Ткаченко Є. К., здобувач гр. ФС-22м
Сибірцев В. В., д-р. екон. наук., професор
Центральноукраїнський національний технічний університет
м. Кропивницький, Україна

СУЧАСНІ ТЕХНОЛОГІЇ УПРАВЛІННЯ КАДРОВОЮ БЕЗПЕКОЮ БАНКІВСЬКОЇ УСТАНОВИ

Українські банки, в умовах воєнного стану, стикаються із підвищеним ризиком стосовно кадрової безпеки, що вимагає впровадження ефективних технологій управління персоналом. Сучасна практика доводить, що в умовах воєнного стану збільшуються інсайдерські загрози, оскільки працівники можуть стати об'єктом впливу з боку зовнішніх сил або спокуситися на привабливі фінансові пропозиції в умовах форс-мажору. Оскільки кібератаки виступають засобом гібридної війни, забезпечення кібербезпеки на рівні персоналу стає критично важливим завданням [1].

Відповідно із результатами дослідження Міжнародної аудиторської компанії PricewaterhouseCoopers (PwC), які щорічно публікуються у «Всесвітньому огляді економічних злочинів» («PwC's Global Economic Crime and Fraud Survey 2022»), 80% збитків фінансовим активам організації чинять власні співробітники і лише 20% спроб втручання в мережі і отримання несанкціонованого доступу до конфіденційної інформації здійснюється ззовні. За даними експертів компанії найбільш поширеними видами економічних злочинів є незаконне привласнення активів (69%), шахрайство при оформлені документів (29%), хабарництво і корупція (27%), кіберзлочини (24%), а також фінансові махінації (22%) [2].

Ефективний механізм управління кадровою безпекою банку включає ряд складових елементів, що взаємодіють між собою для забезпечення дієвого контролю, захисту персональної інформації та інших важливих активів. Ключові складові елементи механізму управління кадровою безпекою у банківській установі представлені на рис.1.

Кадрова політика	• визначення чітких правил та стандартів управління кадровою безпекою, які визначають права, обмеження та вимоги для працівників щодо захисту конфіденційної інформації
Моніторинг та аудит	• системе безперервного спостереження за активністю персоналу та аудиторські механізми для виявлення надмірної або неправомірної активності персоналу в інформаційних системах
Електронна автентифікація	• використання електронних систем та біометричних технологій для додаткового рівня автентифікації та контролю доступу до інформаційних ресурсів
Заходи кібербезпеки та захисту інфраструктури	• використання сучасних кібербезпекових заходів та систем виявлення вторгнень, а також захист фізичного доступу до приміщень та обладнання, що містить конфіденційну інформацію

Рис.1. Елементи механізму управління кадровою безпекою у банківській установі

Дієвість механізму забезпечується за рахунок впровадження сучасних технологій управління кадровою безпекою в практику банків. Серед найбільш поширених технологій є:

1. Адаптація, професійне навчання та залученість персоналу. Регулярне проведення тренінгів та освітніх заходів для працівників щодо важливості безпеки і правил обробки конфіденційної інформації. Залученість персоналу у процес створення і впровадження культури безпеки в робоче середовище, де працівники відчувають відповідальність за збереження інформації.

2. Створення системи електронного контролю доступу та інцидент-центру. Використання електронних карток чи мобільних додатків для контролю доступу до робочих приміщень та обмеження доступу до конфіденційної інформації. Впровадження систем інцидент-виявлення для оперативного реагування на потенційні загрози та виявлення порушень.

3. Партнерство з технологічними компаніями. Співпраця з постачальниками технологій для інтеграції передових систем управління кадровою безпекою. Використання відбитків пальців, розпізнавання обличчя, чи інших біометричних даних для ідентифікації та автентифікації працівників.

4. Співпраця із зовнішніми експертами. Взаємодія з експертами з безпеки для оцінки, аудиту та вдосконалення систем управління кадровою безпекою.

Описані технології допомагають банкам створити комплексні та ефективні системи управління кадровою безпекою, забезпечуючи захист від внутрішніх та зовнішніх загроз.

Сучасні банківські установи вкладають ресурси в регулярні навчальні заходи, щоб підвищити рівень свідомості працівників щодо кібербезпеки, соціального інжинірингу, та правил користування конфіденційною інформацією.

У підсумку варто зазначити, що серед ключових елементів економічної безпеки банківських установ особлива увага приділяється кадровій безпеці, оскільки людський фактор вважається специфічним і найважливішим серед усіх видів економічних ресурсів організації. Керівники банків не тільки прагнуть мати персонал, готовий та здатний належним чином виконувати свої професійні обов'язки, але й активно розглядають можливості збереження, розвитку та підвищення надійності персоналу.

Сучасні банківські установи діють в непередбачуваному та нестабільному середовищі, яке обумовлене численними політичними, економічними та соціальними змінами. У зв'язку з необхідністю швидкої адаптації до технологічних та інформаційних викликів менеджери банків активно впроваджують ефективні системи управління кадровою безпекою.

Умови воєнного стану ставлять перед українськими банками виклики, що вимагають інтеграції передових технологій управління кадровою безпекою в систему банківського менеджменту. Впровадження сучасних технологічних інструментів у сферу управління персоналом є необхідною вимогою для забезпечення стійкості та захисту в умовах надзвичайних обставин.

Література:

2. EMA Partners International, executive search & leadership advisory : HR у час війни 2022 URL: https://www.ema-partners.com/europe/ukraine

3. Global Economic Crime Survey 2022 PricewaterhouseCoopers URL: https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html