Zatwierdzono
UCHWAŁĄ Rady Nadzorczej nr 140/2025 z dnia 17.10.2025
Wchodzi w życie z dniem 17.10.2025
ZAAKCEPTOWANO
UCHWAŁĄ ZARZĄDU NR 975 z dnia 03.10.2025

WYMAGANIA POLITYKI BEZPIECZEŃSTWA W SPÓŁCE AKCYJNEJ „KREDOBANK”

W celu zapewnienia możliwie najwyższego poziomu bezpieczeństwa usług i produktów bankowych dostarczanych Klientom Banku oraz wewnętrznych procesów, infrastruktury, ICT i przetwarzanych informacji Bank wdrożył System Zarządzania Bezpieczeństwem Informacji (SZBI) i zapewnia utrzymanie, doskonalenie i rozwój SZBI, odpowiednio do:
- normatywnych aktów prawnych Narodowego Banku Ukrainy,
- standardów: ISO/IEC 27 001:2022, ISO/IEC 27002:2022 DSTU ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) „Bezpieczeństwa informacyjnego, cyberbezpieczeństwo oraz ochrona poufności. System Zarządzania Bezpieczeństwem Informacji. Wymagania”; DSTU ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) Bezpieczeństwa informacyjnego, cyberbezpieczeństwo oraz ochrona poufności. Środki sprawowania kontroli za bezpieczeństwem informacji;
- wymagań przewidzianych w obowiązującym ustawodawstwie oraz w przepisach wewnętrznych SPÓŁKI AKCYJNEJ KREDOBANK (dalej – Bank);
- wymagań organizacji kartowych i systemów płatniczych, których Bank jest uczestnikiem;
- międzynarodowych standardów w zakresie bezpieczeństwa informacji, cyberbezpieczeństwa oraz bezpieczeństwa informacji w środowisku chmurowym , powszechnie stosowanych w międzynarodowej praktyce zasad zapewnienia bezpieczeństwa informacji orac cyberochrony-
- wymagań wynikających z zawartych umów.

Rozdział 1. Deklaracja Zarządu Banku

1.1. Zarząd Banku jest świadomy, że obecna i przyszła pozycja Banku na rynku finansowym zależy od:
- szybkości, efektywności i dokładności identyfikacji zagrożeń/cyberzagrożeń oraz sprzyjających warunków dla działalności Banku;
- oszacowania prawdopodobieństwa ich wystąpienia;
- oceny ich wpływu na ciągłość, jakość i zgodność z ustawodawstwem procesów biznesowych Banku, a także wpływu na pozycję rynkową i wizerunek Banku;
- efektywności doboru i wdrażania odpowiednich działań zapobiegających zagrożeniom/ cyberzagrożeniom lub ograniczających ich negatywne skutki;
- trafności doboru i implementacji rozwiązań zwiększających prawdopodobieństwo wykorzystania możliwości;
- głębokiej transformacji cyfrowej we wszystkich aspektach działalności, odważnych zmian w modelu operacyjnym i modelu dystrybucji;
- dywersyfikacji i dyscypliny w zakresie zarządzania ryzykiem i cyberbezpieczeństwa, odporności na szoki rynkowe.

1.2. Bank określa okoliczności wewnętrzne i zewnętrzne, które mają znaczenie dla osiągnięcia jego celów i mają wpływ na możliwość osiągnięcia wcześniej zaplanowanych wyników systemu zarządzania bezpieczeństwem informacji.

1.3. Ze względu na to, że charakter zagrożeń w działalności bankowej zmienia się w kierunku cyberzagrożeń, to Zarząd Banku szczególną uwagę kieruje na zapewnienie bezpieczeństwa informacji i cyberochronę ICT Banku oraz przetwarzanych w nich danych, a także uznaje za konieczne przyjęcie całościowego, systemowego podejścia do zarządzania bezpieczeństwem informacji w Banku.

1.4. Funkcjonowanie systemu cyberochrony opiera się na następujących zasadach:
1) proporcjonalność i adekwatność podejmowanych działań w zakresie cyberochrony w stosunku do rzeczywistych oraz potencjalnych cyberzagrożeń;
2) priorytetyzacja działań zapobiegawczych;
3) minimalizacji cyberryzyka w działalności banku;
4) przestrzeganie wymogów normatywnych aktów prawnych Narodowego Banku w kwestiach bezpieczeństwa informacji i cyberochrony, rekomendacji Narodowego Banku na podstawie wyników kontroli;
5) ciągłe wsparcie ze strony Zarządu Banku cyberodporności banku poprzez organizację efektywnego zarządzania cyberryzykiem.

Rozdział 2. System zarządzania bezpieczeństwem informacji

2.1. **Bank stale doskonali, zwiększa przydatność, adekwatność i efektywność SZBI**, który ma na celu zapewnienie pewności kierownictwu co do:
- przestrzegania wymogów Polityki bezpieczeństwa informacji i celów bezpieczeństwa informacji,
- przeprowadzenia analizy zdarzeń i incydentów bezpieczeństwa informacji/cyberbezpieczeństwa i podejmowania działań naprawczych i zapobiegawczych w celu minimalizacji prawdopodobieństwa ich ponownego wystąpienia w przyszłości;
- analizy wyników przeprowadzonych audytów;
- przeprowadzenia oceny ryzyka bezpieczeństwa informacji i sporządzenia planu przetwarzania ryzyka;
- przeprowadzenia analizy wskaźników efektywności SZBI, w tym informacje zwrotne od stron zainteresowanych;
- analizy niezgodności SZBI i planowania działań naprawczych.

2.2. **Bank zarządza ryzykiem bezpieczeństwa informacji,** które realizowane jest z przestrzeganiem modelu trzech linii obrony i zapewnia porównywalność wyników, z uwzględnieniem wymogów aktów normatywnych Narodowego Banku, które regulują organizację działań dotyczących zapewnienia bezpieczeństwa informacji i cyberochrony oraz zapewnia:
- przestrzeganie zasad zapewnienia bezpieczeństwa informacji i cyberochrony oraz obowiązkowych minimalnych wymogów w zakresie organizacji działań dotyczących zapewnienia bezpieczeństwa informacji i cyberochrony;

- wdrożenie efektywnych działań w celu zapewnienia poufności, integralności i dostępności informacji, jej ochrony przed zagrożeniami zewnętrznymi i wewnętrznymi, w tym cyberataki i zagrożenia bezpieczeństwa fizycznego.

2.3 .Zarządzanie zdarzeniami i incydentami bezpieczeństwa informacji obejmuje:

- operatywne identyfikowanie i rejestrowanie zdarzeń bezpieczeństwa informacji, ocenę zdarzeń w celu potwierdzenia klasyfikacji jako incydentu bezpieczeństwa informacji;
- reagowanie na incydent – polega na określeniu i podejmowaniu specjalnych środków bezpieczeństwa lub działań naprawczych, zgodnie z priorytetem przetwarzania incydentu;
- analizę incydentu – polega na ustaleniu, sprawdzeniu informacji o incydencie i podjętych w związku z nim działaniach, która uwzględnia priorytet przetwarzania incydentu, dokumentację i eskalację incydentu (w razie konieczności), zbieranie dowodów i śladów związanych z wystąpieniem incydentu, identyfikację jego przyczyn.
- poprawy, które ograniczają ponowne wystąpienie incydentu bezpieczeństwa – polegają na podejmowaniu działań naprawczych, rozwiązań systemowych mających na celu zapobieganie ponownemu wystąpieniu incydentu bezpieczeństwa w przyszłości;
- informacje otrzymane z analizy i przetwarzania incydentów bezpieczeństwa informacji, stosowane podczas oceny ryzyka bezpieczeństwa informacji w celu zmniejszenia prawdopodobieństwa lub wpływu przyszłych incydentów.

W celu zmniejszenia ryzyka wystąpienia incydentów bezpieczeństwa informacji, w Banku wykonywane są systematyczne działania, w celu podnoszenia poziomu świadomości personelu w zakresie bezpieczeństwa informacji, w szczególności:

- poinformowanie pracowników Banku o wdrożeniu (nowych lub zmian) przepisów wewnętrznych, które określają zasady zapewnienia bezpieczeństwa (w szczególności niniejszej Polityki) i zobowiązania pracowników zapoznać się z nimi i przestrzegać wymogów tych dokumentów;
- przeprowadzenie treningów i szkoleń dla pracowników w zakresie bezpieczeństwa bankowego;
- przeprowadzenie kampanii i działań (aktywności) wewnętrznych, w szczególności po wystąpieniu poważnego incydentu bezpieczeństwa i w przypadku zidentyfikowania informacji w zakresie nowych metod ataków na Banki i ich Klientów;
- przeprowadzenie testów i audytów bezpieczeństwa (w tym testów socjotechnicznych), testowanie planów ciągłości działania Banku i omówienie ich wyników z odpowiedzialnymi osobami odpowiednich jednostek/komórek organizacyjnych.

Każdy pracownik Banku zobowiązany jest do zawiadomienia o wystąpieniu incydentu bezpieczeństwa informacji. Zasady i tryb poinformowania i dane kontaktowe osób, które powinny zostać poinformowane, są określone są w odrębnym dokumencie, który szczegółowo opisuje procedurę reagowania na incydenty bezpieczeństwa informacji.

Wszyscy pracownicy Banku podczas zatrudnienia podpisują zobowiązania o nieujawnieniu informacji z ograniczonym dostępem, w tym tajemnicy bankowej i danych osobowych. Pracownicy Banku zobowiązani są do nieujawniania i niewykorzystywania dla własnej korzyści lub korzyści osób trzecich informacji z ograniczonym dostępem, które stały się znane im podczas pełnienia swoich obowiązków służbowych.

W Banku funkcjonuje Program szkolenia i podnoszenia kwalifikacji pracowników w zakresie bezpieczeństwa informacji, która określa cele, zadania, główne rodzaje szkolenia, tryb interakcji jednostek/komórek organizacyjnych Banku, uprawnienia i obowiązki pracowników przy organizacji szkolenia w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa.

2.4**.** W Banku działa zasada udzielenia minimalnego poziomu uprawnień podczas udzielenia dostępu do systemów informatycznych banku (w tym dostęp użytkowników uprzywilejowanych).

2.5. Oprogramowanie Banku powinno spełniać wymagania dotyczące bezpieczeństwa informacji ustawodawstwa Ukrainy, dokumentów i standardów NBU, a także standardów międzynarodowych ISO 27001 oraz spełniać następujące wymagania:

- obecność wbudowanego systemu ochrony informacji, którego nie można wyłączyć i nie można przetworzyć opracowanie informacji bez jego wykorzystania;
- obecność wbudowanych mechanizmów należytej ochrony informacji podczas jej przekazywania między różnymi podsystemami, w których przetwarzane są informacje;
- do zautomatyzowanych systemów funkcjonujących w trybie „klient-serwer", dostęp użytkowników do bazy danych powinien odbywać się tylko za pośrednictwem dodatkowego oprogramowania, za pomocą którego dokonywane jest uwierzytelnianie i autoryzacja osób uprawnionych do korzystania z tej bazy danych;
- stosowanie wzmożonego uwierzytelniania użytkownika usługi płatniczej;
- obecność wbudowanych mechanizmów zapewniających jednoznaczną i niepodważalną identyfikację użytkownika na każdym urządzeniu dostępu do systemu, w każdym modułu lub elemencie systemu, do którego użytkownik ma dostęp, a także podczas przeprowadzenia wszelkich operacji w systemie;
- zapewnienie możliwości automatycznego blokowania konta w systemie po przekroczeniu liczby dozwolonych nieudanych prób wprowadzenia hasła na dowolnym urządzeniu dostępu do systemu zapewnienia ciągłej technologicznej kontroli nad integralnością informacji i nałożenie/sprawdzenie podpisu cyfrowego na wszystkich bankowych dokumentach płatniczych na każdym etapie cyklu technologicznego ich przetwarzania; zapewnienie szyfrowania elektronicznych dokumentów bankowych zawierających informacje poufne, podczas przekazywania na nośnikach zewnętrznych lub poprzez odpowiednie kanały komunikacyjne w trybie online z odpowiednim potwierdzeniem o ich otrzymaniu zapewnić obowiązkową rejestrację wszystkich prób dostępu, wszystkich operacji i innych działań w systemie, a także zapisywanie ich w zautomatyzowanym systemie zabezpieczonym przed modyfikacją rejestrze elektronicznym, ze stałą kontrolą jego kompletności i integralności.

2.6. Bank wspiera wysoki poziom bezpieczeństwa informacji przetwarzanych, przechowywanych i przekazywanych za pomocą technologii chmurowych przechowywania danych. Procesy nabycia, wykorzystywania, zarządzania i wyjścia z usług chmurowych powinny zostać dostosowane do wymogów bezpieczeństwa informacji Banku z przestrzeganiem wymogów ustawodawstwa.

2.7. W Banku opracowano, działa, testuje się i aktualizuje plan zapewnienia ciągłości działalności, w którym uwzględniono ciągłość funkcjonowania środków bezpieczeństwa informacji w ramach procesu zarządzania ciągłością działalności Banku, środki przywracania systemów informatycznych po zakłóceniach.

2.8. Każdy pracownik lub osoba współpracująca z Bankiem zobowiązana jest do sprzyjania działalności w zakresie osiągnięcia i utrzymywania odpowiedniego poziomu bezpieczeństwa informacji w Banku w zakresie, który odpowiada jego obowiązkom służbowym i udzielonym uprawnieniom.

2.9.**Bank żąda od Dostawców** wiedzy i przestrzegania wymogów dotyczących bezpieczeństwa informacji, w szczególności w relacjach umownych uregulować kwestie dotyczące ochrony aktywów Banku i gwarantować, że uzyskany przez nich dostęp do aktywów Banku zostanie wykorzystany wyłącznie w celu świadczenia usług zgodnie z zawartą umową między Bankiem a tym Dostawcą, i Dostawca nie będzie inicjować dostępu do takich aktywów, jeśli to nie jest określone w pisemnych relacjach umownych między stronami. Dostawca/Pracownicy Dostawcy/Osoby trzecie mogą zapoznać się z wymaganiami polityki bezpieczeństwa informacji umieszczonymi na korporacyjnej stronie internetowej Banku.

Rozdział 3. Cele bezpieczeństwa informacji

Realizowane przez Bank zasady wynikające z SZBI, powinny zapewniać osiągnięcie następujących celów bezpieczeństwa informacji:

- **Zgodność z wymaganiami ustawodawstwa.** Podczas opracowania informacji przez Bank, a w szczególności organizacji jej ochrony, należy przestrzegać obowiązującego ustawodawstwa Ukrainy i wymagań standardów bezpieczeństwa grupy PKO Banku Polskiego S.A.
- **Dostępność informacji.** Informacja i środki jej przetwarzania są dostępne dla osób upoważnionych Banku, osób trzecich zgonie z zobowiązaniami umownymi oraz dla grupy PKO Banku Polskiego S.A. Bank zapewnia akceptowalny poziom dostępności informacji z uwzględnieniem wymagań ustawodawstwa oraz działalności operacyjnej Banku.
- **Poufność informacji.** Informacja jest dostępna wyłącznie dla osób i procesów, które mają odpowiednie prawa dostępu do nich. Prawa te wynikają w szczególności z przynależności informacji (informacja Klientów Banku), a także z obowiązków i zadań wykonywanych na rzecz Banku, przez pracowników i dostawców usług Banku.
- **Integralność informacji.** Bank stosuje środki organizacyjne i techniczne, które chronią dokładność i kompletność informacji oraz chronią prawidłowe funkcjonowanie mechanizmów przetwarzających informacje. W szczególności informacje są chronione przed nieautoryzowanymi zmianami.
- **Obserwowalność.** Zapewnienie możliwości identyfikowania użytkowników i procesów, a także zapisywania działań użytkowników i procesów dotyczących tych informacji w celu zapobiegania i/lub dochodzenia naruszeń polityki bezpieczeństwa.
- **Zastosowanie zasad bezpiecznego przetwarzania informacji.** Przetwarzanie informacji i wykorzystanie środków jej przetwarzania odbywa się zgodnie z ustalonymi zasadami. Zasady obowiązujące zewnętrzne podmioty gospodarcze są realizowane na podstawie umów zawartych z Bankiem.
- **Nadzór nad ochroną informacji.** Bank kontroluje czy sposób przetwarzania informacji jest zgodny z wymaganiami w zakresie ochrony informacji. W przypadku potwierdzenia niezgodności w odpowiednim terminie podejmowane są działania zmierzające do jej usunięcia.
- **Adekwatna ochrona informacji i środków jej przetwarzania w zakresie poziomu ryzyka.** Dobór środków ochrony wynika z zarządzania ryzykiem informacyjnym w Banku. Dzięki takiemu podejściu możliwe jest zapewnienie efektywności procesów informacyjnych.
- **Adekwatna optymalizacja środków ochrony odpowiednio do potrzeb bieżących Banku.** Poprzez zarządzanie ryzykiem, audyt, przegląd i pomiar efektywności, Bank ustala czy organizacyjne i techniczne środki ochrony są optymalne dla wymagań bezpieczeństwa i działalności operacyjnej Banku.
- **Zapewnienie szybkiej i efektywnej reakcji na naruszenie bezpieczeństwa informacji.** Bank operatywnie reaguje na wszelkie oznaki naruszenia bezpieczeństwa informacji/cyberbezpieczeństwa, co pozwala zminimalizować prawdopodobne negatywne skutki zdarzenia i podjąć natychmiastowe działania naprawcze.

Rozdział 4. Główne zasady zapewnienia bezpieczeństwa informacji

Organizacja bezpieczeństwa informacji Banku oparta jest na następujących podstawowych zasadach:

Zasada minimalnych uprawnień: dostęp pracowników Banku i użytkowników do pomieszczeń, systemów informatycznych, zasobów Banku powinien zostać zorganizowany w taki sposób, aby udzielać tylko te uprawnienia, które są niezbędne do wykonywania zadań służbowych.

Zasada konieczności wiedzy: każdy pracownik lub osoba współpracująca z Bankiem posiada wyłącznie te informacje o zasobach informacyjnych Banku, zasobach ich przetwarzania i sposobach ich ochrony, które są niezbędne do wykonywania wyznaczonych zadań i obowiązków. Osoby trzecie mają dostęp wyłącznie do tych informacji, które Bank określił jako publiczne (otwarte).

Zasada podziału obowiązków: wykonanie zadań, które są krytyczne z punktu widzenia bezpieczeństwa zasobów informacyjnych i finansowych Banku, systemów informacyjno-telekomunikacyjnych i usług banku zorganizowane są w taki sposób, aby ich realizacja wymagała udziału więcej niż jednej osoby („zasada dwóch par rąk").

Zasada autoryzacji działań: te działania pracowników Banku, które są wyraźnie niedozwolone ustawodawstwem, aktami normatywnymi NBU, wewnętrznymi ustanawiającymi lub normatywnymi dokumentami są zakazane.

Zasada legalności: SZBI Banku uwzględnia wymagania obowiązującego ustawodawstwa Ukrainy oraz wymagania międzynarodowych wymogów normatywnych w zakresie bezpieczeństwa informacji.

Zasada spójności i jedności: cele i zadania bezpieczeństwa informacji są zgodne z celami strategicznymi i zadaniami biznesowymi Banku, a zarządzanie bezpieczeństwem informacji jest częścią integralną zarządzania Bankiem.

Zasada adekwatności i efektywności: środki ochrony zasobów informacyjnych wdrażane są zgodnie z ich krytycznością, czyli kategorią klasyfikacji i poziomem ryzyka zasobu informacyjnego w oparciu o zasady oceny ryzyka zaakceptowanego przez Bank.

Zasada praktyczności: środki ochrony zasobów informacyjnych powinny być praktyczne i wspierać równowagę między wydajnością a bezpieczeństwem systemów informatycznych.

Zasada ciągłości: bezpieczeństwo informacji jest ciągłym procesem przeciwdziałania zagrożeniom/cyberzagrożeniom i zarządzania ryzykiem właściwym dla obszaru działalności Banku.

Zasada odpowiedzialności: kierownictwo Banku wszystkich poziomów, pracownicy, dostawcy i inne trzecie osoby mające dostęp do zasobów informacyjnych Banku powinny przestrzegać wymogów dokumentów wewnętrznych Banku w zakresie bezpieczeństwa informacji oraz ponoszą osobistą odpowiedzialność za ich wykonanie.

Zasada ciągłego udoskonalenia: wdrożony w Banku system zarządzania bezpieczeństwem informacji zawiera mechanizmy i wskaźniki do pomiaru i kontroli efektywności systemu zarządzania i wdrożonych zabezpieczeń w celu racjonalnego planowania i realizacji działań mających na celu doskonalenie.

Zasada wielopoziomowej ochrony: organizacja bezpieczeństwa informacji przewiduje utworzenie następującego szeregu kolejnych poziomów ochrony zasobów informacyjnych i personelu Banku przed prawdopodobnymi zagrożeniami/cyberzagrożeniami:

- poziom organizacyjno-prawny, który określa wymogi prawne i normatywne oraz zobowiązania personelu, użytkowników zasobów informacyjnych i kontrahentów Banku w zakresie bezpieczeństwa informacji;
- fizyczny poziom ochrony, który zapobiega nieuprawnionemu dostępowi fizycznemu, uszkodzeniu lub wtargnięciu do pomieszczeń służbowych Banku w celu nieuprawnionego dostępu do informacji;
- poziom oprogramowania użytkowego, który odpowiada za interakcję z użytkownikiem zasobów informacyjnych;
- poziom systemu zarządzania bazami danych, który odpowiada za przechowywanie i przetwarzanie danych;
- poziom systemu operacyjnego, który odpowiada za bezpieczną i niezawodną obsługę oprogramowania użytkowego i systemów zarządzania bazami danych;
- poziom sieci, który odpowiada za interakcję węzłów systemu informatycznego Banku.

Zasada kompleksowości i systemowości: bezpieczeństwo informacji Banku budowane jest kompleksowo, uwzględniając wszystkie aspekty ochrony informacji, w szczególności:

- strategie i cele bezpieczeństwa,
- zarządzanie zasobami informacyjnymi i nośnikami informacji,
- bezpieczeństwo zasobów ludzkich,
- zarządzanie bezpieczeństwem fizycznym i bezpieczeństwem środowiska,
- bezpieczeństwo relacji z dostawcami,
- bezpieczeństwo procesów komunikacji wewnętrznych i zewnętrznych,
- zarządzanie zgodnością z wymaganiami prawnymi, normatywnymi i umownymi,
- zarządzanie incydentami bezpieczeństwa informacji,
- zarządzanie ciągłością biznesu,
- bezpieczeństwo w procesach projektowania, poszukiwania, rozwoju, wdrożenia i wsparcia systemów IT,
- bezpieczeństwo w procesach eksploatacji systemów IT,
- 100 % zidentyfikowanie ryzyka zmian systemów dotyczących ciągłości i integralności ich funkcjonowania.

Przyjęta przez Bank systemowość podejścia do zarządzania bezpieczeństwem informacji przewiduje zapewnienie spójności procesów i działań przeprowadzanych w zakresie bezpieczeństwa:

- z warunkami środowiska, w którym funkcjonuje Bank,
- ze strategią i celami biznesowymi Banku,
- z wynikami oceny ryzyka i możliwości,
- z wynikami oceny efektywności systemu zarządzania i wdrożenia środków ochrony,
- ze wszystkimi aspektami zarządzania działalnością operacyjną i technologiami informacyjnymi Banku.