

ЗАТВЕРДЖЕНО:  
Правління АТ «ПРАВЕКС БАНК»

Протокол №19\_23 від 09.06.2023, питання 4 порядку  
денного

## ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (ЗОВНІШНЯ) АТ «ПРАВЕКС БАНК»

Класифікація документа за рівнем безпеки: Відкрита інформація

Перелік змін:

| Версія | Власник                                                                 | Ключові зміни                                           | Скасовані документи                                                                                                                                                          |
|--------|-------------------------------------------------------------------------|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3.1.   | Департамент управління інформаційною безпекою та безперервністю бізнесу | Актуалізація документа відповідно до змін законодавства | Політика інформаційної безпеки (зовнішня) АТ «ПРАВЕКС БАНК», затверджена рішенням Комітету з управління інформаційною безпекою від 21.10.2020 № 3_20.1 (№260 від 20.11.2020) |

Розміщення документа:

<https://my.pravex.ua> – INTERNAL RULES & REGULATIONS BASE – GOVERNANCE DOCUMENTS – Guidelines - ICT and Security Management

Дата набуття чинності: 09.06.2023



| Список погодження                                                                                                                                                                                                                                                                                                                                                                              |                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
| Голова Правління                                                                                                                                                                                                                                                                                                                                                                               | <input type="checkbox"/>            |
| Головний бухгалтер                                                                                                                                                                                                                                                                                                                                                                             | <input type="checkbox"/>            |
| Департамент внутрішнього аудиту                                                                                                                                                                                                                                                                                                                                                                | <input type="checkbox"/>            |
| Департамент юридичної підтримки та генерального секретаріату                                                                                                                                                                                                                                                                                                                                   | <input type="checkbox"/>            |
| Департамент управління ризиками                                                                                                                                                                                                                                                                                                                                                                | <input type="checkbox"/>            |
| Департамент комплаєнсу та протидії легалізації доходів, отриманих злочинним шляхом                                                                                                                                                                                                                                                                                                             | <input checked="" type="checkbox"/> |
| Відділ зв'язків з громадськістю та маркетингу                                                                                                                                                                                                                                                                                                                                                  | <input type="checkbox"/>            |
| Департамент управління персоналом та організаційними змінами                                                                                                                                                                                                                                                                                                                                   | <input checked="" type="checkbox"/> |
| Департамент управління інформаційною безпекою та безперервністю бізнесу                                                                                                                                                                                                                                                                                                                        | <input type="checkbox"/>            |
| Головне управління роздрібного бізнесу                                                                                                                                                                                                                                                                                                                                                         | <input type="checkbox"/>            |
| Головне управління корпоративного бізнесу                                                                                                                                                                                                                                                                                                                                                      | <input type="checkbox"/>            |
| Головне фінансове управління                                                                                                                                                                                                                                                                                                                                                                   | <input type="checkbox"/>            |
| Головне кредитне управління                                                                                                                                                                                                                                                                                                                                                                    | <input type="checkbox"/>            |
| Головне операційне управління                                                                                                                                                                                                                                                                                                                                                                  | <input checked="" type="checkbox"/> |
| Список розсилання                                                                                                                                                                                                                                                                                                                                                                              |                                     |
| Департамент управління інформаційною безпекою та безперервністю бізнесу<br>Департамент внутрішнього аудиту<br>Департамент юридичної підтримки та генерального секретаріату<br>Департамент управління ризиками<br>Департамент комплаєнсу та протидії легалізації доходів, отриманих злочинним шляхом<br>Відділ управління організаційними змінами та проектами<br>Головне операційне управління |                                     |

## Зміст

|   |                                     |    |
|---|-------------------------------------|----|
| 1 | ВСТУП.....                          | 5  |
| 2 | ТЕРМІНИ ТА СКОРОЧЕННЯ.....          | 5  |
| 3 | ПРИНЦИПИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ..... | 6  |
| 4 | ЦІЛЬ ПОЛІТИКИ .....                 | 7  |
| 5 | СФЕРА ЗАСТОСУВАННЯ .....            | 7  |
| 6 | ПРЕДМЕТ ДОКУМЕНТУ ТА ОПИС ДІЙ ..... | 7  |
| 7 | РОЛІ ТА ВІДПОВІДАЛЬНОСТІ .....      | 13 |
| 8 | ПЕРЕГЛЯД ДОКУМЕНТУ .....            | 14 |
|   | Додатки .....                       | 14 |

## 1 ВСТУП

Політика інформаційної безпеки (зовнішня) АТ «ПРАВЕКС БАНК» (далі – Політика) розроблена відповідно до вимог «Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» затвердженого Постановою Правління Національного банку України №95 від 28.09.2017 та вимог:

- Закону України "Про Національний банк України";
- Закону України "Про банки і банківську діяльність";
- Закону України "Про захист інформації в інформаційно-телекомунікаційних системах";
- Закону України "Про національну безпеку України";
- указу Президента України від 13 лютого 2017 року № 32/2017 "Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації"
- указу Президента України від 15 березня 2016 року № 96/2016 "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України",
- Національних стандартів України, а саме:
  - ДСТУ ISO/IEC 27000:2015 "Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник" (далі - ДСТУ ISO/IEC 27000:2015);
  - ДСТУ ISO/IEC 27001:2015 "Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги" (далі - ДСТУ ISO/IEC 27001:2015);
  - ДСТУ ISO/IEC 27002:2015 "Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки" (далі - ДСТУ ISO/IEC 27002:2015).
- методичних рекомендацій з питань кібербезпеки Материнської компанії Intesa Sanpaolo Group;
- міжнародних стандартів з питань інформаційної безпеки, загальноприйнятих у міжнародній практиці принципів забезпечення інформаційної безпеки і кіберзахисту, з метою підвищення рівня інформаційної безпеки в банківській системі України.

1.2. Ця Політика описує прийняту та впроваджену Банком політику щодо інформаційної безпеки при роботі з клієнтами та постачальниками Банку.

## 2 ТЕРМІНИ ТА СКОРОЧЕННЯ

У цій Політиці, та нормативних документах Банку використовуються наступні поняття:

- **АС** – Автоматизована система.
- **Багатофакторна автентифікація** - автентифікація, яка здійснюється за допомогою захищених механізмів двох або більше типів [наприклад, застосування для автентифікації пароля разом із апаратним засобом захисту інформації (токеном) або біометричної автентифікації разом із паролем].
- **Бізнес-процес** – це структурована послідовність дій з виконання певного виду діяльності на всіх етапах життєвого циклу банківської діяльності, метою якої є отримання заданого результату, що має цінність для Банку.
- **Банк** – АТ «ПРАВЕКС БАНК».
- **Геш-Функція** – перетворення вхідного масиву даних довільної довжини у вихідний бітовий рядок фіксованої довжини таким чином, щоб зміна вхідних даних приводила до непередбаченої зміни вихідних даних.
- **ДУІБтаББ** – департамент управління інформаційною безпекою та безперервністю бізнесу Банку.
- **Загроза (threat)** – потенційна причина небажаного інциденту, який може призвести до шкоди для системи або організації.

- **Зловмисний код** - комп'ютерна програма/комплекс комп'ютерних програм або частина програмного коду інформаційної системи, що впроваджується за участю користувача або виконується автоматично, створює загрозу або умови для реалізації загрози порушення штатної роботи обладнання банку та/або порушення конфіденційності, цілісності, доступності інформації, яка обробляється в інформаційних системах Банку.
- **Інформаційна безпека** – це захист інформації від широкого діапазону загроз з метою забезпечення безперервності бізнесу, мінімізації ризику бізнес-процесів і отримання максимальної рентабельності інвестицій і бізнес-можливостей.
- **Інформація з обмеженим доступом** – відомості, що становлять банківську таємницю, комерційну таємницю та персональні дані. Класифікація інформації наведена у **Додатку 1** до даної Політики).
- **Інцидент інформаційної безпеки** – одна або серія небажаних чи непередбачуваних подій інформаційної безпеки, що мають значну ймовірність компрометації бізнес-операцій і загрози інформаційній безпеці чи можуть привести до значних фінансових чи іміджевих втрат Банку.
- **Клієнт (Клієнт Банку)** – особа, яка має рахунок у Банку, або користується його послугами.
- **Комбінація логін/пароль** – це засіб, що засвідчує і підтверджує дії конкретного працівника в автоматизованих системах Банку.
- **Критичний бізнес-процес (КБП)** – бізнес-процес, який обробляє інформацію з обмеженим доступом, яка обробляється за допомогою програмно-технічного комплексу, що забезпечує функціонування бізнес-процесу, розголошення якої може нанести суттєву шкоду Банку та/або зупинити роботу Банку. Необхідно вважати бізнес-процес критичним у разі якщо він обробляє, зберігає, передає інформацію з обмеженим доступом.
- **Мережа Банку** - комплекс технічних засобів телекомунікацій, призначених для маршрутизації, комутації, передавання та/або приймання інформації дротовим та/або бездротовим зв'язком між кінцевим обладнанням (комп'ютерне обладнання, інші компоненти інформаційних систем банку) усередині периметра Банку;
- **Мінімальний рівень повноважень** - повноваження та права доступу, мінімально необхідні для якісного виконання працівниками Банку службових обов'язків;
- **Несанкціонована особа, об'єкт, процес або подія** – особа, об'єкт, процес або подія, які не контролюються Банком та/або не задовольняють вимоги, які до них висуваються.
- **Подія інформаційної безпеки** – ідентифікована подія системи, служби або мережі, яка вказує на можливе порушення чинної Політики інформаційної безпеки Банку, або відмову засобів захисту чи раніше невідому ситуацію, яка може мати відношення до безпеки.
- **Постачальники** – фізичні та/або юридичні особи, з якими Банк має певні відносини відповідно до укладеного договору про надання послуг або виконання інших робіт.
- **Ресурси СУІБ (asset)** – критичні інформаційні ресурси системи управління інформаційною безпекою Банку, на які розповсюджуються вимоги цієї політики.
- **Ризик-орієнтований підхід до забезпечення інформаційної безпеки** - прийняття управлінських рішень на підставі аналізу порівняння поточних ризиків інформаційної безпеки з прийнятними.
- **Санкціонований об'єкт** – об'єкт, який контролюється Банком та/або задовольняє вимоги, які до нього висуваються.
- **Система криптографічного захисту інформації (СКЗІ)** – сукупність засобів криптографічного захисту інформації, необхідної ключової, нормативної, експлуатаційної, а також іншої документації (у тому числі такої, що визначає заходи безпеки), використання яких забезпечує належний рівень захищеності інформації, що обробляється, зберігається й (або) передається.
- **СУІБ – система управління інформаційною безпекою** – перелік цілей, принципів керування, методів, заходів з захисту інформації та забезпечення стійкості бізнес-процесів в інформаційній інфраструктурі Банку.

### 3 ПРИНЦИПИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Принципи, на яких Банк будує інформаційну безпеку, як у внутрішній діяльності, так і при взаємодії з клієнтами і контрагентами, повинні задовольняти наступні вимоги:

- 1) підхід до забезпечення інформаційної безпеки має бути системним (комплексним);
- 2) процес удосконалення та розвитку інформаційної безпеки має бути безперервним і здійснюватися шляхом обґрунтування та реалізації раціональних засобів, методів, заходів із застосуванням найкращого міжнародного досвіду;
- 3) заходи захисту від реальних та потенційних загроз інформаційній безпеці мають бути своєчасні й адекватні;
- 4) забезпечення належного рівня інформаційної безпеки неможливе без підтримки та контролю з боку керівництва Банку;
- 5) сталий розвиток систем інформаційної безпеки можливий лише в разі забезпечення достатності ресурсів Банку.
- 6) процеси управління ризиками інформаційної безпеки повинні оброблятися в рамках системи управління операційними ризиками Банку. Банк має право самостійно визначати підходи (методики) оцінювання та оброблення ризиків інформаційної безпеки. Свою діяльність Банк вибудовує орієнтуючись на ризик-орієнтований підхід, відповідно до вимог ДСТУ ISO/IEC 27001:2015 (додаток А) та ДСТУ ISO/IEC 27002:2015.

### 4 ЦІЛЬ ПОЛІТИКИ

Ціллю Політики є впровадження та ефективне функціонування системи управління інформаційною безпекою, яка буде забезпечувати безпечність та надійність функціонування бізнес-процесів, захист інформації та ресурсів Банку від зовнішніх та внутрішніх загроз та загроз, які пов'язані з навмисними та ненавмисними діями працівників Банку, постачальниками та клієнтами відповідно до договору, забезпечувати безперервну роботу Банку, сприяти мінімізації ризиків операційної діяльності Банку та створювати позитивну репутацію Банку при роботі з Клієнтами.

Основним завданням інформаційної безпеки є захист інформаційних ресурсів Банку від зовнішніх та внутрішніх, навмисних та ненавмисних загроз.

### 5 СФЕРА ЗАСТОСУВАННЯ

- Відповідно до вимог регуляторних документів Національного банку України, мінімальною сферою застосування Політики є усі визначені Банком критичні бізнес-процеси та застосовується для всіх критичних бізнес-процесів Банку при роботі з постачальниками.
- Банк має право розширити сферу застосування даної Політики відповідно до особливостей діяльності, характеру та обсягу банківських, фінансових послуг та інших видів діяльності.

### 6 ПРЕДМЕТ ДОКУМЕНТУ ТА ОПИС ДІЙ

6.1. Основними принципами інформаційної безпеки, яких дотримується Банк, є підтримання належного захисту інформації із забезпеченням її:

**Цілісності** - властивість захищеності, безпомилковості та повноти ресурсів СУІБ.

**Конфіденційності** - властивість інформації не ставати доступною та розкритою для несанкціонованих осіб, об'єктів або процесів.

**Доступності** - властивість доступності та можливості використання ресурсів СУІБ на вимогу санкціонованого об'єкта.

**Спостережності** - властивість системи (автоматизованої, контролю доступу, моніторингу тощо) фіксувати діяльність ідентифікованих користувачів і процесів.

Це в першу чергу стосується інформації з обмеженим доступом, перелік якої наведено в **Додатку 1** до даної Політики.

6.2. Основні об'єкти та ресурси, на які розповсюджується дія цієї Політики:

**інформаційні ресурси** - інформація та дані у будь-якому вигляді, що отримуються, зберігаються, обробляються, передаються, оголошуються, у тому числі знання працівників, партнерів Банку, бази даних та файли, документація, посібники користувача, навчальні матеріали, описи процедур, архівована інформація тощо;

**програмне забезпечення** - прикладне програмне забезпечення, системне програмне забезпечення, сервісне програмне забезпечення та будь-яке інше програмне забезпечення, незалежно від форми отримання (придбання, власної розробки, таке, що вільно розповсюджується), яке використовується у Банку працівниками та системами, для роботи та взаємодії з клієнтами та іншими внутрішніми та зовнішніми системами тощо;

**фізичні ресурси** - апаратні засоби ІТ (сервери, робочі станції, міжмережеві екрани, принтери, копіювальна техніка, телекомунікаційне обладнання, обладнання зв'язку, маршрутизатори, АТС, факси, модеми та т.і.), носії даних (накопичувачі інформації усіх видів), меблі, приміщення, виробниче обладнання, інші засоби які використовуються при роботі з постачальниками та клієнтами Банку;

**сервісні ресурси** - обчислювальні та комунікаційні сервіси (Інтернет, електронна пошта, канали зв'язку тощо), інші технічні сервіси (опалення, освітлення, енергозбереження, кондиціювання повітря, системи сигналізації та моніторингу), усі послуги, пов'язані з отриманням, наданням, використанням, передачею та знищенням ресурсів, усі юридичні та фізичні особи, організації, установи та підприємства (а також їх працівники), послугами яких користується Банк для отримання, використання, передачі та знищення ресурсів;

**людські ресурси** – усі працівники Банку, фізичні особи з якими Банк має договірні відносини, працівники компаній, з якими Банк уклав договори на отримання/постачання послуг, клієнти Банку (як фізичні так і юридичні особи).

6.3. Для кожного ресурсу визначаються можливі ризики інформаційної безпеки та шляхи їх мінімізації, тобто Банк використовує ризик-орієнтований підхід, який забезпечує розуміння, моніторинг та зменшення ризиків операційної діяльності та інформаційної безпеки. Політика базується на вимогах законодавчих, регуляторних та нормативних документів з інформаційної безпеки.

6.4. Банком використовуються наступні підходи щодо забезпечення інформаційної безпеки:

- створено та затверджено перелік відомостей, що містять інформацію з обмеженим доступом;
- створено та затверджено перелік критичних бізнес-процесів;
- встановлено правила доступу до інформаційних ресурсів та програмно-технічних комплексів;
- забезпечується контроль фізичного та логічного доступу до всіх визначених ресурсів;
- забезпечується парольний захист програмних та сервісних ресурсів;
- забезпечується антивірусний захист програмних та сервісних ресурсів;
- забезпечується захист мережі;
- забезпечується віддалений доступ до ресурсів мережі (локальної, мережі Інтернет, мереж інших організацій);
- забезпечується ідентифікація та автентифікація всіх визначених ресурсів;
- забезпечується криптографічний захист інформації.

6.5. Всі працівники Банку та постачальники обізнані та виконують вимоги інформаційної безпеки в роботі.

6.6. Під час розроблення, впровадження та функціонування програмно-технічних комплексів враховуються вимоги інформаційної безпеки, а саме:

**Закони України:**

- «Про інформацію»;
- «Про захист інформації в інформаційно-телекомунікаційних системах»;
- «Про електронні документи та електронний документообіг»;
- «Про електронні довірчі послуги»;

«Про захист персональних даних»;  
«Про Національний банк України»;  
«Про банки і банківську діяльність»;  
«Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення»;  
«Кодекс України про адміністративні правопорушення»;  
«Кримінальний кодекс України».

*Нормативно-правові акти Національного банку України:*

«Інструкція про виконання міжбанківських платіжних операцій в Україні в національній валюті», затверджена постановою Правління Національного банку України від 16.08.2006р. N320 (зі змінами);

«Положення про забезпечення безперервного функціонування інформаційних систем Національного банку та банків України», затверджене постановою Правління Національного банку України від 17.06.2004р. N265 (зі змінами);

«Правила зберігання, захисту, використання та розкриття банківської таємниці», затверджені постановою Правління Національного банку України від 14.07.2006р. N267 (зі змінами);

«Положення про здійснення банками фінансового моніторингу», затверджене постановою Правління Національного банку України від 19.05.2020р. N65 (зі змінами);

«Положення про захист електронних банківських документів з використанням засобів захисту інформації Національного банку України», затверджені постановою Правління Національного банку України від 26.11.2015р. N829 (зі змінами);

«Правила з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи», затверджені постановою Правління Національного банку України від 04.07.2007р. N243 (зі змінами);

Внутрішні нормативні документи Банку з питань інформаційної безпеки.

6.7. Публічні сервіси Банку та рівень забезпечення інформаційної безпеки внутрішніх інформаційних ресурсів повинні відповідати:

- вимогам законодавства України, яке регулює зазначену діяльність;
- вимогам регуляторних документів Національного банку України;
- вимогам Групи «Інтеза Санпаоло»;
- вимогам стандартів серії ISO 2700.

Банк повинен забезпечувати постійне вдосконалення процесу забезпечення захисту інформації при її створенні, обробці, передаванні та зберіганні.

6.8. При укладенні договорів з зовнішніми постачальниками/контрагентами/клієнтами в договори вносяться відповідні вимоги, щодо забезпечення належного рівня інформаційної безпеки, відповідно до переліку послуг, які надаються/отримуються Банком. Перелік вимог з інформаційної безпеки наведено у **Додатку 2** до даної Політики.

6.9. Для зменшення ризиків виникнення інцидентів інформаційної безпеки Керівництво Банку надає рекомендації щодо забезпечення відповідного рівня інформаційної безпеки при роботі з інформаційними ресурсами Банку, та розміщує їх відповідних ресурсах.

6.10. Для забезпечення надійної роботи Банк створює, затверджує та забезпечує тестування Плану забезпечення безперервної діяльності та дій у разі виникнення надзвичайних ситуацій АТ «ПРАВЕКС БАНК».

Усі постачальники послуг в сфері ІТ повинні також забезпечувати безперервність своєї діяльності та надавати до Банку відповідні документи, що підтверджують виконання даної вимоги.

6.11. Про кожний інцидент інформаційної безпеки постачальник повинен повідомити Банку будь-якими доступними засобами, а потім оформити опис інциденту відповідно до Додатку 2 даної Політики, та надіслати його до ДУІБтаББ на адресу електронної пошти

[itsecurity\\_mailbox@pravex.ua](mailto:itsecurity_mailbox@pravex.ua). Зазначена вимога закріплюється в усіх договорах Банку з постачальниками послуг, які укладаються з Банком в сфері надання:

- інформаційних послуг;
- консультаційних послуг;
- послуг, в результаті надання яких постачальник отримує доступ до інформації, яка відповідно до вимог закону України «Про інформацію» не може розповсюджуватись публічно.

6.12. У разі виникнення інциденту інформаційної безпеки у клієнта Банку: клієнт повинен терміново сповістити про це Банк, у будь-який доступний спосіб.

6.13. Інформація про інциденти інформаційної безпеки, у Банку передається наступними засобами/каналами:

- контрольні журнали прикладних інформаційних систем;
- систем захисту та контролю цілісності інформаційних ресурсів, тому числі, підсистем виявлення атак;
- внутрішньої корпоративної пошти;
- сповіщення, які надходять по електронній пошті та системі JIRA;
- засобами зовнішніх телекомунікації (до контакт-центру та на офіційну пошту Банку: [bank@pravex.ua](mailto:bank@pravex.ua));
- засобами пошти НБУ.

6.14. Усі працівники Банку та постачальники при отриманні інформації про будь-які нетипові події інформаційної безпеки щодо порушення роботи обладнання; антивірусного захисту інформації; резервного копіювання; захисту мережі Банку; контролю доступу; криптографічного захисту інформації; парольного захисту; користування інформацією з обмеженим доступом, управлінням послугою постачальника, захисту персональних даних, повинні обов'язково проінформувати своїх безпосередніх керівників (у випадку інциденту на території постачальника, пов'язаного з Банком, негайно повідомляється ДУІБтаББ).

6.15. У випадку порушення принципів організації та вимог щодо захисту ресурсів СУІБ Банку від загроз, пов'язаних з впливом зловмисного та мобільного коду; порушення принципів організації та вимог щодо використання криптографічних засобів для захисту інформації; порушення правил розмежування доступу та аутентифікації користувачів; порушення процесу забезпечення контролю доступу до електронної інформації, інформації в паперовому вигляді та інформації на змінних носіях; порушення принципів внесення змін до програмного забезпечення та програмно-технічних комплексів; порушення принципів управління, правил отримання реєстрації, введення/виведення обладнання з експлуатації, усунення несправностей, проведення періодичного огляду, списання та знищення обладнання; порушення принципів захисту та побудови мережі Банку, яка забезпечує передачу та обробку інформації, відповідальні фахівці ДУІБтаББ в залежності від типу порушень вживають відповідні заходи щодо усунення інциденту.

6.16. Для електронних платіжних документів цілісність забезпечується за допомогою використання електронного цифрового підпису чи одноразового коду, який криптографічно пов'язаний з інформацією, яку він підтверджує.

Усі електронні платіжні документи передаються каналами зв'язку тільки у зашифрованому вигляді. СКЗІ будується на основі засобів КЗІ, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи в сфері КЗІ. Архітектура СКЗІ, порядок її функціонування у складі автоматизованих систем Банку відповідає вимогам Національного Банку України щодо захисту інформації. СКЗІ складається з підсистеми керування криптографічними ключами та підсистеми КЗІ. СКЗІ має універсальну, масштабовану й гнучку підсистему керування криптографічними ключами, що не залежить від технологічних, архітектурних і функціональних особливостей автоматизованих систем Банку.

6.17. Особам, які використовують СКЗІ, категорично забороняється:

- передавати будь-кому свій таємний криптографічний ключ;
- залишати свій таємний криптографічний ключ на робочому місці (крім особистого сейфу) без нагляду;
- розголошувати пароль доступу свого таємного криптографічного ключа будь-кому, в тому числі безпосередньому керівнику;

- порушувати порядок і регламент отримання/зберігання/роботи з СКЗІ та криптографічними ключами.

6.18. Під час розробки, впровадження та функціонування програмно-технічних комплексів, що використовують засоби криптографічного захисту інформації, в обов'язковому порядку враховуються та реалізуються вимоги цієї Політики.

6.19. У Банку забезпечується виконання усіх вимог щодо криптографічного захисту інформації, які наявні в угодах з третіми особами стосовно платіжних систем та систем переказу коштів, включаючи регламенти центрів сертифікації ключів, які надають Банку послуги електронного цифрового підпису. Дані, що являють собою таємні криптографічні ключі, відносяться до інформації з обмеженим доступом.

При компрометації таємних ключів, засобів шифрування та іншої електронної інформації фахівці ДУІБтаББ чи постачальники (в залежності від типу порушень та територіальному розташуванню інциденту) вживають заходи для припинення будь-яких операцій з використанням цих ключів і іншої інформації та заходи щодо зміни ключів шифрування та паролів.

6.20. З метою захисту інформаційних систем і ресурсів Банку, у всіх системах Банку, для організації доступу до інформаційних ресурсів і сервісів, повинні використовуватися системи організації парольного захисту, що відповідають нижчевикладеним вимогам:

- Усі початкові паролі, які встановлені адміністраторами автоматизованих систем, розробниками програмного забезпечення та виробниками обладнання, в обов'язковому порядку повинні бути замінені на власні при першому вході в систему.
- Усі паролі користувачів (персонального комп'ютера, комп'ютерної мережі, електронної пошти і т.п.) та всі паролі системного рівня (адміністраторів систем) повинні мінятися не рідше одного разу на 60 днів та не частіше 1 разу на день.
- Довжина пароля не повинна бути меншою 8 символів для користувачів та 12 символів для адміністраторів.
- Пароль повинен складатись з великих та маленьких букв з додаванням цифр або спеціальних символів (!,!,\$,&, та ін.), де це можливо.
- Пароль не повинен повторюватись як мінімум 10 останніх змін.
- Облікові записи користувачів, яким надані привілеї системного рівня, повинні мати унікальні паролі даного облікового запису відносно паролів цих користувачів до особистих облікових записів Internet-сервісів, інформаційних та інших систем загального користування.
- Паролі не повинні передаватися за межі Банку в поштових або інших інформаційних повідомленнях.
- При використанні SNMP, community string (ряд символів, що виконує роль пароля) повинен відрізнятись від стандартних (установлених за замовчуванням) "public", "private" та "system" і повинен відрізнятись від паролів, що використовуються в діалоговому режимі. Де можливо, повинен використовуватись ключовий хеш (наприклад SNMPv2).
- Новий обліковий запис повинен бути заблокованим, якщо він не був активованим протягом 40 днів (параметр повинен мати можливість налаштування) після генерації.
- Термін дії пароля не повинен перевищувати 60 днів (параметр повинен мати можливість налаштування, але не більше 365 днів). Для зниження ризику виникнення помилки при вводі нового пароля, він повинен вводитися 2 рази в одному меню введення/зміни пароля (у т.ч. разом зі старим) і система повинна перевірити їх коректність на збіг і відповідність іншим параметрам даного розділу.
- У системі повинні зберігатися 10 попередніх паролів (параметр повинен мати можливість налаштування) користувачів. При зміні пароля користувачем, система повинна перевірити, щоб новий пароль не збігався з 10 попередніми паролями (параметр повинен мати можливість налаштування);
- Не менш ніж за 10 днів (параметр повинен мати можливість налаштування) до закінчення терміну дії пароля користувачеві (при кожному вході в систему) повинне видаватися повідомлення про закінчення терміну дії пароля із пропозицією його зміни.
- Після третього підряд неправильного введення пароля, не залежно від часу логіна (параметр повинен мати можливість налаштування), обліковий запис повинен бути заблокований. Період часу, на який повинен блокуватись обліковий запис, не менше 10 хвилин

(параметр повинен мати можливість налаштування). При повторному блокуванні після чергових трьох невдалих спроб уведення пароля - обліковий запис повинен бути заблокований. При цьому система аутентифікації повинна сформулювати та відправити адміністраторові безпеки та/або адміністраторові системи спеціальне повідомлення, що сигналізує про спробу підбору паролю (механізм можна реалізовувати повідомленням по електронній пошті, відправленням СМС і виводом сигнальної (аудіо і у вигляді спливаючого вікна на моніторі адміністратора) інформації.

- Розблокування облікового запису можливе тільки працівником у ролі адміністратора користувачів і/або адміністратора безпеки і/або системи, залежно від реалізації прав адміністраторів у системі.

- Заборонено використовувати для роботи/активації автоматичних і автоматизованих технологічних процесів і входу в системи інженерні облікові записи (які використовувались при розробці системи) і паролі виробника.

- Пароль для первісного входу в систему, призначений адміністратором повинен бути унікальним, і може бути використаний тільки для виводу на екран пропозиції про зміну пароля на новий і повинен бути змінений користувачем при першому вході в систему (повинна виводитися інформація для користувача про обов'язкову зміну пароля і вимогах до складності пароля). Доступ у систему з первинним паролем, призначеним адміністратором системи/користувачів, надаватися не повинен. Відповідальність за зміну первісного пароля в систему(и) несе користувач системи. Відповідальність за підтримку вимог діючих політик в АС несе адміністратор АС і його безпосередній і/або прямі керівники.

- При використанні технічних ресурсів Банку, при кожній спробі входу в систему повинна відображатися на українській або англійській мовах інформація наступного змісту (параметр повинен мати можливість налаштування): "Увага: Ви не маєте права користуватися комп'ютером, якщо ви не є працівником АТ «ПРАВЕКС БАНК, чи з Вами не підписано відповідного договору».

- У адміністратора системи повинна бути можливість блокування й розблокування облікового запису, у тому числі на заданий період часу.

- Всі спроби (вдалого і невдалого) входу, виходу в АС повинні фіксуватися в контрольних журналах із вказівкою імені, результатів перевірки пароля, дати, часу, IP і MAC-адреси (MAC - по можливості) користувача системи. Такі контрольні журнали повинні бути захищені від модифікації.

- Паролі адміністраторів повинні відповідати тим же вимогам, що й користувачів, за винятком довжини пароля - мати не менш 12 символів і термін дії пароля - можуть мати більш тривалий строк дії, але не більше 90 днів (параметр повинен мати можливість налаштування, але не більше 90 днів).

- Система не повинна дозволяти одночасне підключення декількох користувачів до однієї автоматизованої системи/сервісу під одним обліковим записом.

- Система не повинна дозволяти одночасне одержання доступу різних користувачів до однієї автоматизованої системи/сервісу з однієї робочої станції (перевірка за ім'ям робочої станції та/або IP-адресою).

6.21. Якщо з технічних причин вищезазначені вимоги не можуть бути реалізовані, то для впровадження нестандартної системи парольного захисту необхідно одержати погодження ДУІБтаББ.

6.22. Необхідно пам'ятати, що ні за яких умов пароль не повинен бути відомий третім особам, і ніхто і ні при яких обставинах не має права вимагати від суб'єкта розкриття пароля. Кожен працівник Банку/Постачальника несе персональну відповідальність за збереження своїх паролів і всі дії, зроблені в системі, вхід у яку виконаний з його використанням.

6.23. У випадку виникнення підозри на компрометацію пароля або його копії, необхідно негайно зробити наступні дії:

- a. вийти із системи, якщо ввійшли в неї. Якщо не входили, то не входити в систему;
- b. заблокувати доступ до комп'ютера, якщо він не заблокований;
- c. негайно повідомити про підозру свого безпосереднього керівника, адміністратора системи/користувачів для одержання нового облікового запису, у тому числі необхідно відразу ж інформувати будь-кого з працівників ДУІБтаББ,

за допомогою дзвінка на робочий або мобільний телефон, а також відправивши дублююче повідомлення електронною поштою та в систему JIRA;

- d. при одержанні такого повідомлення, адміністратор зобов'язаний негайно (у будь-який час доби будь-якими доступними засобами) інформувати працівників ДУІБтаББ для одержання подальших вказівок. Адміністраторові системи заборонено блокувати "скомпрометований" обліковий запис до одержання відповідних вказівок від працівників ДУІБтаББ, якщо вони були інформовані про інцидент, для відстеження дій потенційного злоумисника.
- e. Ніхто не має права вживати які-небудь дії для входу в систему під старим ім'ям і зі старим паролем.

**6.24. Вимоги до управління доступом:**

Доступ до інформаційних ресурсів Банку дозволяється користувачам, які пройшли процедуру багатофакторної ідентифікації.

6.25. Усі події (у тому числі невдалі спроби) фіксується в захищеному від несанкціонованої модифікації електронному журналі моніторингу, в якому забезпечується фіксація наступних подій:

- використання ідентифікаційного та аутентифікаційного механізму;
- запит на доступ до інформаційного ресурсу;
- опис ресурсу до якого запитується доступ;
- тип доступу;
- результат обробки запиту.

6.26. Записи журналу моніторингу мають бути доступні для пошуку, класифікації та формування звітів. Журнал моніторингу періодично переглядається ДУІБтаББ. Результатами перегляду є впроваджені коригувальні або попереджувальні дії (в разі фіксації критичних подій).

6.27. Факт порушення будь-яких визначених документом положень являє собою інцидент інформаційної безпеки. За всіма виявленими інцидентами фахівці ДУІБтаББ збирають інформацію і при необхідності проводять службові перевірки із зазначенням своєї експертної оцінки і проведеними (запропонованими) коригуючими і попереджувальними діями.

## **7 РОЛІ ТА ВІДПОВІДАЛЬНОСТІ**

Керівництво Банку чітко розуміє, що інформаційна безпека Банку є основою життєдіяльності Банку та сприяє (організаційно та фінансово) впровадженню, контролю та підтримці прийнятої Політики.

Документи системи управління інформаційною безпекою доступні працівникам третіх сторін у межах їх повноважень і призначені надавати допомогу у виконанні вимог інформаційної безпеки (відповідно до договору про співробітництво).

Постійний контроль впровадження, виконання, вдосконалення та підтримки Політики в актуальному стані покладається на директора департаменту управління інформаційною безпекою та безперервністю бізнесу.

Кожний працівник несе відповідальність за порушення положень Політики в межах, встановлених законодавством України та у відповідності до договорів підписаних між Банком та постачальником/контрагентом/клієнтом.

## **8 ПЕРЕГЛЯД ДОКУМЕНТУ**

Політика підтримується в актуальному стані та переглядається за необхідності, але не рідше одного разу на рік.

Причинами внесення змін до Політики, є зміни в законодавстві України, в інформаційній інфраструктурі та/або впровадження нових інформаційних технологій, доповнення регулюючих, внутрішньо-нормативних документів Банку.

## Додаток 1 до Політики

**Банківською таємницею (БТ) є інформація визначена Законом України «Про банки і банківську діяльність», зокрема, але не виключно:**

- відомості про банківські рахунки клієнтів, у тому числі кореспондентські рахунки Банку у Національному банку України (НБУ) та у банках-контрагентах;
- інформація про операції, які були проведені на користь чи за дорученням клієнта, вчинені ним правочини;
- фінансово-економічний стан клієнтів;
- інформація про організацію та здійснення охорони Банку та осіб, які перебувають у приміщеннях Банку;
- інформація про організаційно-правову структуру юридичної особи – клієнта, її керівників, напрями діяльності;
- відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;
- інформація щодо звітності Банку, за винятком тієї, що підлягає опублікуванню;
- коди, що використовуються Банком для захисту інформації.

Інформація про Банк чи клієнтів Банку, що збирається під час здійснення банківського нагляду, валютного нагляду, нагляду (оверсайту) платіжних систем та систем розрахунків, а також нагляду у сфері запобігання та протидії легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення, становить банківську таємницю.

Перелік інформації, яка підлягає обов'язковому опублікуванню, встановлюється Регуляторними органами, зокрема Національним банком України, Національною комісією з цінних паперів та фондового ринку, та додатково самим Банком.

*Приклад інформації, яка містить БТ:*

- документація (паперова чи електронна), що містить відомості про держателя картки, а саме: номер платіжної карти (PAN), а також ім'я держателя картки, сервісний код, дата закінчення терміну дії картки, якщо вони зберігаються разом з PAN;
- журнал (реєстр) фінансових операцій, які підлягають фінансовому моніторингу;
- довідки НБУ, складені за результатами перевірки Банку з питань дотримання вимог чинного законодавства, що регулюють питання запобігання (протидії) відмивання доходів, одержаних злочинним шляхом та фінансування тероризму чи з інших питань;
- і таке інше.

### **Відомості, що становлять комерційну таємницю (КТ) Банку**

Комерційною таємницею є інформація про діяльність Банку, розголошення якої може призвести до фінансових чи іміджевих втрат Банку, чи недоотримання Банком прибутку.

Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

Склад і обсяг відомостей, що становлять комерційну таємницю, порядок її захисту, правила обробки та доступу до неї визначаються Банком самостійно з дотриманням чинного законодавства України.

*Зокрема, комерційну таємницю Банку становлять:*

- **Відомості стосовно принципів управління Банком:**

- відомості про підготовку, прийняття і виконання окремих рішень керівництва Банку з усіх нижче перелічених питань;
  - відомості про перспективні плани та методи управління Банком;
  - відомості про факти підготовки, цілі та ведення ділових переговорів, про предмет і цілі нарад і засідань органів управління Банку;
  - документація Правління Банку, Наглядової Ради Банку, загальних зборів акціонерів;
- **Відомості про фінансову діяльність Банку (якщо вона не є оприлюдненою за рішенням керівництва Банку):**
    - відомості, що розкривають показники фінансового плану;
    - відомості про планові та звітні дані по валютних операціях;
    - відомості про продукти, що розробляються Банком;
    - відомості про специфіку міжнародних розрахунків з іншими банками;
    - відомості про стратегію і тактику у валютних і кредитних питаннях;
    - відомості про методи розрахунків, структуру і розмір знижок;
    - відомості про кредитні та валютні відносини з іноземними банками і фірмами;
    - відомості про умови взаємовідносин сторін за договорами (контрактами);
    - відомості про умови платежів за контрактами;
    - відомості про порядок користування печаткою та штампами Банку;
    - зразки підписів і відбитків печаток.
  - **Відомості в області програмного забезпечення Банку:**
    - документація щодо програмного забезпечення, що використовується в Банку;
    - програмне забезпечення, що використовується в роботі Банку;
    - відомості про структуру інформаційно-обчислювальної мережі Банку;
    - документація Банку, що регламентує порядок використання програмного забезпечення, баз даних та телекомунікаційного обладнання;
    - документація стосовно системи захисту інформаційних активів Банку та порядок її використання.
  - **Інші відомості:**
    - відомості про порядок та стан організації захисту банківської, комерційної таємниці і іншої інформації яка обробляється в інформаційних системах Банку
  - **Відомості про персонал Банку**
    - відомості, що містяться в особових справах працівників Банку;
    - відомості про заплановані зміни в кадровій політиці Банку;
    - відомості про фонд заробітної плати.
  - **Відомості про систему матеріально-технічного забезпечення Банку**
    - відомості про транспортні та енергетичні потреби Банку;
    - відомості про маршрути та цілі поїздок банківського транспорту;
    - відомості про розташування складських і підсобних приміщень, режимі надходження цінностей, обладнання та іншого майна;
    - відомості про системи банківського телефонного та радіозв'язку.
  - **Відомості, що носять конфіденційний характер**
    - відомості про паролі та коди, що використовуються працівниками Банку для доступу до банківських комп'ютерних програм, локальної мережі, мережевого та серверного обладнання, а також для доступу до мережі Інтернет;
    - відомості та документи стосовно здійснення в Банку процедур, пов'язаних з протидією легалізації доходів, одержаних злочинним шляхом, та фінансування тероризму, в тому числі акти, складені за результатами аудиторських перевірок;
    - персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована;

- інформація стосовно діяльності підрозділів, що займаються безпекою Банку.

**Комерційну таємницю не становлять:**

- установчі документи, документи, що дозволяють займатися підприємницькою діяльністю та її окремими видами;
- інформація за всіма встановленими формами державної звітності;
- дані, необхідні для перевірки обчислення і сплати податків та інших обов'язкових платежів;
- відомості про чисельність і склад працюючих, їхню заробітну плату в цілому та за професіями й посадами, а також наявність вільних робочих місць;
- документи про сплату податків і обов'язкових платежів;
- інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізацію продукції, що завдає шкоду здоров'ю, а також інші порушення законодавства України та розміри заподіяних при цьому збитків;
- документи про платоспроможність;
- відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, спілках, об'єднаннях та інших організаціях, які займаються підприємницькою діяльністю;
- відомості, що відповідно до чинного законодавства підлягають оголошенню.

**Перелік інформації, що становить персональні дані**

1. ПІБ клієнтів;
2. Адреса клієнтів;
3. Телефон клієнтів;
4. Паспортні дані клієнтів;
5. Реєстраційний номер облікової картки платника податків клієнтів;
6. Фінансова інформація клієнтів;
7. ПІБ працівників Банку;
8. Паспортні дані працівників;
9. Дата та місце народження працівників;
10. Місце проживання фактичне та за державною реєстрацією працівників;
11. Громадянство працівників;
12. Освіта, професія, спеціальність, кваліфікація, трудовий стаж працівників;
13. Стать, сімейний стан, склад сім'ї працівників;
14. Відомості про військовий облік працівників;
15. Індивідуальний податковий номер працівників;
16. Дані, що підтверджують право працівника на пільги встановлені законодавством про працю, та законодавством про захист інвалідів;
17. Житлові умови працівників;
18. Номери телефонів, електронні адреси, фотографії працівників.

**Перелік вимог АТ «ПРАВЕКС БАНК»  
щодо забезпечення інформаційної безпеки  
при взаємодії з третіми сторонами**

**1. Правила безпеки для захисту інформаційних активів АТ «ПРАВЕКС БАНК»**

1.1. ПОСТАЧАЛЬНИК зобов'язується при наданні послуг виконувати вимоги актуальної версії Політики інформаційної безпеки (зовнішньої) АТ «ПРАВЕКС БАНК» (далі – Політика) в межах, які стосуються забезпечення інформаційної безпеки при виконанні умов договору.

1.2. ПОСТАЧАЛЬНИК повинен обробляти дані відповідно до їхнього рівня класифікації, приділяючи особливу увагу забезпеченню відповідного рівня конфіденційності.

1.3. ПОСТАЧАЛЬНИК визнає та приймає умови про конфіденційність інформації, що містить інформацію про архітектуру та конфігурацію інформаційної систем Банку, заходи безпеки, будь-яких вразливостей, виявлених під час надання Послуги.

1.3.1. При виявленні вразливостей в програмному забезпеченні, яке надає/створює ПОСТАЧАЛЬНИК, він зобов'язується у найкоротший термін забезпечити закриття виявлених вразливостей. Проведення зазначених робіт здійснюється за рахунок ПОСТАЧАЛЬНИКА.

1.4. ПОСТАЧАЛЬНИК визнає виключне право власності Банку на дані, програмне забезпечення, технічну та нормативну документацію та ІКТ-ресурси Банку, якщо вони використовуються або іншим чином надаються ПОСТАЧАЛЬНИКУ у використанні для виконання умов договору.

1.5. ПОСТАЧАЛЬНИК визнає право Банку в будь-який час відкликати дозвіл на здійснення будь-якої діяльності та роботу з ресурсами Банку при порушенні вимог Політики.

1.6. ПОСТАЧАЛЬНИК зобов'язується у будь-якому випадку розірвання Договору з Банком забезпечити видалення усієї інформації, яка буда отримана від Банку, за допомогою засобів, які унеможливають її відтворення. Після знищення інформації – ПОСТАЧАЛЬНИК надає Банку відповідний гарантійний лист/акт про знищення інформації

1.7. При розірванні договору, чи завершенні надання послуг - ПОСТАЧАЛЬНИК повертає Банку усі матеріальні та нематеріальні активи (у тому числі ліцензії), які були отримані від Банку для надання відповідних послуг.

1.8. При наданні послуг ПОСТАЧАЛЬНИК зобов'язується використовувати міжнародні стандарти інформаційної безпеки та найкращі міжнародні практики з забезпечення інформаційної безпеки.

1.9. ПОСТАЧАЛЬНИК зобов'язується виконувати вимоги безпеки, описані в додатку 2 до Політики, також у випадках, коли Послуга надається в режимі дистанційної роботи. У випадку, якщо персонал ПОСТАЧАЛЬНИКА працює за межами території України, він повинен отримати попередній дозвіл від Банку на здійснення діяльності поза межами України.

**2. Контактні особи з питань безпеки**

2.1. ПОСТАЧАЛЬНИК зобов'язаний надати інформацію про контактну особу, з якою Банк зможе зв'язатися у разі виникнення інциденту ІТ-безпеки чи наявності у Банку інформації про такий інцидент.

**3. Персонал та організація ПОСТАЧАЛЬНИКА**

Стосовно персоналу, який бере участь у виконанні договірних зобов'язань (включаючи працівників, які працюють у будь-якій якості), ПОСТАЧАЛЬНИК зобов'язується, забезпечити наступні вимоги з забезпечення інформаційної безпеки, протягом терміну дії договору, а саме:

3.1. гарантувати, що персонал який залучається до надання послуг, має відповідну кваліфікацію;

3.2. гарантувати, що працівники проходять підготовку, необхідну для виконання своїх завдань, а також пройшли відповідні курси з інформаційної безпеки;

3.3. запроваджувати належну політику щодо розподілу обов'язків під час призначення завдань;

3.4. розподіляти завдання та обов'язки між своїми працівниками таким чином, щоб забезпечити ефективний моніторинг ключових внутрішніх і зовнішніх загроз;

3.5. прийняти формальні та безпечні процедури для негайного відкликання облікових даних користувача та забезпечити повернення всіх інструментів, які використовувалися для виконання договірних дій, включаючи перепустки, ключі та інші засоби доступу, засоби багатфакторної ідентифікації, якщо його працівники переведені на інші проекти/посади або з ними розірвано/припинено відносини.

3.6. У випадку зміни в організаційно штатній структурі ПОСТАЧАЛЬНИКА доводити інформацію про нові посади осіб, які надають відповідні послуги Банку.

3.7. ПОСТАЧАЛЬНИК зобов'язується не вносити зміни в організацію послуг і ланцюгу поставок, які можуть знизити рівень забезпечення безпеки сервісу, який надається.

#### **4. Фізична та логічна безпека ПОСТАЧАЛЬНИКА**

4.1. Знищення даних/носіїв інформації після припинення діяльності, передбаченої контрактом, має відбуватися відповідно до процедур і стандартів, які відповідають вимогам безпеки, та погоджені з Банком.

4.2. ПОСТАЧАЛЬНИК зобов'язується прийняти відповідні процедури для відокремлення даних, якими він керує від імені Банку, від даних, якими він керує від імені інших клієнтів, щоб забезпечити конфіденційність, доступність і цілісність таких даних.

#### **5. Розробка та супровід програмного забезпечення**

5.1. У разі розробки або обслуговування програмного забезпечення, або діяльності, яка передбачає створення/модифікацію програмного забезпечення, що використовується Банком, ПОСТАЧАЛЬНИК зобов'язується використовувати безпечні методи розробки програмного забезпечення, які включають, принаймні, перевірку вхідних даних, перевірки внутрішньої обробки, перевірки дійсності повідомлень і вихідних даних, використання передового досвіду щодо конкретної мови програмування, або використовуваного середовища розробки. Ця вимога особливо стосується розробки веб-додатків, протягом усього терміну дії договору з Банком та протягом дії гарантійного терміну.

5.2. ПОСТАЧАЛЬНИК зобов'язується дотримуватися вказівок щодо безпечного програмування, що містяться в Open Web Application Security Project (OWASP) і CWE/SANA.

5.3. Якщо розробка стосується застосування продукту в рамках, на які розповсюджуються вимоги з PCI-DSS, ПОСТАЧАЛЬНИК зобов'язується тримати своїх членів команди в курсі вимог з техніки розробки безпечного коду шляхом відповідної ініціативи навчання щонайменше раз на рік.

#### **6. Підключення до інформаційних ресурсів, що належать Банку.**

У разі якщо діяльність ПОСТАЧАЛЬНИКА в межах дії Договору передбачає підключення до інформаційних ресурсів Банку, ПОСТАЧАЛЬНИК гарантує:

(а) використовувати лише виділені лінії доступу попередньо погоджуючи з Банком, з використанням фіксованого переліку IP-адрес з яких буде здійснюватися підключення;

(б) при наданні доступу – ПОСТАЧАЛЬНИК надає заявку до системи Jira з повним описом типу з'єднання та переліком портів;

(с) доступ надається лише на час дії договору. У випадку продовження дії договору – створюється додатковий запит на доступ до інформаційних ресурсів Банку;

(д) при доступі до інформаційних ресурсів Банку ПОСТАЧАЛЬНИК гарантує, що доступ буде здійснюватися виключно для надання послуг в межах Договору;

(е) при підключенні до інформаційних ресурсів Банку ПОСТАЧАЛЬНИК гарантує виконання усіх вимог чинних внутрішніх нормативних документів Банку, які врегульовують питання інформаційної безпеки Банку.

(ф) ПОСТАЧАЛЬНИК визнає та погоджується з тим, що Банк може контролювати усі дії ПОСТАЧАЛЬНИКА при підключенні до інформаційних ресурсів Банку, та зобов'язується надати Банку пояснення у випадку виникнення питань, які можуть виникати під час проведення контрольних заходів в найкоротші терміни, але не пізніше ніж через добу з моменту отримання запиту.

## **7. Діяльність щодо обслуговування обладнання, яке належить Банку**

7.1. У разі вилучення або заміни ІТ-обладнання, яке використовується Банком, та/або будь-яких пристроїв зберігання даних, що містять комп'ютерні програми чи дані, які належать Банку та/або клієнтам Банку, а також усі дані, що містяться в запам'ятовуючих пристроях, які підлягають заміні – зазначені дані повинні бути остаточно стерті ПОСТАЧАЛЬНИКОМ після перенесення даних на нове обладнання або на відповідний носій, на вимогу Банку.

7.2. У всіх заходах з технічного обслуговування та всіх заходах з проектування системи та керування мережею слід вживати запобіжних заходів (у координації з Банком) – щоб уникнути випадкової чи іншої втрати даних, включаючи дані, що зберігаються на іншому обладнанні, крім того, що підлягає технічному обслуговуванню.

## **8. Адміністрування інформаційних ресурсів.**

8.1. ПОСТАЧАЛЬНИК повинен підтримувати оновлений список «системних адміністраторів», уповноважених працювати з даними або системами Банку, і надавати ці відомості на запит та/або відповідно до узгодженої періодичності.

8.2. ПОСТАЧАЛЬНИК проводить необхідні перевірки надійності заздалегідь захисту адміністративних облікових записів, та будь-які інші регулярні перевірки, які забезпечують відповідний рівень інформаційної безпеки ПОСТАЧАЛЬНИКА, та інформує Банк про їх проведення.

8.3. Доступ до інформаційних ресурсів Банку, персоналу ПОСТАЧАЛЬНИКА вимагає застосування засобів багатфакторної ідентифікації.

## **9. Перелік додаткових вимог, які вносяться до договорів з ПОСТАЧАЛЬНИКОМ**

9.1. При наданні послуги з розробки, модернізації чи внесенні інших змін виконавець гарантує:

- Що вся інформація, яка стала відома ПОСТАЧАЛЬНИКУ під час взаємодії з Банком, вважається інформацією з обмеженим доступом.
- ПОСТАЧАЛЬНИК забезпечує конфіденційність інформації з обмеженим доступом протягом п'яти років з моменту її отримання;
- У разі припинення дії договору – ПОСТАЧАЛЬНИК забезпечує видалення усіх даних, які були отримані від Банку, та надає Банку протягом п'яти робочих днів з моменту припинення договору, завірені відповідним чином акти виконаних робіт про знищення інформації. При цьому інформація знищується методом, який гарантовано унеможлиблює її відтворення;
- Доступ до інформації з обмеженим доступом, отримують виключно працівники ПОСТАЧАЛЬНИКА, які мають необхідну (підтверджену на момент виконання робіт) кваліфікацію, та які підписали відповідні зобов'язання про нерозголошення інформації;
- Залучення до виконання робіт третіх сторін ПОСТАЧАЛЬНИКОМ заборонено без попередньої оцінки зазначених сторін зі сторони ДУІБтаББ Банку.
- При створенні ПЗ – ПОСТАЧАЛЬНИК гарантує (та несе юридичну та фінансову відповідальність):
  - o відсутність у програмному коді зловмисного коду, чи функцій, які не санкціоновано здійснюють збір інформації;
  - o відсутність у програмному коді відомих вразливостей, а у разі їх виявлення після впровадження – гарантує їх закриття на безоплатній основі протягом погодженого з Банком терміну, який не може перевищувати 15 календарних днів;
  - o виправлення помилок у програмному коді здійснюється за рахунок ПОСТАЧАЛЬНИКА у погоджений з Банком термін.

## Додаток 3 до Політики

### Формат сповіщення Банку про інцидент інформаційної безпеки

Заповнюється ПОСТАЧАЛЬНИКОМ із усією наявною та застосовною інформацією, пов'язаною з конкретною подією, що сталася.

### ЗАГАЛЬНА ІНФОРМАЦІЯ

#### Загальний опис події

*Будь ласка, введіть всю необхідну інформацію, яка дозволить отримати уявлення про подію, що сталася*

#### Хронологія події

1. Дата та час виявлення <sup>1</sup>події: \_\_\_\_\_
2. Дата і час настання події, якщо відомо: \_\_\_\_\_
3. Дата та час закриття заходу, якщо є: \_\_\_\_\_

#### Хто в компанії виявив подію?

| <u>Внутрішня організація</u>                                  |                          | <u>Зовнішня організація</u>           |                          |
|---------------------------------------------------------------|--------------------------|---------------------------------------|--------------------------|
| ІТ безпека                                                    | <input type="checkbox"/> | Зовнішній аудитор                     | <input type="checkbox"/> |
| ІМТ / внутрішні функції (бізнес або підтримка) – співробітник | <input type="checkbox"/> | Сторонній постачальник                | <input type="checkbox"/> |
|                                                               |                          | Клієнт/ Користувач платіжного сервісу | <input type="checkbox"/> |
| Внутрішній аудит                                              | <input type="checkbox"/> | Нападник (попередження)               | <input type="checkbox"/> |
| <u>Інший</u>                                                  |                          |                                       | <input type="checkbox"/> |
| <i>Будь ласка уточніть:</i>                                   |                          |                                       |                          |

<sup>1</sup> У разі порушення даних, виявленого зовнішнім постачальником, датою та часом виявлення вважається момент, коли повідомлення від постачальника надходить до компетентного контактної пункту юридичної особи Intesa Sanpaolo Group, як зазначено в угоді.

## ТАКСОНОМІЯ ПОДІЙ

| Кіберподія                      |                          |                          |                          |                                                            |                          |                                                   |                          |
|---------------------------------|--------------------------|--------------------------|--------------------------|------------------------------------------------------------|--------------------------|---------------------------------------------------|--------------------------|
| Шкідливе програмне забезпечення |                          | Соціальна інженерія      |                          | Інсайдерська подія/подія стороннього постачальника         |                          | Несанкціонований доступ                           |                          |
| програми-вимагачі               | <input type="checkbox"/> | Фішинг / * фішинг        | <input type="checkbox"/> | Випадкове зловживання правами доступу                      | <input type="checkbox"/> | Атака грубою силою                                | <input type="checkbox"/> |
| троянський кінь                 | <input type="checkbox"/> | Фішинг                   | <input type="checkbox"/> | Навмисне зловживання правами доступу постачальником послуг | <input type="checkbox"/> | Ін'єкція зловмисного сценарію та/або керування ОС | <input type="checkbox"/> |
| Вірус                           | <input type="checkbox"/> | Претекстування           | <input type="checkbox"/> | Навмисне зловживання правами доступу інсайдером            | <input type="checkbox"/> | SQL ін'єкція                                      | <input type="checkbox"/> |
| Черв'як                         | <input type="checkbox"/> | Кіберприсідання          | <input type="checkbox"/> | Порушення політики (інсайдер або TRP)                      | <input type="checkbox"/> | Інша використана вразливість                      | <input type="checkbox"/> |
| Шпигунське/рекламне ПЗ          | <input type="checkbox"/> | Інша соціальна інженерія | <input type="checkbox"/> | Інша внутрішня загроза/TRP                                 | <input type="checkbox"/> | Інформаційний вплив                               | <input type="checkbox"/> |
| Мобільні шкідливі програми      | <input type="checkbox"/> |                          |                          |                                                            |                          | Інша подія несанкціонованого доступу              | <input type="checkbox"/> |
| Інші шкідливі програми          | <input type="checkbox"/> |                          |                          |                                                            |                          |                                                   |                          |

| <u>Атака на відмову в обслуговуванні</u> |                          | <u>Інші кіберподії</u>                          |                          | <u>Додаткова класифікація : класифікується як АРТ?</u> |  |
|------------------------------------------|--------------------------|-------------------------------------------------|--------------------------|--------------------------------------------------------|--|
| DoS                                      | <input type="checkbox"/> | Псування                                        | <input type="checkbox"/> | <u>Будь ласка, вкажіть :</u>                           |  |
| DDos                                     | <input type="checkbox"/> | Зловживання брендом у ЗМІ та соціальних мережах | <input type="checkbox"/> |                                                        |  |
|                                          |                          | Наклеп на головних осіб у ЗМІ та соцмережах     | <input type="checkbox"/> |                                                        |  |
|                                          |                          | Сканування вразливостей                         | <input type="checkbox"/> |                                                        |  |
|                                          |                          | Інший                                           | <input type="checkbox"/> |                                                        |  |

| Оперативна подія                                                                                                                                                                          |                          |                                                            |                          |                                            |                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|------------------------------------------------------------|--------------------------|--------------------------------------------|------------------------------|
| <u>Збій процесу</u>                                                                                                                                                                       | <input type="checkbox"/> | <u>Випадкові події</u><br>(наприклад, помилка людини)      | <input type="checkbox"/> | <u>Проблема ПЗ/збій системи</u>            | <input type="checkbox"/>     |
| <u>Проблема HW</u>                                                                                                                                                                        | <input type="checkbox"/> | <u>Інфраструктурні проблеми</u><br>(внутрішні та зовнішні) | <input type="checkbox"/> | <u>Відсутність ключових осіб / навичок</u> | <input type="checkbox"/>     |
| <u>Зовнішні події</u> (природні, соціально-політичні, кримінальні, проблеми транспорту, проблеми навколишнього середовища, здоров'я /санітарія, війни/конфлікти, пандемії, інші зовнішні) |                          |                                                            |                          | <input type="checkbox"/>                   | <u>Інша оперативна подія</u> |
| <u>Будь ласка, вкажіть:</u>                                                                                                                                                               |                          |                                                            |                          |                                            |                              |

## ПЕРИМЕТР АТАКИ

| Географічне розширення                |                          |               |
|---------------------------------------|--------------------------|---------------|
| Виберіть географічне розширення подій |                          |               |
| <u>Міжнародний</u>                    | <input type="checkbox"/> | <u>Регіон</u> |
| <u>Країна</u>                         | <input type="checkbox"/> | <u>Місто</u>  |
| <u>Будь ласка, вкажіть:</u>           |                          |               |

| Контрзаходи активовано / Буде активовано                             |                          |                                                    |                          |
|----------------------------------------------------------------------|--------------------------|----------------------------------------------------|--------------------------|
| Будь ласка, уточніть, чи були активовані контрзаходи внаслідок події |                          |                                                    |                          |
| <u>BCP активований</u>                                               | <input type="checkbox"/> | <u>DRP активований</u>                             | <input type="checkbox"/> |
| <u>Кіберстрахування</u>                                              | <input type="checkbox"/> | <u>інший план на випадок надзвичайних ситуацій</u> | <input type="checkbox"/> |
| <u>Інші надзвичайні заходи активовані</u>                            | <input type="checkbox"/> | <u>Активовано інші контрзаходи</u>                 | <input type="checkbox"/> |
| <u>Інші контрзаходи, які будуть активовані</u>                       | <input type="checkbox"/> | <u>Будь ласка, вкажіть:</u>                        |                          |

| <u>Загальний вплив</u>        |                          |                                    |                          |
|-------------------------------|--------------------------|------------------------------------|--------------------------|
| На який вимір вплинула подія? |                          |                                    |                          |
| Доступність <sup>2</sup>      | <input type="checkbox"/> | Цілісність <sup>3</sup>            | <input type="checkbox"/> |
| Конфіденційність <sup>4</sup> | <input type="checkbox"/> | Автентичність <sup>5</sup>         | <input type="checkbox"/> |
| Безперервність <sup>6</sup>   | <input type="checkbox"/> | Будь ласка, вкажіть <sup>7</sup> : |                          |

| <u>Постраждав комерційний канал (Якщо застосовно)</u> |                          |                                  |                          |
|-------------------------------------------------------|--------------------------|----------------------------------|--------------------------|
| Комерційний канал, який постраждав від події          |                          |                                  |                          |
| Відділення                                            | <input type="checkbox"/> | Мобільний банкінг                | <input type="checkbox"/> |
| Електронний банкінг                                   | <input type="checkbox"/> | банкомати                        | <input type="checkbox"/> |
| Телефонний банкінг                                    | <input type="checkbox"/> | Точка продажу                    | <input type="checkbox"/> |
| Інший                                                 | <input type="checkbox"/> | Якщо інше, будь ласка, вкажіть : |                          |
| <u>Додаткова інформація :</u>                         |                          |                                  |                          |

| <u>Тип порушення процесу/послуги</u>                                                           |                          |                                       |                          |
|------------------------------------------------------------------------------------------------|--------------------------|---------------------------------------|--------------------------|
| Тип збою, викликаного подією в службі та компонентах                                           |                          |                                       |                          |
| Уповільнення                                                                                   | <input type="checkbox"/> | Несправність (часткова недоступність) | <input type="checkbox"/> |
| Повна недоступність                                                                            | <input type="checkbox"/> | Інший                                 | <input type="checkbox"/> |
| Будь ласка, вкажіть кількість внутрішніх користувачів, які експериментують з наслідками події: |                          |                                       |                          |
| <u>Додаткова інформація :</u>                                                                  |                          |                                       |                          |

| <u>Тип постраждалих клієнтів (якщо застосовно)</u>                                                                            |                          |                    |                          |
|-------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------|--------------------------|
| Чи має подія якісь наслідки для клієнтів? Якщо так, будь ласка, вкажіть тип клієнта, який експериментував з наслідками події. |                          |                    |                          |
| Роздрібні клієнти                                                                                                             | <input type="checkbox"/> | Приватні клієнти   | <input type="checkbox"/> |
| Корпоративний                                                                                                                 | <input type="checkbox"/> | Фінансові установи | <input type="checkbox"/> |
| Будь ласка, вкажіть :                                                                                                         |                          |                    |                          |

## Кореляція подій

<sup>2</sup> Властивість процесу/послуги бути доступною та придатною для використання користувачами та клієнтами

<sup>3</sup> Властивість захисту точності та повноти активів (включаючи дані)

<sup>4</sup> Властивість, що інформація не стає доступною та не розкривається неавторизованим особам, організаціям або процесам

<sup>5</sup> Властивість джерела – це те, за що воно претендує

<sup>6</sup> Властивість процесів, завдань і послуг організації бути повністю доступними та працювати на прийнятних попередньо визначених рівнях

<sup>7</sup> У випадку персональних даних, будь ласка, складіть спеціальну таблицю для порушення безпеки персональних даних

|                                                                              |                          |                                             |                          |
|------------------------------------------------------------------------------|--------------------------|---------------------------------------------|--------------------------|
| <i>Оцініть, чи подія пов'язана з іншими подіями (загрозою чи інцидентом)</i> |                          |                                             |                          |
| <i>Окремий захід</i>                                                         | <input type="checkbox"/> | <i>Повторне виникнення тієї самої події</i> | <input type="checkbox"/> |
| <i>Подія, пов'язана з іншою подією</i>                                       | <input type="checkbox"/> | <i>Інший</i>                                | <input type="checkbox"/> |
| <i><u>Будь ласка, вкажіть:</u></i>                                           |                          |                                             |                          |

*Загальні коментарі щодо периметра удару (необов'язковий файл)*