Політика інформаційної безпеки «АТ «КБ «ГЛОБУС» (публічна)

Загальні принципи інформаційної безпеки Банку

1. Банком використовуються наступні підходи щодо забезпечення інформаційної безпеки (далі – ІБ):
   1) створено та затверджено перелік відомостей, що містять інформацію з обмеженим доступом;
   2) створено та затверджено перелік критичних бізнес-процесів, за якими проводиться оцінка ризиків інформаційної безпеки та подальша їх обробка;
   3) встановлено правила доступу до інформаційних ресурсів та програмно-технічних комплексів;
   4) забезпечується контроль фізичного та логічного доступу до всіх визначених ресурсів;
   5) забезпечується парольний захист програмних та сервісних ресурсів;
   6) забезпечується антивірусний захист програмних та сервісних ресурсів;
   7) забезпечується захист мережі;
   8) забезпечується ідентифікація та автентифікація всіх визначених ресурсів;
   9) забезпечується криптографічний захист інформації;
   10) проводяться аудити системи управління інформаційною безпекою (далі – СУІБ) та аналіз СУІБ з боку керівництва Банку;
   11) здійснюється моніторинг та вдосконалення СУІБ.

2. Банк дотримується наступних правил в частині забезпечення ІБ та безперебійної діяльності:
   1) працівники Банку та третіх сторін беруть участь у підтримці відповідного рівня ІБ в межах своїх обов'язків та повноважень і несуть відповідальність за його порушення в межах, встановлених чинним законодавством України та актами внутрішнього регулювання Банку;
   2) під час розроблення, впровадження та функціонування програмно-технічних комплексів враховуються вимоги ІБ;
   3) публічні сервіси Банку та внутрішні мережі Банку відповідають ІБ;
   4) Банком забезпечується встановлення та моніторинг виконання усіх вимог ІБ, які наявні в угодах з третіми сторонами стосовно участі у міжнародних платіжних системах та системах переказу коштів;
   5) Банк дотримується Стратегії розвитку ІБ та інформаційних технологій Банку;
   6) керівництво Банку створює працівникам Банку умови для систематичного навчання нормам та заходам з ІБ, для зменшення ризиків виникнення інцидентів ІБ;
   7) у Банку складаються, діють, систематично тестуються та оновлюються плани на випадок різних непередбачуваних критичних ситуацій:
      - план забезпечення безперервної діяльності на випадок надзвичайних ситуацій;
      - план забезпечення безперервного функціонування інформаційних систем у разі виникнення надзвичайних ситуацій.

3. Інформація, яка створюється, обробляється або знаходиться у розпорядженні Банку у зв'язку з провадженням банківської діяльності, а також процеси обробки інформації та інформаційні активи, що використовуються цими процесами, є важливими бізнес-ресурсами, що мають цінність для Банку.
   Банк здійснює заходи щодо захисту інформації та інформаційних активів від загроз несанкціонованого використання, модифікації, знищення, блокування доступу, а

також щодо забезпечення цілісності, керованості та спостереженості процесів обробки інформації.
Головним завданням ІБ є мінімізація ризиків ІБ Банку, що пов'язані з банківською діяльністю, відповідно до вимог Політики ІБ Банку.

4. Визначення цілей, розробка та реалізація стратегії і основних напрямків ІБ Банку, контроль їх виконання належить до компетенції та є прерогативою Правління Банку.
Функції з керування та забезпечення режиму ІБ, а також розробки та актуалізації політики ІБ покладаються Правлінням Банку на окремий структурний підрозділ ІБ.
Всі співробітники Банку повинні бути ознайомлені, правильно розуміти та виконувати свої обов'язки та функції щодо забезпечення ІБ Банку.
Режим безпеки розуміється та безумовно підтримується керівництвом Банку.

5. Політика ІБ Банку будується виключно на підставі його виробничих інтересів у відповідності до вимог законодавства України, договорів, зобов'язань, що мають виконуватись Банком.
У випадку виникнення розбіжностей вимоги законодавства України мають пріоритет щодо вимог інших нормативних актів.

6. Вся інформація, що знаходиться у розпорядженні Банку у зв'язку з провадженням банківської діяльності, класифікується за категоріями обмеження доступу та критичністю щодо здійсненням цієї діяльності.
Банк має забезпечити згідно з вимогами законодавства України обмеження доступу до відомостей, що стосуються діяльності та фінансового стану клієнтів, а також неоприлюдненої інформації стосовно емітентів та їх цінних паперів, якщо ці відомості віднесено до категорії «банківська таємниця» та «інсайдерська інформація» відповідно.
Банк має забезпечити згідно з вимогами законодавства України обмеження доступу до персональних даних, які обробляються у базах персональних даних Банку, стосовно яких він виступає у якості володільця або розпорядника, за винятком персональних даних певних категорій громадян чи їх вичерпного переліку, віднесення яких до інформації з обмеженим доступом (далі – ІзОД) заборонено законодавством України.
Банк використовує право щодо обмеження доступу до відомостей, пов'язаних з його діяльністю, та оголошення їх комерційною таємницею або конфіденційною інформацію, якщо розголошення цих відомостей може завдати шкоди інтересам Банку, за винятком тих відомостей, які відповідно до законодавства України не можуть бути віднесені до комерційної таємниці, конфіденційної інформації або відомостей, доступ до якої не може бути обмежено.
Доступ до ІзОД співробітникам Банку та працівникам–аутстаферам надається тільки за умов підписання ними зобов'язань щодо нерозголошення цієї інформації.
Доступ до ІзОД та іншої критичної інформації стороннім організаціям, що мають ділові відношення з Банком, надається тільки за умов наявності юридично значущих документів, які визначають вимоги ІБ та зобов'язання сторін стосовно захисту цієї інформації.
Поширення персональних даних можливе лише за згодою фізичної особи, стосовно якої відповідно до закону здійснюється обробка її персональних даних.

7. Вимоги ІБ щодо взаємодії Банку з іншими учасниками у складі платіжних систем будуються на підставі моделі взаємної недовіри.

8. Банк має право та зобов'язаний у визначених законодавством України випадках відстоювати із застосуванням всіх необхідних для цього легітимних заходів свої права та права власних клієнтів у випадках несанкціонованого розголошення ІзОД або інших несанкціонованих дій щодо критичної інформації або інформаційних активів, що знаходяться у розпорядженні Банку у зв'язку з провадженням банківської діяльності.

9. ІБ забезпечується шляхом застосування комплексу заходів контролю ІБ (системи захисту інформації – СЗІ), який реалізує вимоги Політики ІБ Банку.
   СЗІ має забезпечувати:
   1) неможливість відключення або обходу СЗІ;
   2) цілісність на неперервність захисту на всіх етапах життєвого циклу інформації;
   3) оптимальність на мінімальну достатність ступеня захисту;
   4) розмежування доступу та повноважень виконавців до інформаційних активів Банку та процесів обробки інформації за принципом мінімальної достатності (принцип «need-to-know»);
   5) мінімізацію кількості шлюзів між внутрішніми середовищами обробки інформації, що контролюються Банком, та зовнішніми неконтрольованими середовищами;
   6) побудову систем автоматизації банку із застосуванням сучасних технологій та криптографічних алгоритмів захисту інформації, захищених операційних систем та систем керування базами даних;
   7) максимальний рівень захисту ключової інформації СЗІ;
   8) мінімізацію «людського фактора» в процесі застосування засобів захисту інформації.

10. Персонал Банку є важливою і невід'ємною складовою СЗІ.
    Банк встановлює рівень вимог щодо професійного рівня та репутації персоналу, що виконує ключові ролі стосовно забезпечення ІБ.
    Банк вживає заходів щодо доведення вимог Політики ІБ, підвищення свідомості та кваліфікації співробітників Банку у галузі ІБ.

11. Банком на постійній основі здійснюється аналіз ризиків ІБ та рівень відповідності СЗІ цим ризикам. Політика ІБ Банку підлягає періодичному перегляду та корегуванню з метою урахування та мінімізації поточного рівня ризиків ІБ.

12. Банком запроваджується механізм оповіщення та реагування щодо інцидентів ІБ.

13. Банком на постійній основі здійснюється моніторинг роботи СЗІ та критичних систем обробки інформації.
    Банк декларує своє право та здійснює у межах, передбачених законодавством України, моніторинг дій персоналу та сторонніх організацій щодо доступу до ІзОД, критичної інформації та інформаційних активів Банку.

14. Банк превентивно планує заходи забезпечення безперервності банківської діяльності щодо обробки інформації, збереження критичної інформації та інформаційних активів, недопущення розголошення ІзОД Банку в умовах надзвичайних ситуацій. Політика управління безперервною діяльністю затверджуються Правління Банку і передбачає проведення комплексу заходів щодо збереження критичної інформації (в тому числі комерційної та банківської таємниці).