ЖЕРТВА КІБЕРЗЛОЧИНІВ: ОЗНАКИ ТА МЕТОДИ ВИЯВЛЕННЯ

Яровенко Ганна Миколаївна
ORCID ID: 0000-0002-8760-6835
д-р. екон. наук, доцент, доцент кафедри економічної кібернетики
Сумський державний університет, Україна

За останнє десятиліття спостерігається стрімке зростання кіберзлочинів у різних сферах життєдіяльності суспільства, що є наслідком Четвертої промислової революції. Діяльність кіберзлочинців направлена на викрадення особистої інформації та порушення функціонування кіберфізичних систем. Жертвами таких злочинів можуть виступати, в першу чергу, індивіди, які використовують мобільні та програмні додатки для здійснення платежів, операцій в Інтернет-магазинах, спілкування в соціальних мережах, електронного листування, онлайн-комунікації, тощо. В результаті, вони можуть втратити свої персональні та фінансові дані, або будуть змушені сплатити кошти, які незаконно вимагають кіберзлочинці. Також жертвами можуть виступати суб'єкти господарювання через витоки даних, порушення їх цілісності, доступності, конфіденційності. Як наслідок, вони втрачають інформацію, клієнтів та прибуток. Держава в особі державних органів та компаній може бути об'єктом кіберзагроз, що проявляється у здійсненні кібершпигунства, кібертероризму, кібервійн, хактивізму, масштабних кіберзлочинів та атак на електронний уряд. Наслідки таких злочинів є катастрофічними, оскільки вражаються секретні об'єкти або об'єкти надмірно важливі для забезпечення життєдіяльності та безпеки держави. Такі дії призводять до зриву та порушення їх діяльності в коротко- та середньостроковій перспективі, отримання великих обсягів фінансових втрат, суттєвих для держави.

Таким чином, основними ознаками жертв кіберзлочинців є: за наслідками – фінансові, технічні, соціальні, політичні, репутаційні, психологічні; за нематеріальними об'єктами впливу – інформація та знання; за матеріальними об'єктами впливу – кіберфізичні пристрої, інформаційні системи, IP-адреси, поштові сервери, тощо; за суб'єктністю жертви – індивіди, суб'єкти господарювання, держава в особі державних органів.

Як можна протидіяти кіберзлочинам? На практиці, на жаль, не існує універсальних інструментів для боротьби із ними. Це пов'язано із досить широким спектром таких злочинів, різноманітністю об'єктів впливу та масовим характером їх реалізації. Головним є організація спеціалізованих підрозділів кіберзахисту, якщо мова йде про суб'єктів господарювання та державні органи, або персонального захисту у випадку індивідів. Також значну роль в цьому відіграє обізнаність та поінформованість користувачів щодо потенційних ризиків та кіберзагроз. Але найбільш ефективними засобами виступають спеціалізоване програмне забезпечення, наприклад, антивірусні програми, системи безперервного моніторингу, блокування та розпізнавання кібершахрайств, математичні методи та інструменти. Останні виступають досить потужним засобом для виявлення потенційних загроз шляхом здійснення моделювання та прогнозування ситуацій, виходячи з ретроспекції попередніх подій. Тут можна виділити інструменти інтелектуального аналізу даних, такі як нейронні мережі, дерева рішень, генетичні та еволюційні алгоритми, асоціативний та кластерний аналіз, регресійний аналіз.

Таким чином, сьогодні кіберзлочинність набуває значних масштабів та може охоплювати широкі верстви населення, бізнес та державу. Дане явище подолати повністю не можливо, оскільки вміння та навики кіберзлочинців завжди будуть на крок уперед від заходів безпеки. Але це не відміняє необхідність та можливість протидії злочинцям, що полягатиме у розробці та застосуванні комплексних та більш складних методів та заходів захисту.

Робота виконана в рамках держбюджетної науково-дослідної роботи 0121U109559 «Національна безпека через конвергенцію систем фінансового моніторингу та кібербезпеки: інтелектуальне моделювання механізмів регулювання фінансового ринку».