Федюк А. В., студентка групи 68,
Брудько О. Л.,
викладач вищої категорії кафедри професійної освіти
Київський професійно-педагогічний коледж імені Антона Макаренка

ПИТАННЯ КОМПЮТЕРНОЇ КІБЕРБЕЗПЕКИ У СВІТІ ЮРИСПРУДЕНЦІЇ

Згідно з результатами досліджень, майже всі юридичні фірми мають відкриті критичні прогалини на ПК і серверах, половина – на мережевому обладнанні. 65% юрфірм не мають навіть мінімальної системи захисту, 60% уразливі для дій інсайдерів, а 70% – не захищені від зовнішніх загроз. Причинами цього є відсутність шифрування даних, процесів забезпечення безпеки і реагування на інциденти; відкриті права доступу; з усіх засобів захисту в основному присутні тільки антивірус і слабкі паролі [1]. На практиці для юридичної фірми або адвокатського об'єднання це означає: високу ймовірність злому; моментальну доступність конфіденційної інформації при втраті або виїмці пристрою, на якій вона зберігається; неможливість відстеження дій інсайдерів; неможливість дізнатися і відреагувати на кібератаку. Для побудови фундаменту правильної та надійної стратегії кібербезпеки юридичній компанії необхідно врахувати ряд аспектів, що допоможуть вберегтися хоча б на мінімальному, початковому рівні кібератак, а у разі вже наявного факту такої атаки вийти ситуації з найменшими втратами [2].

Є дві міжнародні, офіційно визнані експертами плани-стратегії, які потрібно розробити кожній юридичній компанії, що турбується про свою кібербезпеку. Перша – це стратегія безперервності бізнесу (англ. Business Continuity Planning), друга – стратегія аварійного відновлення (англ. Disaster Recovery Plan). Перша – це комплексний стратегічний ряд організаційних заходів, спрямованих на зниження ризиків переривання бізнес-процесів і мінімізацію негативних наслідків у разі збоїв IT-інфраструктури. Друга – стратегія повного розуміння, як потрібно реагувати на стихійне лихо або іншу надзвичайну подію, які можуть вплинути на інформаційні системи, та мінімізувати негативний вплив на діяльність компанії.

План-стратегія – це внутрішній документ компанії, який буде виз-начати кроки і дії, які необхідно вчинити у випадку кібератаки. Розроб-ка такого плану має бути процесом щоденним та динамічним, оскільки способи кібератак постійно змінюються, а отже, план також має змінюватись та відповідно підлаштовуватись [2].

Як показали масштабні кібератаки в Україні 27 червня 2017 року, вправні хакери можуть зламати будь-яку систему, незважаючи на масштаб компанії та її ресурси. І тут критично важливо саме вчасно вия-вити пролом у системі. Ґрунтовний аналіз кібератаки може бути здійснений лише тоді, коли відомо, як і за яких умов вона відбулася, який обсяг даних було скомпрометовано тощо. Відповіді на ці питання можуть допомогти вибудувати правильну позицію захисту та повідомлення для клієнтів, дані яких були викрадені. Важливим фактором є те, що у випадку атаки на юридичний софт 65% інформації, до якої отримують доступ хакери, належить клієнтам компанії. Юристам слід врахувати, як вирішувати проблему з персональними даними, та прописати ці моменти у договорі про надання юридичних послуг [3].

9 травня 2018 року вступив у силу ЗУ «Про основні засади забезпечення кібербезпеки України», що створює засади національної системи кібербезпеки як сукупності політичних, соціальних, економічних та інформаційних відносин разом із організаційно-адміністративними та техніко-технологічними заходами державного і приватного секторів та громадянського суспільства. З'являлися такі терміни, як *кібербезпека, кіберзагроза, кіберпростір, кіберінцидент, кібершпигунство, кібертероризм* тощо.

За кібербезпеку в межах своїх повноважень відповідальні міністерства, місцеві держадміністрації, органи місцевого самоврядування, правоохоронні органи, розвідка і контррозвідка, суб'єкти оперативно-розшукової діяльності, ЗСУ, Нацбанк, підприємства, які належать до об'єктів критичної інфраструктури, підприємства і громадяни, які працюють у сфері національних інформаційних ресурсів, інформаційних електронних послуг [4]. На офіційному сайті CERT-UA кожен користувач або компанія може знайти найпростіші рекомендації стосовно кібер-безпеки.

Проте кожному варто пам'ятати, що кібербезпека починається з персональної відповідальності кожного та дотримання найпростіших правил кібергігієни [5].

Список використаних джерел

1. ЗУ «Про Стратегію кібербезпеки України».
2. APT Notes/data – відкритий реєстр матеріалів на тему відомих кібератак з боку угрупувань типу розвинена стала загроза.
3. ЗУ «Про основні засади забезпечення кібербезпекиУкраїни».
4. ТОП-10 основних правил кібербезпеки. URL: https://uteka.ua/ua/publication/news-14-delovye-novosti-36-top10-osnovnyx-pravil-kiberbezopasnosti
5. Кібергігієна. URL: https://cert.gov.ua/recommendations.