КІБЕРБЕЗПЕКА – ЯК ІНСТРУМЕНТ ВИЯВЛЕННЯ ТА ПОПЕРЕДЖЕННЯ КОРУПЦІЙНИХ ПРАВОПОРУШЕНЬ

Ващенко О.М. *канд. екон. наук, доцент,* ***Шутенко А.Л.****, канд. екон. наук, доцент, Харківський національний університет міського господарства імені О.М. Бекетова*

Кіберзагрози набули глобальний тренд. Державні і приватні компанії стали частіше страждати від кібератак.

Згідно Закону України «Про запобігання корупції» [1], «…корупційним правопорушенням визнані такі діяння, що містять ознаки корупції, що вчинені особою…,уповноваженою на виконання функцій держави або місцевого самоврядування», або особою, яка прирівнюються до осіб, уповноважених на виконання функцій держави або місцевого самоврядування та осіб, які «…постійно або тимчасово обіймають посади, пов'язані з виконанням організаційно – розпорядчих чи адміністративно – господарських обов'язків, або осіб, спеціально уповноважені на виконання таких обов'язків у юридичних особах приватного права незалежно від організаційно – правової форми…, та інші особи, які не є службовими особами та перебувають з підприємствами, установами, організаціями в трудових відносинах».

На думку експертів в галузі ІТ – технологій та фінансово – економічної безпеки кібербезпека - це такі відповідні дії по захисту систем, мереж і програмних додатків від цифрових атак, які спрямовані на отримання конфіденційної інформації та на вимагательство у користувачів фінансових ресурсів і порушення стійкої роботи компанії (фірми).

Правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки визначені Законом України №2163-VIII «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 [2].

За Законом [2] кібербезпека визначається 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.

З метою забезпечення безпеки руху грошових коштів користувачів та конфіденційної інформації застосовуються контрзаходи, які включають посилення контролю доступу, проведення звірок та аудиту, тестування на проникнення та вимоги авторизації, постійна оцінка можливих ризиків. Потенційним об'єктом крадіжки особистих даних що призводить до обману користувачів та провокує останніх повідомити такі дані неофіційним соціальним мережам є фальшиві сповіщення про отримані подарунки, а також електронні

листи з вимогами від певного користувача вказати особисту інформацію чи навіть домашню адресу. На перший погляд, надання такого роду інформації може видаватись нічим не підозрілою дією, однак хакери можуть обмінюватися та торгувати здобутими фактичними даними, поєднуючи їх з уже наявними у них, що на перспективу дозволяє отримати доступ до конфіденційної інформації. Наприклад, які загрози можуть виникнути у користувачів платіжними операціями в системі он-лайн та інтернет-банкінгу (Privat 24 в Україні, Vtb24 в Росії та Pekao 24 у Польщі). Ще прикладом загроз є використання електронних гаманців ***«eWallet»,*** які поступово перетворюються на об'єкт зацікавленості хакерів, що може привести до крадіжки особистої інформації.

Широке впровадження зручних технологій мобільних платежів, а саме мобільні телефони становлять для хакерів ще більшу цінність. Даний процес схожий на загрозу «Firesheep», що працює спеціально для перехоплення чужих Wi-Fi сесій, а тому можна вже в найближчий час очікувати створення й появи на ринку спеціальних хакерських програм, які будуть перехоплювати особисту платіжну інформацію користувачів та застосовувати її з користю для зловмисників.

Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з міжнародною кіберзлочинністю.

Список використаних джерел:

1. Законодавство України про боротьбу з корупцією: Збірник законодавчих актів. – К.: Алетра, 2014. – 136 с.

2. Законом України №2163-VIII «Про основні засади забезпечення кібербезпекиУкраїни» від 05.10.2017. - [Електронний ресурс] – Режим доступу : http://zakon.rada.gov.ua/laws/show/2163-19