підприєствах створено можливість безперешкодного повідомлення про факти правопорушень і зловживань. Одним з методів є організація «гарячої лінії» та анонімних скриньок.

Безпосередній захист прав акціонера у протидії корпоративним злочинам завжди покладається на внутрішню службу безпеки. Така служба, як правило, має розгалужену структуру, окрім центрального офісу має територіальні органи, укомплектована необхідним обладнанням та переважно складається з працівників, що мають досвід оперативно-розшукової діяльності. Взаємодія правоохоронних органів та внутрішньої служби безпеки – важливий крок до ефективної протидії корпоративній злочинності.

Проте, внутрішня служба безпеки може бути неефективною в деяких випадках, або ж намагатися не виносити на публічний рівень окремі корпоративні злочини. Окрім цього, корпоративні злочини можуть завдавати значної шкоди акціонеру в особі держави, отже в цьому випадку виникає необхідність

Таким чином, протидія корпоративним злочинам вимагає впровадження комплексу заходів щодо запобігання та протидії фактами таких злочинів і контролю за їх дотриманням. Внутрішньокорпоративна система заходів не може бути тимчасовим заходом, а повинна носити системний і застережливий характер, постійно вдосконалюючись з урахуванням мінливої ситуації. В той же час у правоохоронних органів, в чиї обов'язки входить питання розслідування фінансових зловживань, виникає нова компетенція – протидія корпоративній злочинності в господарюючих суб'єктах в основі якої лежить урахування внутрішніх політик і процедур господарюючого суб'єкта та ефективна взаємодія з внутрішньою службою безпеки.

Список використаних джерел

1. Про внесення змін до деяких законодавчих актів України щодо управління об'єктами державної та комунальної власності: Закон України станом на 20 берез. 2021 р. *Відомості Верховної Ради України*, 2016. № 28. ст. 533.

2. Бігняк О.В. Порушення корпоративних прав акціонерів. *Правове життя сучасної України: Матеріали міжн. наук. конф. проф.-виклад. складу* (Одеса, 20-21 квітня 2012 р.). О.: Фенікс, 2012. С. 161–163.

3. Басова М.Е. Проблемы борьбы с корпоративным мошенничеством. *Право и экономика*. 2019. №4 (374). С. 75–79.

Лугіна Наталія Анатоліївна,
доцент кафедри кримінального права
та кримінології Університету ДФС України,
кандидат юридичних наук, доцент

УДОСКОНАЛЕННЯ МЕХАНІЗМІВ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В БАНКІВСЬКІЙ СФЕРІ

Кожного дня ми користуємося банківськими картками, смартфонами та Інтернетом. Водночас законодавство, яке повинне створювати безпечні умови для користувачів, безмежно застаріло, адже було впроваджене понад 10 років тому.

Нещодавно було створено Міністерство цифрової трансформації, яке в комітетських слуханнях вирішує основні питання щодо захисту держави в інформаційній сфері. О. Федієнко зазначив, що актуальність проведення слухань викликана тим, що сьогодні кожен стикається з необхідністю користування інформаційними технологіями. Це стосується соціальних мереж, банкоматів, банківських рахунків, платіжних систем тощо. Варто сказати, що на засіданнях неодноразово зазначалось про недостатність коштів для вирішення всіх наявних проблем. Через це все більше уваги буде приділятися державно-приватному партнерству. Означає це те, що замість того, щоб на належному рівні фінансувати відповідні заходи, такий обов'язок перекладуть на приватний бізнес.

Наступною важливою проблемою є відсутність належно розробленої термінології та закріплення її у законодавстві. Проект закону, що може це здійснити «Про захист критичної інфраструктури» ще не розглядається у раді. На державному рівні планується якісніше готувати науковців в даній сфері, натомість правоохоронці стверджують, що належно підготовлений спеціаліст йде у комерційні підприємства, що готові створювати і кращі умови, і платити адекватну зарплату. Через це фактично держава готує кваліфікований персонал і відразу відбувається відтік цих кадрів.

Також представники силових відомств постійно висловлюються за необхідність проведення комплексного перегляду всього законодавства щодо питань інформаційної безпеки з метою створення системи узгодження в законах окремих питань, усунення суперечностей та прогалин.

На цих засіданнях всі учасники прийшли до висновку, що неможливо повністю захистись від кіберзлочинності без масштабного та системного аналізу статистичних даних відповідних процесів. Такі дані повинні бути отримані з усіх можливих джерел для постійного моніторингу, для цього пропонується впровадити тотальну ідентифікацію всіх абонентів мереж, що звичайно суспільством неодмінно буде розцінено як посилення контролю з боку держави.

Сумний факт полягає в тому, що в Україні майже відсутні фахівці, які вміють та здатні знаходити вразливість безпеки в програмному забезпеченні. Зважаючи на швидкий розвиток он-лайн платежів та цифровізацію економіки, без адекватного законодавства ні бізнес середовище, ні правоохоронці не зможуть убезпечити громадян від величезних ризиків.

О. Довгань в своїх дослідженнях виокремив основні питання, які слід вирішити для забезпечення захисту від кібезлочинів: 1) розробка закону, яким повністю *визначаться* основні поняття; 2) розробка державної політики забезпечення інформаційної безпеки, зокрема і в банківській сфері; 3) виділення об'єктів інформаційної безпеки, суб'єктів та механізми її забезпечення; 4) координування та основні правила діяльності суб'єктів захисту від кіберзагроз, порядок взаємовідносин між державою та приватними структурами щодо реагування на виклики та загрози, тощо [1, с. 6].

Варто зазначити, що удосконалення та забезпечення цих механізмів є неможливим без аналізу та вивчення зарубіжного досвіду та прагнення адаптувати законодавство до найновіших стандартів. Однією із найуспішніших країн Європи у сфері боротьби з кіберзлочинністю є Великобританія. Уряд Великої Британії оприлюднив 5-річний план реалізації Стратегії національної кібербезпеки і виділив на це рекордні 1,9 млрд. фунтів.

Досліджуючи зарубіжний досвід забезпечення кібербезпеки, не можна не звернути увагу на нашого сусіда – Польщу, яка сьогодні активно розвиває систему кіберзахисту на державному рівні. За деякими аналітичними даними невдовзі Польща може посісти провідне місце в ІТ-галузі в Центрально-Східній Європі. На разі п'ятсот тисяч осіб працює в секторі високих технологій, а вартість ринку ІТ-послуг у Польщі сягнула майже три мільярда доларів і продовжує зростати. Дуже активний розвиток даного сектору економіки приваблює інвесторів та спеціалістів. Серед основних причин, якими зумовлено успішний розвиток ІТ виділяють продуману та грамотну політику держави. Як вважають деякі аналітики, якщо такі позитивні тенденції продовжуватимуться, то в 2020 році вартість ІТ сектору досягне 4 мільярдів доларів, тоді як ринок ІТ-послуг усієї Центрально-Східної Європи коштуватиме 11 мільярдів доларів. Ці дані оприлюднила дослідницька фірма IDC.

Аналіз досвіду вказаних вище країн дає змогу виокремити наступні напрямки розвитку інституту забезпечення кібербезпеки в Україні: по-перше, необхідно збільшити фінансування суб'єктів, діяльність яких спрямована на забезпечення кібербезпеки в державі; по-друге, слід покращити якість освіти працівників кіберполіції; по-третє, кардинального оновлення потребує Стратегія кібербезпеки України; по-четверте, необхідно розширювати міжнародне співробітництво у сфері забезпечення кібербезпеки, не обмежуючись співпрацею з однією конкретною країною.

Одним із перспективних напрямків удосконалення забезпечення кібербезпеки в Україні є оптимізація системи суб'єктів, що уповноважені здійснювати діяльність у цій сфері, а також налагодження ефективної взаємодії між ними. Досвід іноземних країн та особливості українських реалій свідчать, що розв'язання основних завдань

кібербезпеки неможливе без створення міжвідомчого структурного органу, який на постійній основі забезпечував би координацію діяльності певних відомств, правоохоронних і силових структур України з питань забезпечення кібернетичної безпеки. Кібератака 27 червня 2017 року на Україну довела неефективність діяльності Національного координаційного центру кібербезпеки, поставила питання не про демагогічні та популістські формування недієздатних органів, а про формування відповідно до національних інтересів національної системи кібербезпеки, власне, як на те вказується безпосередньо в Стратегії кібербезпеки України.

У банківській та фінансовій сфері головними заходами для захисту від кіберзагроз повинні бути дії, що полягають у впровадженні потужних засобів автентифікації (на нашу думку, біометрична автентифікація є безпечнішою за всі інші), а також, розробку програм контролю та аудиту. Щодо автентифікації, на сьогодні існують різні способи двофакторної автентифікації, такі як, наприклад, електронні ключі або генератори надійних одноразових паролів.

Також, пильної уваги потребують бази зберігання даних, що повинні бути захищені найновішими криптографічними засобами, а також банкомати та термінали, що повинні забезпечуватися новими та надійними засобами антивірусного захисту, що призведе до створення закритого програмно-апаратного середовища та виключить установку чи приєднання будь-яких сторонніх пристроїв.

Отже, основні завдання з забезпечення захисту від кіберзлочинності в кредитно-фінансовій сфері являють собою оперативне та адекватне реагування на інциденти та атаки, що можуть призвести на переривання в роботі та аварії, збереження даних та цілісності технічних засобів, збереження репутації як банків так і правоохоронних органів, недопущення кіберзлочинів, спрямованих на людей та їх власність.

Список використаних джерел

1. Довгань О.Д. Правові засади формування і розвитку системи забезпечення інформаційної безпеки України. *Інформаційна безпека людини, суспільства, держави*. 2015, № 3 (19), С. 6-17.