ПРАВЕКС БАНК
Bank of INTESA SANPAOLO

ЗАТВЕРДЖЕНО:
Правління АТ «ПРАВЕКС БАНК»

Протокол № 27_24 від 13.09.2024, питання 8 порядку денного

Реєстраційний номер № 257 від 13.09.2024

ПРАВЕКС БАНК
Bank of INTESA SANPAOLO

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АТ «ПРАВЕКС БАНК»

Класифікація документу за рівнем безпеки: Відкрита інформація

Перелік змін:

Версія	Власник	Ключові зміни	Скасовані документи
3.2.	Департамент управління інформаційною безпекою та безперервністю бізнесу	- уточнено вимоги щодо управління доступом до інформаційних ресурсів Банку; - додано розділ 7 "Навчання персоналу" та розділ 8 "Звітування та інформування".	- Політика інформаційної безпеки (зовнішня) АТ «ПРАВЕКС БАНК», затверджена Правлінням АТ "ПРАВЕКС БАНК", Протокол № 19_23 від 09.06.2023, питання 4 Порядку денного (№159 від 16.06.2023). - Політика інформаційної безпеки (скорочена) АТ «ПРАВЕКС БАНК», затверджена Рішенням Комітету з управління інформаційною безпекою АТ «ПРАВЕКС БАНК» від 21.10.2020 №3_20.1 (20.11.2020 №260).

Розміщення документу:
https://learning.pravex.ua – INTERNAL RULES & REGULATIONS BASE – GOVERNANCE DOCUMENTS – Guidelines - ICT and Security Management

Дата набуття чинності: 13.09.2024

ПРАВЕКС БАНК
Bank of INTESA SANPAOLO

Список погодження	
Голова Правління	☐
Головний бухгалтер	☐
Департамент внутрішнього аудиту	☐
Департамент юридичної підтримки та генерального секретаріату	☐
Департамент управління ризиками	☐
Департамент комплаєнсу та протидії легалізації доходів, отриманих злочинним шляхом	☒
Відділ зв'язків з громадськістю та маркетингу	☐
Департамент управління персоналом та організаційними змінами	☒
Департамент управління інформаційною безпекою та безперервністю бізнесу	☐
Головне управління бізнесу	☐
Головне фінансове управління	☐
Головне кредитне управління	☐
Головне операційне управління	☒

Список розсилання
Головний бухгалтер Департамент внутрішнього аудиту Департамент юридичної підтримки та генерального секретаріату Департамент управління ризиками Департамент комплаєнсу та протидії легалізації доходів, отриманих злочинним шляхом Відділ зв'язків з громадськістю та маркетингу Головне операційне управління Департамент управління персоналом та організаційними змінами Головне управління бізнесу Головне фінансове управління Відділення Відділ управління організаційними змінами та проектами

ПРАВЕКС БАНК
Bank of INTESA SANPAOLO

Зміст

1. ВСТУП

Політика інформаційної безпеки (зовнішня) АТ «ПРАВЕКС БАНК» (далі – Політика) описує прийняту та впроваджену АТ «ПРАВЕКС БАНК» (далі – Банк) політику щодо інформаційної безпеки при роботі з клієнтами та постачальниками Банку та 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:

- **Законів України**
  - Закону України "Про Національний банк України";
  - Закону України "Про банки і банківську діяльність";
  - Закон України «Про захист персональних даних»;
  - Закон України «Про платіжні послуги»;
  - Закон України «Про електронні документи та електронний документообіг»;
  - Закону України "Про захист інформації в інформаційно-телекомунікаційних системах";
  - Закону України "Про національну безпеку України";
  - Закону України "Про Інформацію»;
  - Закону України «Про електрону ідентифікацію та електронні довірчі послуги»;
  - Закон України «Про основні засади забезпечення кібербезпеки України»;
  - Закон України «Про ліцензування певних видів господарської діяльності»;
  - Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення».

- **Указів 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";
  - від 15 березня 2016 року № 96/2016 "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України".

- **Постанов Національного банку України**
  - Постанови № 99 від 14.09.2018 (Положення про порядок формування, зберігання та знищення відокремлених електронних даних, отриманих за результатами роботи інформаційних систем у Національному банку України і банках України);
  - Постанови №75 від 04.07.2018 (Положення про організацію бухгалтерського обліку, бухгалтерського контролю під час здійснення операційної діяльності в банках України – Додаток: Вимоги до інформаційного забезпечення операційної діяльності банку);
  - Постанови №178 від 12.08.2022 (Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України);
  - Постанови №58 від 03.05.2023 (Положення про автентифікацію та застосування посиленої автентифікації на платіжному ринку);
  - Постанови №172 від 20.12.2023 (Положення про використання електронного підпису та електронної печатки);
  - Постанови №243 від 17.08.2007 (Правила з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи);
  - Постанови №64 від 11.06.2018 (Положення про організацію системи управління ризиками в банках України та банківських групах);
  - Постанови №4 від 16.01.2021 (Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг);
  - Постанови № 42 від 08.03.2022 (Про використання банками хмарних послуг в умовах воєнного стану в Україні).

- **Національних стандартів України**
  - 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 інформаційної безпеки Материнської компанії Групи Інтеза Санпаоло, які не суперечать вимогам законодавства України;
- 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.
- інших нормативних документів України, які регулюють діяльність з питань захисту інформації в банківській сфері.

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, комерційну таємницю, таємницю надавача платіжних послуг, таємницю страхування, таємницю фінансової послуги, таємницю фінансового моніторингу, професійну таємницю на ринках капіталу та організованих товарних ринках, комерційну таємницю та персональні дані. Перелік видів інформації, що становить комерційну таємницю, наведений у Додатку 1 до цієї 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.

Керівництво Банку – Голова Правління, члени Правління Банку, члени Комітету з питань управління кризою, які вказані у Плані забезпечення безперервної діяльності та дій у разі виникнення надзвичайних ситуацій АТ «ПРАВЕКС БАНК» (п. 2.1.1).

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;

НБУ – Національний банк України;

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 оброблятись 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.

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.

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. 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 IT (сервери, робочі станції, міжмережеві екрани, принтери, копіювальна техніка, телекомунікаційне обладнання, обладнання зв'язку, маршрутизатори, АТС, факси, модеми тат 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).

6.2. 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.

6.3. 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.

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

6.5. Під час розроблення, впровадження та функціонування програмно-технічних комплексів враховуються вимоги інформаційної безпеки, з дотриманням нормативних актів вказаних у п. 1 цієї Політики.

6.6. 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 та рекомендаціям Групи «Інтеза Санпаоло», які не суперечать законодавству України;
- вимогам стандартів серії ISO 2700.

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

6.7. 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.

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

6.9. 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.

6.10. Про кожний інцидент інформаційної безпеки постачальник повинен повідомити Банк будь-якими доступними засобами, а потім оформити опис інциденту відповідно до Додатку 3 даної Політики, та надіслати його до ДУІБтаББ на адресу електронної пошти 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.

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

6.12. 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);
- засобами пошти НБУ.

6.13. 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, управління 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).

6.14. 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.

6.15. Для електронних платіжних документів цілісність забезпечується за допомогою використання кваліфікованого підпису, удосконаленого 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.

6.16. 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.

6.17. 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.

6.18. 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.

6.19. 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 уведення/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 уведення 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 сформувати 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).

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

6.21. 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.

6.22. 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 зловмисника;
e. ніхто не має права вживати які-небудь дії для входу в систему під старим ім'ям і зі старим паролем.

6.23. Вимоги до управління доступом:

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

Дистанційний доступ до інформаційних систем Банку може здійснюватися виключно:

- з використанням засобів, які належать Банку (комп'ютерна техніка, мобільні пристрої, ін.);
- з використанням шифрування каналів зв'язків на базі сертифікату особистого ключа КНЕДП Банку за гілкою RSA;
- з використанням сертифікованих засобів для зберігання особистих ключів криптографічного захисту (таких, як «Алмаз» та «Кристал»);
- з обов'язковим використанням шифрування засобу обчислювальної техніка, з якої надається доступ.

Доступ до інформаційних ресурсів надається виключно по завершенню ідентифікації користувача та ініціалізації усіх політик та систем захисту інформації, які використовуються в Банку.

6.24. Усі події (у тому числі невдалі спроби) фіксуються 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.

6.25. 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).

6.26. 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 попереджуючими діями.

6.27. Банк вживає заходів для захисту інформації з обмеженим доступом шляхом обмеження кола осіб, які мають доступ до такої інформації, спеціального порядку зберігання такої інформації, технічного захисту такої інформації або в інший спосіб, визначений Банком, а також для недопущення її неправомірного розголошення. Розголошення інформації з обмеженим доступом можливе лише у випадках і порядку, передбачених законом, внутрішніми документами Банку, договором.

7. НАВЧАННЯ ПЕРСОНАЛУ

7.1. У відповідності до вимог нормативних документів НБУ, міжнародних стандартів, внутрішніх документів Банку та рекомендацій Групи усі працівники Банку, які мають доступ до інформаційних ресурсів проходять навчання з питань інформаційної, фізичної, економічної безпеки та безпеки життя.

7.2. Для працівників Банку навчальний процес здійснюється з використанням відповідної електронної системи Банку, яка забезпечує:

- інформування працівника про призначення відповідного навчального курсу;
- ознайомлення з навчальними матеріалами у заплановані терміни;
- проходження оцінювання рівня знань;
- фіксацію результатів та підготовку статистичних звітів по результатах оцінювання.

Працівники, які не набрали необхідну кількість балів при оцінюванні рівня знань 3 рази поспіль чи проігнорували навчальний процес - не допускаються до роботи з інформаційними ресурсами Банку до моменту успішного проходження відповідного навчання.

7.3. Проведення первинного інструктажу з питань інформаційної безпеки забезпечується при прийомі нового працівника на роботу чи встановленні відповідних ділових відносин з Банком протягом 30 днів з дня прийому.

7.4. При відновленні працівника на посаді (наприклад – при поверненні з тривалої відпустки) – зазначений працівник проходить первинний інструктаж, аналогічний з прийняттям працівника на роботу.

7.5. При підписанні договорів, в результаті, яких обслуговуюча компанія (компанія, яка надає Банку певні послуги, в результаті яких її працівники отримують доступ до інформаційних ресурсів Банку чи інформації з обмеженим доступом) бере на себе відповідальність за організацію навчання свого персоналу з питань інформаційної безпеки за правилами Банку.

7.6. Для забезпечення відповідного рівня інформаційної безпеки при взаємодії з клієнтами – на сайті Банку (сторінки систем віддаленого доступу та управління рахунком) розміщено рекомендації з питань інформаційної безпеки.

8. ЗВІТУВАННЯ ТА ІНФОРМУВАННЯ

8.1. У відповідності до вимог НБУ, рекомендацій Групи та міжнародних стандартів з інформаційної безпеки, по результатам діяльності із забезпечення інформаційної безпеки Банку департаментом управління інформаційною безпекою та безперервністю бізнесу забезпечується відповідне звітування, а саме:

- раз на рік (до 01.04) до Національного банку України надається звіт у відповідності до вимог «Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг», затвердженого постановою №4 від 16.01.2024;
- раз на рік (до 15 січня) «Кваліфікований надавач електронних довірчих послуг АТ «ПРАВЕКС БАНК» надає звіт за підсумками діяльності у відповідності до вимог постанови Кабінету Міністрів України від 28 червня 2024 р. № 764 на адресу Адміністрації ДССЗЗІ України. Звіт надається у відповідності до встановленого ДССЗЗІ шаблону;
- раз на рік (до 15 січня) «Кваліфікований надавач електронних довірчих послуг АТ «ПРАВЕКС БАНК» надає звіт за підсумками діяльності у відповідності до вимог постанови НБУ від 19.09.2019 № 116 «Про затвердження Положення про кваліфікованих надавачів електронних довірчих послуг, внесених до Довірчого списку за поданням засвідчувального центру. Звіт надається у встановленому НБУ форматі;
- раз на рік (до 01.02) у відповідності до вимог Постанови НБУ від 14 квітня 2023 №49 «Положення про використання засобів криптографічного захисту інформації Національного банку України», надає до НБУ звіт щодо використання засобів криптографічного захисту інформації НБУ. Звіт надається у встановленому НБУ форматі.

У разі виникнення надзвичайних ситуацій, які призвели до зупинки сервісів захисту інформації – забезпечується негайне інформування керівництва Банку, Департаменту

безпеки Національного банку України, Державної служби спеціального зв'язку (у відповідності до існуючих регламентів роботи КНЕДП АТ «ПРАВЕКС БАНК»).

У разі виявлення інцидентів у сфері економічної безпеки, фізичної безпеки та безпеки життя – інформуються правоохоронні органи та органи місцевої влади, якщо це передбачено вимогами законодавства.

8.2. Раз на півроку, на засідання Наглядової Ради Банку подається звіт щодо результатів діяльності ДУІБтаББ з напрямів: інформаційна безпека, економічна безпека, фізична безпека, безпека життя та забезпечення безперервності діяльності Банку.

8.3. Щоквартально Комітет з управління інформаційною безпекою Банку розглядає звіт діяльності ДУІБтаББ з напрямів: інформаційна безпека, економічна безпека, фізична безпека, безпека життя та забезпечення безперервності діяльності Банку; та додатково звіт із забезпечення впровадження вимог плану інтеграції інформаційної безпеки Групи (Pravex Bank – Status Security Integration Plan).

9. 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 даної Політики в межах, встановлених законодавством України та у відповідності до договорів підписаних між Банком та постачальником/ контрагентом/ клієнтом.

10. 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

**Перелік видів інформації,
що становить комерційну таємницю**

- ***Відомості стосовно принципів управління Банком:***

- відомості про підготовку, прийняття і виконання окремих рішень керівництва Банку з питань, які стосуються інформації з обмеженим доступом;
- відомості про перспективні плани та методи управління Банком;
- відомості про предмет і цілі нарад і засідань органів управління Банку;
- документація Правління Банку, Наглядової Ради Банку, загальних зборів акціонерів, комітетів, робочих груп, проєктних команд та інших подібних утворень Банку;

- ***Відомості про фінансову, комерційну, господарську діяльність Банку:***

- відомості, що розкривають показники фінансового плану, бюджету;
- відомості про планові та звітні дані за операціями Банку;
- відомості про продукти, що розроблюються Банком;
- відомості про умови і порядок розрахунків з банками, іншими контрагентами;
- відомості про стратегію і тактику у питаннях кредитування, управління активами і пасивами, інвестування тощо;
- відомості про методи розрахунків, структуру і розмір тарифів, знижок, інших умов визначення винагороди;
- відомості про платіжні, кредитні, майнові та інші відносини з контрагентами;
- відомості про наміри Банку щодо вчинення операцій з майном;
- відомості про ведення переговорів з контрагентами (потенційними контрагентами), факт вчинення і умови правочинів з контрагентами, стан і результат виконання цих правочинів;
- відомості про порядок користування печаткою та штампами Банку;
- зразки підписів і відбитків печаток.

- ***Відомості у сфері програмного забезпечення Банку:***

- відомості про програмне забезпечення Банку;
- документація щодо програмного забезпечення, що використовується в Банку;
- відомості про структуру, потужність та інші властивості 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.

- ***Відомості про персонал Банку:***

- відомості, що містяться в особових справах працівників Банку, членів Наглядової Ради Банку, інші відомості про працівників Банку, членів Наглядової Ради Банку;
- відомості про заплановані зміни в кадровій політиці Банку;
- відомості про фонд заробітної плати;
- відомості про умови найму працівників, види і обсяги грошових виплат, додаткових благ, іншого забезпечення працівників Банку, членів Наглядової Ради Банку.

- ***Відомості про систему матеріально-технічного забезпечення Банку***

- відомості про транспортні, енергетичні та інші ресурсні 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.

- ***Інші відомості:***

- 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;
- відомості про порядок та стан організації захисту банківської, комерційної таємниці та іншої інформації, що обробляється в інформаційних системах або у документах Банку;
- інформація стосовно діяльності підрозділів, що займаються безпекою Банку.

Не є комерційною таємницею інформація, що підлягає оприлюдненню або яка відповідно до закону не може бути визнана комерційною таємницею.

Додаток 2

**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 використання 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 унеможливлюють 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 даної 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.

1.10. ПОСТАЧАЛЬНИК зобов'язаний інформувати Банк про всі інциденти інформаційної безпеки відповідно до затвердженої форми, у відповідності до Додатку 3 Політики.

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 багатофакторної 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 стосуються 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:

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

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

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

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

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

(f) 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 IT-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 багатофакторної 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 буди 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 унеможливлює 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):
  - відсутність у програмному коді зловмисного коду, чи функцій, які не санкціоновано здійснюють збір інформації;
  - 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;
  - виправлення помилок у програмному коді здійснюється за рахунок ПОСТАЧАЛЬНИКА у погоджений з Банком термін.

ПРАВЕКС БАНК
Bank of INTESA SANPAOLO

Додаток 3

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 [1]події:* _____
2. *Дата і час настання події, якщо відомо:* _____
3. *Дата та час закриття заходу, якщо є:* _____

Хто в компанії виявив подію?			
Внутрішня організація		***Зовнішня організація***	
IT безпека	☐	*Зовнішній аудитор*	☐
IMT / внутрішні функції (бізнес або підтримка) – співробітник	☐	*Сторонній постачальник*	☐
		Клієнт/ Користувач платіжного сервісу	☐
Внутрішій аудит	☐	*Нападник (попередження)*	☐
Інший			☐
Будь ласка уточніть:			

[1] *У разі порушення цілісності даних, чи порядку доступу до них, виявленого зовнішнім постачальником, датою та часом виявлення вважається момент, коли постачальний надіслав, а Банк прийняв повідомлення про виявлений інцидент.*

ТАКСОНОМІЯ ПОДІЙ

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

Атака на відмову в обслуговуванні		***Інші кіберподії***		***Додаткова класифікація*** : *класифікується як APT?*	☐
DoS	☐	*Псування*	☐	*Будь ласка, вкажіть :*	
DDos	☐	*Зловживання брендом у ЗМІ та соціальних мережах*	☐		
		Наклеп на головних осіб у ЗМІ та соцмережах	☐		
		Сканування вразливостей	☐		
		Інший	☐		

Оперативна подія							
Збій процесу	☐	***Випадкові події*** *(наприклад, помилка людини)*	☐	***Проблема ПЗ/збій системи***	☐	***Диверсія (фізична атака)***	☐
Проблема HW	☐	***Інфраструктурні проблеми*** *(внутрішні та зовнішні)*	☐	***Відсутність ключових осіб / навичок***	☐	***Проблема зовнішнього постачальника***	☐
Зовнішні події *(природні, соціально-політичні, кримінальні, проблеми транспорту, проблеми навколишнього середовища , здоров'я /санітарія, війни/конфлікти, пандемії, інші зовнішні)*					☐	***Інша оперативна подія***	☐
Будь ласка, вкажіть :							

ПЕРИМЕТР АТАКИ

Географічне розширення			
Виберіть географічне розширення подій			
Міжнародний	☐	*Регіон*	☐
Країна	☐	*Місто*	☐
Будь ласка , вкажіть:			

Контрзаходи активовано / Буде активовано			
Будь ласка, уточніть, чи були активовані контрзаходи внаслідок події			
BCP активований	☐	*DRP активований*	☐
Кіберстрахування	☐	*інший план на випадок надзвичайних ситуацій*	☐
Інші надзвичайні заходи активовані	☐	*Активовано інші контрзаходи*	☐
Інші контрзаходи, які будуть активовані	☐	*Будь ласка, вкажіть:*	

Загальний вплив			
На який вимір вплинула подія?			
Доступність[2]	☐	*Цілісність*[3]	☐
Конфіденційність[4]	☐	*Автентичність*[5]	☐
Безперервність[6]	☐	*Інше* _____[7]*:*	

Постраждав комерційний канал (Якщо застосовно)			
Комерційний канал, який постраждав від події			
Відділення	☐	*Мобільний банкінг*	☐
Електронний банкінг	☐	*банкомати*	☐
Телефонний банкінг	☐	*Точка продажу*	☐
Інший	☐	*Якщо інше, будь ласка, вкажіть :*	
Додаткова інформація :			

Тип порушення процесу/послуги			
Тип збою, викликаного подією в службі та компонентах			
Уповільнення	☐	*Несправність (часткова недоступність)*	☐
Повна недоступність	☐	*Інший*	☐
Будь ласка, вкажіть кількість внутрішніх користувачів , які експериментують з наслідками події:			
Додаткова інформація :			

Тип постраждалих клієнтів (якщо застосовно)			
Чи має подія якісь наслідки для клієнтів? Якщо так, будь ласка, вкажіть тип клієнта, який експериментував з наслідками події.			
Роздрібні клієнти	☐	*Приватні клієнти*	☐
Корпоративний	☐	*Фінансові установи*	☐
Будь ласка, вкажіть :			

Кореляція подій

[2] *Властивість процесу/послуги бути доступною та придатною для використання користувачами та клієнтами*
[3] *Властивість захисту точності та повноти активів (включаючи дані)*
[4] *Властивість, що інформація не стає доступною та не розкривається неавторизованим особам, організаціям або процесам*
[5] *Властивість, яка гарантує, що суб'єкт або ресурс ідентичні заявленим*
[6] *Властивість процесів, завдань і послуг організації бути повністю доступними та працювати на прийнятних попередньо визначених рівнях*
[7] *У випадку персональних даних, будь ласка, складіть спеціальну таблицю про порушення безпеки персональних даних*

Оцініть, чи подія пов'язана з іншими подіями (загрозою чи інцидентом)			
Окремий захід	☐	*Повторне виникнення тієї самої події*	☐
Подія , пов'язана з іншою подією	☐	*Інший*	☐
Будь ласка, вкажіть :			

Загальні коментарі щодо периметра удару (необов'язковий файл)