доц. О.Л. Перхач

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА: СУЧАСНІ ВИКЛИКИ ТА ЗАГРОЗИ

Інформаційний світ набуває стрімкого розвитку. Важко уявити, що те, що колись починалося як невелика кількість великих комп'ютерів у 1970-х роках, перетворилося на мільярди підключених пристроїв з персональних комп'ютерів, мобільних телефонів та пристроїв Інтернету речей. І все ж, поява персональних обчислень пов'язана з ціною додаткових ризиків для безпеки як у повсякденному житті, так і для бізнесу. Так само ризик для підприємств, пов'язаних із мережевою кібератакою, зростає експоненціально. Загрози можуть виникнути в будь-якій точці Інтернету, де є потенційна слабкість, якою хакери можуть скористатись або через фішинг-повідомлення електронної пошти, підробку в мережах, або, навіть, пошкоджене обладнання. Зі збільшенням кількості пристроїв збільшується ризик загроз витоку комерційної та конфіденційної інформації підприємства.

Додаткові ризики для інформаційної безпеки також зросли з поширенням хмарних обчислень. В опитуванні корпоративних хмарних обчислень IDG виявив, що 28% усіх підприємств будуть покладатися на приватні хмари як частину своєї IT-інфраструктури. Приблизно 32% будуть використовувати громадський простір або гібридну модель хмарних обчислень. Аналіз ринку хмарних обчислень Cisco показав, що 83% всього трафіку центрів обробки даних буде засновано у хмарі найближчим часом [1]. Це збільшення, що поєднується з додатковими збільшеннями витрат, зазначеними у звіті Forrester Research [1], ще більше збільшить потребу в посиленні заходів кібербезпеки в наступні роки. Така статистика пов'язана з проблемою національної інформаційної безпеки від початку створення держави. Адже, служби статистики створювалися при державних структурах, які відповідальні за національну та інформаційну безпеку.

Загалом, інформаційну безпеку можна визначити як захист даних, якими володіє підприємство чи особа від загроз та / або ризику. Сутність безпеки в цілому можна окреслити як якість або стан безпеки, тобто позбавлення від шкоди [2]. У більш оперативному розумінні «безпека» передбачає вживання заходів для забезпечення безпеки країни, людей, цінних речей тощо, від необґрунтовані дії інших [2]. Тому, метою безпеки є захист від ворогів, тобто тих, хто завдасть шкоди, навмисно чи іншим чином. На думку Вайтмена і Маторда (Whitman and Mattor) (2005), інформаційна безпека – це захист інформації та її критичних елементів, включаючи системи та обладнання, які використовують, зберігають та передають цю інформацію. Інформаційна безпека – це сукупність технологій, стандартів, політики та практик управління, які застосовуються до інформації для її збереження.

Отже, під поняттям «безпека» ми розуміємо насамперед розроблення плану дій спрямованого для захисту від зовнішнього та внутрішнього впливу на функціонування певної системи, а «інформаційна безпека» – це комплекс заходів, призначений для захисту конфіденційності, доступності, цілісності даних, а також цифрової інформації, яка циркулює внутрішніми каналами системи від внутрішніх і зовнішніх, шкідливих та випадкових загроз.

Інформаційна безпека виконує такі важливі функції для підприємства:

- забезпечує безпечну роботу програми, реалізованої в системах інформаційних технологій будь-якого підприємства;
- здійснює захист даних, які підприємство збирає та використовує;
- захищає технологічні активи, що використовуються на підприємстві;
- захищає здатність підприємства функціонувати.

Однією із цілей інформаційної безпеки є захист даних, які підприємство збирає та використовує. Якщо інформація залишається незахищеною, до них може отримати доступ будь-хто. Якщо інформація потрапить в чужі руки, вона може зруйнувати життя, бізнес, а також може бути використана для заподіяння шкоди. Програми інформаційної безпеки забезпечують захист відповідної інформації як за діловими, так і юридичними вимогами, вживши заходів щодо захисту даних підприємства. Крім того, такі заходи покликані забезпечити збереження конфіденційності, комерційних таємниць та запобігання крадіжці інформації.

На підприємстві інформація є важливим комерційним активом. Це вимагає створення відповідної системи її захисту, що важливо в умовах бізнесу, де інформація наражається на все більшу кількість та різноманітність загроз і вразливих місць. Нанесення збитків, таких як зловмисний код, злом комп'ютера та відмова у службових атаках, стають все більш поширеними, амбітними та складнішими. Таким чином, впровадивши засади інформаційної безпеки на підприємстві, дозволить захистити технологічні активи, фінансові операції, комерційну та конфіденційну інформацію.

Так, К. Корнелл (один із фундаторів американської компанії Swimlane, завданням якої є посилення здатності підприємств та урядових структур, забезпечити власну інформаційну безпеку) узагальнив і опублікував ключові статистичні факти щодо інформаційної безпеки, які одночасно підкреслюють як вагомість самої проблематики, так і значні виклики для суспільства у цій сфері [2]:

- понад 169 млн. персональних записів були наражені на небезпеку через витік інформації із 781 джерела фінансового, ділового, освітнього, урядового та медичного секторів;
- середня загальна вартість кожного втраченого, пошкодженого чи викраденого запису, який містить конфіденційну та важливу інформацію, склала 154 дол. США;
- випадки інформаційних атак зросли на 38% порівняно з попереднім роком (2016р.);

- 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.).