ОСНОВНІ АСПЕКТИ КІБЕРБЕЗПЕКИ

Федик О.І.,
здобувач вищої освіти
спеціальності 071 «Облік і оподаткування»,
Миколаївський національний аграрний університет

У сучасному світі все більше виробництв і послуг спираються на інформаційні технології. Виробництво і постачання енергії, очищення і постачання питної води, керування транспортом, освітлення міст, зв'язку, доступ людей до інформації, охорона здоров'я, оплата товарів і послуг. Ми залежимо від безперервності та коректності функціювання комп'ютерних систем об’єктів критичної інфраструктури, і атаки з боку та засобами кіберпростору на такі системи спричиняють реальні загрози для безпеки людей і суспільства. Законом України «Про основні засади забезпечення кібербезпеки України» поняття кібербезпеки визначено як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [1], проте дія цього Закону України не поширюється на відносини та послуги, пов’язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах, соціальних мережах, приватних електронних інформаційних ресурсах в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси).

Чому кібербезпека важлива? Із збільшенням кількості користувачів, пристроїв і програм на сучасному підприємстві, у поєднанні зі збільшенням потоку даних, більша частина яких є конфіденційною, значення кібербезпеки продовжує зростати. Зростаючий обсяг і витонченість кіберзловмисників і методів атак посилюють проблему ще більше. Спецслужбу з кібербезпеки можуть представляти фахівці з організації інформаційної безпеки та проведення тестування на проникнення, інспектори з організації захисту секретної інформації, аналітики проектів із кібербезпеки, системні адміністратори, адміністратори комп’ютерних мереж, менеджери систем з інформаційної безпеки, аналітики систем забезпечення кібербезпеки [2].

Сферу кібербезпеки можна розбити на кілька різних розділів, координація яких всередині організації є вирішальною для успіху програми кібербезпеки. Ці розділи включають наступне: безпека інформації або даних, безпека мережі, аварійне відновлення/планування безперервності бізнесу, оперативна безпека, хмарна безпека, безпека критичної інфраструктури, фізична безпека, освіта кінцевих користувачів [3].

Одним з найбільш проблемних елементів кібербезпеки є розвиток ризиків безпеки. З появою нових технологій і використанням технологій по-новому або по-різному, розвиваються нові шляхи атаки. Не відставати від цих частих змін і прогресу атак, а також оновлювати методи захисту від них може бути складно. Проблеми включають забезпечення постійного оновлення всіх елементів кібербезпеки для захисту від потенційних вразливостей. Це може бути

особливо важко для невеликих організацій без персоналу або внутрішніх ресурсів. Значення кібербезпеки зростає. По суті, наше суспільство більш технологічно залежне, ніж будь-коли раніше, і немає жодних ознак того, що ця тенденція сповільниться. Витоки даних, які можуть призвести до викрадення особистих даних, тепер публічно публікуються в акаунтах у соціальних мережах. Конфіденційна інформація, як-от номери соціального страхування, дані кредитної картки та дані банківського рахунку, тепер зберігається в хмарних службах зберігання, як-от Dropbox або Google Drive. Крадіжка інформації є найдорожчим і найбільш швидкозростаючим сегментом кіберзлочинності. Значною мірою зумовлено збільшенням доступу до Інтернету ідентифікаційної інформації через хмарні сервіси.

Але це не єдина мета. Промислові засоби контролю, які керують електромережами та іншою інфраструктурою, можуть бути порушені або знищені. І крадіжка особистих даних — не єдина мета, кібератаки можуть мати на меті порушити цілісність даних (знищити або змінити дані), щоб викликати недовіру до організації чи уряду.

На жаль, кіберзлочинність постійно вдосконалюється і йде в ногу з технологіями. Це ускладнює виявлення та протидію зазначеним протиправним діям. Тому варто усвідомити, що проблема кібербезпеки – це проблема не лише загальнодержавного рівня, а кожного окремо взятого підприємства. Таким чином, на кожному підприємстві повинна бути створена програма визначених дій, спрямованих на створення кіберзахисту облікової інформації, сфера застосування якого поширюється на людські ресурси і не обмежується винятково технологічними аспектами.

Бібліографічний список

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII.
2. Шевченко А.С., Самойлов І.В., Пономарьов О.А., Науменко О.Г. Аналіз застосування штучних нейронних мереж у задачах виявлення кіберзагроз.
3. Трофіменко О. Г. Кібербезпека України: аналіз сучасного стану / О. Г. Трофіменко, Ю. В. Прокоп, Н. І. Логінова, О. В. Задерейко // Захист інформації. Том 21. - 2019. - № 3. - С. 150-157.

Науковий керівник
Вишневська Ольга Миколаївна,
д-р екон. наук, професор,
декан обліково-фінансового факультету, МНАУ