**Акціонерне товариство комерційний банк "ПриватБанк"**

**ЗАТВЕРДЖЕНО**
**рішення Правління банку**
**протокол № 72 від 04.10.2024**
**Голова засідання Бьош Герхард**

# Політика інформаційної безпеки

**Реєстраційний номер:** 2024/7575090
**Гриф документа:** відкритий
**Дані про затвердження:**
рішення Правління банку, протокол № 52 від 19.07.2023;
рішення Правління банку, протокол № 58 від 26.08.2022;
рішення Правління банку, протокол № 23 від 18.05.2021;
рішення Правління банку, протокол № 34 від 13.08.2019;
рішення Правління банку, протокол № 32 від 07.08.2018

Київ

**ЗМІСТ**

## 1. ВСТУП

1.1. Політика інформаційної безпеки розроблена відповідно до внутрішніх нормативних документів Банку, вимог чинного законодавства України, у тому числі нормативно-правових актів Національного банку України, зокрема:

- Постанова Правління Національного банку України від 28.09.2017 № 95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України»;
- Постанова Правління Національного банку України від 12.08.2022 № 178 «Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України»;
- Закон України “Про основні засади забезпечення кібербезпеки України”;
- Закон України “Про банки і банківську діяльність”;
- Закон України “Про захист персональних даних”;
- Закон України “Про хмарні послуги”;
- ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) ”Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги”;
- ДСТУ ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) “Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки”;
- Статут АТ КБ “ПриватБанк”,

та з урахуванням міжнародних стандартів з питань інформаційної безпеки, кібербезпеки та безпеки інформації у хмарних середовищах, загальноприйнятих у міжнародній практиці принципів забезпечення інформаційної безпеки та кіберзахисту.

1.2. Політика інформаційної безпеки є документом верхнього рівня у системі управління інформаційною безпекою. Складові процесу управління інформаційною безпекою, які не зазначені у Політиці, представлені в інших внутрішніх нормативних документах Банку (порядках, процедурах тощо).

## 2. ВИЗНАЧЕННЯ ТА СКОРОЧЕННЯ

2.1. Визначення та скорочення в цьому документі використовуються в таких значеннях:

- **Банк** — АКЦІОНЕРНЕ ТОВАРИСТВО КОМЕРЦІЙНИЙ БАНК «ПРИВАТБАНК» (АТ КБ «ПРИВАТБАНК»).
- **Конфіденційність** — властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем та/або процесом.
- **Цілісність** — властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем та/або процесом.
- **Доступність** — властивість досяжності й можливості використання інформації на вимогу авторизованого об’єкта.
- **Спостережність** — властивість системи, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об’єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання

порушення політики безпеки та/або забезпечення відповідальності за певні дії.

- **Політика** — Політика інформаційної безпеки.
- **Ризик** — імовірність виникнення збитків або додаткових втрат або недоотримання доходів, або невиконання стороною договірних зобов'язань унаслідок впливу негативних внутрішніх та зовнішніх факторів;
- **Ризик інформаційної безпеки (складова операційного ризику)** — ймовірність виникнення збитків або додаткових втрат, або недоотримання запланованих доходів внаслідок порушення конфіденційності, цілісності, доступності даних в інформаційних системах банку, недоліків або помилок в організації внутрішніх процесів або настання зовнішніх подій, включаючи кібератаки або неадекватну фізичну безпеку. Ризик інформаційної безпеки включає кіберризик;
- **СУІБ** — система управління інформаційною безпекою.
- **Інформаційна безпека** — багаторівневий комплекс організаційних заходів банку, програмних і технічних засобів, які забезпечують захист інформації від випадкових і навмисних загроз, у результаті реалізації яких можливе порушення доступності, цілісності, конфіденційності інформації, а також які забезпечують безперервність бізнес-процесів, зниження операційних ризиків і оптимізацію витрат банку.
- **Інцидент інформаційної безпеки (інцидент ІБ)** — це поява одного або декількох небажаних або несподіваних подій інформаційної безпеки, які пов'язані з настанням або значною вірогідністю настання негативних наслідків для інформаційної безпеки, інформації, інформаційних активів, бізнес-процесів або завдати шкоди Банку та системі захисту.
- **Інцидент кібербезпеки (кіберінцидент)** – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють ймовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.
- **Інформаційний ресурс** — сукупність людських, апаратних та програмних ресурсів в інформаційних системах та процесах Банку.
- **Інформація з обмеженим доступом (ІзОД)** — це відомості які становлять банківську таємницю, комерційну таємницю, таємницю страхування, персональні дані та іншу конфіденційну інформацію Банку. Інформація, яка віднесена до банківської таємниці, комерційної таємниці, таємниці страхування, персональних даних, конфіденційної інформації визначена у «Положенні про класифікатор інформації».
- **Критичний (ключовий) процес діяльності Банку** — процес, відсутність ефективного управління та контролю над яким несе загрозу діяльності Банку та/або не дозволить Банку досягти цілей.
- **Кібербезпека** — захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

- **Мінімальний рівень повноважень** — повноваження та права доступу, мінімально необхідні для якісного виконання співробітниками Банку посадових обов'язків.

Інші терміни, що вживаються в Політиці, використовуються в значеннях, визначених законами України, нормативно-правовими актами Національного банку та ДСТУ EN ISO/IEC 27000:2022.

## 3. ЦІЛЬ ДОКУМЕНТА

3.1. Ціллю Політики є впровадження та ефективне функціонування системи управління інформаційною безпекою, яка забезпечує:

- захист інформаційних ресурсів банку (у тому числі тих, що розташовані у хмарному середовищі) від реальних та потенційних зовнішніх і внутрішніх загроз, у тому числі пов'язаних з навмисними та ненавмисними діями працівників банку;
- безперервну роботу банку;
- зменшення ризиків операційної діяльності банку;
- підтримання доброчесної ділової репутації і ділової корпоративної культури банку.

## 4. СФЕРА ЗАСТОСУВАННЯ

4.1. Дія Політики розповсюджується на весь Банк.

## 5. ОРГАНІЗАЦІЙНА СТРУКТУРА ПРОЦЕСУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

5.1 Банк використовує ризик-орієнтований підхід до забезпечення інформаційної безпеки/кібербезпеки та процесний підхід до діяльності. В Банку впроваджена трирівнева модель управління ризиками з розподілом обов'язків між підрозділами відповідно до наступного:

- **перша лінія** – бізнес-підрозділи та підрозділи підтримки, які є власниками всіх операційних ризиків, що виникають у сфері їх відповідальності;
- **друга лінія** – Департамент управління операційними ризиками, що координує в цілому систему управління операційним ризиком, Напрямок Compliance, який забезпечує контроль дотриманням норм законодавства, та внутрішніх положень Банку;
- **третя лінія захисту** – внутрішній аудит, який здійснює оцінку ефективності системи управління операційним ризиком підрозділами першого та другого рівнів захисту, включаючи оцінку ефективності системи внутрішнього контролю.

Відповідно до організаційної структури Системи управління ризиками – підрозділ інформаційної безпеки відноситься до першої лінії захисту. В рамках системи управління ризиками підрозділ з інформаційної безпеки несе відповідальність за ризики інформаційної безпеки/кіберризики (далі – ризики ІБ) та звітує Керівному органу СУІБ щодо поточного стану управління такими ризиками та Системи управління інформаційною безпекою в цілому.

5.2 Банк при щорічному перегляді Політики інформаційної безпеки визначає зацікавлені сторони СУІБ, їх ролі, відповідальності та враховує їх вимоги.

5.2.1 Організаційна структура **с**истеми управління інформаційною безпекою складається з (внутрішні зацікавлені сторони):

**Наглядова рада:**

1. Затверджує внутрішнє положення яке регламентує діяльність підрозділу з інформаційної безпеки;
2. Розглядає звіти Комітету з питань технологій, даних та інновацій, щодо питань інформаційної безпеки.
3. Затверджує План забезпечення безперервності діяльності Банку, а також Політику управління безперервною діяльністю

**Комітет з питань технологій, даних та інновацій Наглядової ради:**

1. Сприяє Наглядовій раді у реалізації її повноважень щодо визначення підходів Банку з питань інформаційної безпеки і захисту даних.

2. Забезпечує підтримку технічних аспектів інформаційної безпеки (кібербезпека, шахрайство тощо), захисту даних (включаючи особисті дані).

3. Надає консультації та рекомендації Комітету Наглядової ради з питань ризиків щодо технологічних ризиків, включаючи інформаційну безпеку (кібербезпеку, шахрайство тощо), управління ризиком ІТ, захисту даних (включаючи особисті дані).

4. Оцінює на постійній основі та принаймні один раз на рік звітує Наглядовій раді про результати роботи.

**Правління:**

1. Забезпечує впровадження та функціонування СУІБ відповідно до нормативно-правових актів Національного банку України.
2. Забезпечує безпеку інформаційних систем банку і систем, що застосовуються для зберігання активів клієнтів.
3. Визначає перелік відомостей, що становлять комерційну таємницю та конфіденційну інформацію про діяльність Банку, та порядок їх використання та охорони.

**Комітет з управління операційними ризиками та інформаційною безпекою (далі - КУОР)**

У банку функціонує колективний керівний орган, який створено для забезпечення комплексності та ефективності процесів управління операційним та інформаційним ризиками, впровадження та функціонування систем внутрішнього контролю та управління інформаційною безпекою, управління ризиками, що виникають в процесі взаємовідносин з небанківськими установами.

**КУОР:**

1. Погоджує та переглядає політики інформаційної безпеки, положення щодо застосовності та стратегії розвитку інформаційної безпеки банку;
2. Узгоджує впровадження нових проектів, напрямів, стратегічних завдань з питань інформаційної безпеки банку та заходів інформаційної безпеки;

3. Розглядає, затверджує та контролює виконання проектів щодо розроблення, упровадження, функціонування, моніторингу, перегляду, підтримання та вдосконалення СУІБ банку;

4. Визначає необхідні оптимальні ресурси для впровадження заходів інформаційної безпеки;

5. Організовує практичні заходи щодо підвищення обізнаності/навчання персоналу банку з питань інформаційної безпеки;

6. Забезпечує своєчасний моніторинг стану впровадження та ефективності функціонування СУІБ банку з подальшою оцінкою можливостей удосконалення та потреби проведення коригувальних дій.

**Технологічний та Архітектурний комітет:**

1. Забезпечує реалізацію стратегії інформаційно-технологічного розвитку Банку.

2. Затвердження внутрішніх документів Банку, що стосуються технічних, техніко-технологічних та експлуатаційних аспектів інформаційних технологій, визначають їх функціонування та взаємодію.

3. Погоджує технічні завдання на закупку/розробку інформаційних сервісів та технологій.

**Відповідальний за інформаційну безпеку в Банку (Chief Information Security Officer):**

1. Забезпечує стратегічне керівництво з питань інформаційної безпеки банку.

2. Визначає напрямки розвитку інформаційної безпеки банку, їх відповідність стратегії розвитку банку.

3. Приймає рішення щодо внесення змін до стратегії розвитку ІБ в рамках її планового перегляду, або позапланового, через значні зміни, які впливають на державну діяльність або на діяльність Банку.

4. Забезпечує відповідність заходів безпеки інформації потребам бізнес-процесів/банківських продуктів.

5. Контролює впровадження заходів безпеки інформації в банку.

6. Виносить питання щодо застосування заходів впливу до порушників вимог інформаційної безпеки.

7. Забезпечує виконання заходів щодо перегляду та підтримання в актуальному стані переліку об'єктів критичної інформаційної інфраструктури, надання актуального переліку об'єктів критичної інформаційної інфраструктури до Національного банку України.

8. Забезпечує виконання заходів щодо перегляду та підтримання в актуальному стані відомостей про об'єкти критичної інформаційної інфраструктури, надання актуальних відомостей до Національного банку України.

9. Забезпечує участь Банку у інформаційному обміну з Національним банком України та іншими банками України.

10. Забезпечує пріоритетну реалізацію заходів кіберзахисту критичної інформаційної інфраструктури Банку відповідно до розробленого Плану реагування в разі кібератаки (спроби реалізації кіберзагрози) на об’єкти кіберзахисту Банку.

11. Забезпечує надання інформації про аутсорсинг функції кіберзахисту Банку на

запит Національного банку України в обсязі та в термін, що встановлені в такому запиті.

12. Забезпечує створення умов для підвищення кваліфікації працівників підрозділу з питань кіберзахисту (Напрямку інформаційної безпеки), навчання працівників Банку стосовно цифрових навичок, кіберобізнаності щодо сучасних кіберзагроз та протидії їм.

**Напрямок інформаційної безпеки:**

1. Забезпечує функціонування системи управління інформаційною безпекою у відповідності до вимог чинного законодавства, Національного банку України, міжнародних платіжних систем, інших контрагентів Банку, регуляторних органів, стандартів PCI DSS, 3D Security тощо.
2. Здійснює управління ризиками інформаційної безпеки/кіберризиками Банку.
3. Здійснює розробку, актуалізацію та тестування планів безперервності діяльності бізнес-процесів та інформаційних систем Банку.
4. Здійснює управління рольовою моделлю та доступами до інформаційних ресурсів Банку.
5. Здійснює контроль за виконанням заходів щодо забезпечення безпеки інформації на всіх стадіях життєвого циклу інформаційних систем Банку.
6. Забезпечує організаційний та технічний захист інформації.
7. Здійснює управління вразливостями та інцидентами інформаційної безпеки/кіберінцидентами.
8. Контролює витік інформації з обмеженим доступом.
9. Розробляє, або бере участь у розробленні, документів Банку щодо інформаційної безпеки та кіберзахисту.
10. Підтримує стабільну роботу програмно-технічних комплексів центру сертифікації ключів Банку.
11. Забезпечує надання до Департаменту управління операційними ризиками даних щодо внутрішніх подій (інцидентів) інформаційної безпеки/кіберінцидентів.

**Інші підрозділи, які залучаються до процесу управління інформаційною безпекою**

**Підрозділи інформаційних технологій:**

1. Співпрацюють з Напрямком інформаційної безпеки з питань оцінки ризиків ІБ при впровадженні нових проектів.
2. Забезпечують усунення вразливостей в інформаційних системах, які були виявлені Напрямком Інформаційної безпеки
3. Забезпечують дотримання вимог ІБ під час розроблення, модернізації та придбання інформаційних ресурсів.
4. Забезпечують безпечне конфігурування серверних операційних систем, баз даних та мережевого обладнання.
5. Забезпечують належне користування хмарними технологіями з метою дотримання конфіденційності, цілісності та доступності інформації, яка циркулює в хмарному середовищі.

**Дирекція з HR та корпоративного управління:**

1. Забезпечення високого рівня кадрової безпеки та благонадійності співробітників з метою загальної оптимізації діяльності.

2. Виявлення кадрових ризиків кандидатів та співробітників банку, які ґрунтуються на перевірці подій минулого або вчинків та зловживань.

**Напрямок "Служба Безпеки":**

1. Забезпечує проведення внутрішніх службових розслідувань, з метою підтвердження фактів порушення вимог інформаційної безпеки;

2. Розглядає питання впровадження заходів зі збереження інформаційних ресурсів Банку від зовнішніх та внутрішніх загроз;

3. Протидіє кіберзлочинності та телефонному шахрайству, забезпечує високий рівень захисту електронних платежів та послуг;

4. Забезпечує захист електронних платіжних інструментів у міжнародних платіжних системах;

**Управління із захисту персональних даних:**

1. Забезпечують організацію та контроль дотримання норм чинного законодавства України щодо захисту персональних даних у Банку;

2. Проводять навчання та консультування працівників Банку з питань додержання законодавства про захист персональних даних;

3. Розробляють внутрішні нормативні документи Банку (стандартів, політик, розпорядчих документів) щодо захисту персональних даних;

4. Проводять аналіз загроз безпеки персональних даних.

**Департамент управління операційним ризиком:**

1. Розробляє, впроваджує та забезпечує постійний розвиток системи управління операційним ризиком;

2. Оцінює величину операційного ризику Банку.

3. Здійснює контроль за розробленням Плану забезпечення безперервної діяльності

4. Розробляє разом з підрозділами першої лінії захисту перелік специфікацій ключових індикаторів операційного та ризику інформаційної безпеки/кіберризику.

5. Забезпечує своєчасну ідентифікацію і попередження подій операційного, та ризику інформаційної безпеки/кіберризику.

**Напрямок "Compliance":**

1. Забезпечує організацію контролю за захистом персональних даних відповідно до законодавства України;

2. Забезпечує організацію контролю за дотриманням Банком норм законодавства, внутрішньобанківських документів, в тому числі процедур, та відповідних стандартів професійних об'єднань, ринкових стандартів дія яких поширюється на Банк;

3. Забезпечує моніторинг змін у законодавстві та відповідних стандартах професійних об'єднань, дія яких поширюється на Банк, та здійснює оцінку впливу таких змін на процеси та процедури, запроваджені в Банку, а також забезпечує доведення та контроль за імплементацією відповідних змін у внутрішньобанківські документи;

**Напрямок Правової підтримки Бізнесу:**

1. Надає правову підтримку та корегує рівень заходів впливу щодо порушників вимог інформаційної безпеки.

2. Відповідно до встановленого в Банку порядку погоджує проекти внутрішніх положень Банку з інформаційної безпеки та перевіряє їх відповідність статутним документам Банку, нормам чинного законодавства.

**Напрямок судового захисту та загальної підтримки:**

1. Забезпечує правову підтримку діяльності Банку для коректного тлумачення законодавства з метою відповідності вимогам з питань інформаційної безпеки;

5.2.2 Зовнішні зацікавлені сторони:

**Верховна Рада України:**

1. Приймає нові законодавчі акти, які впливають на подальшу роботу банківської системи та необхідності внесення змін до СУІБ.

**Кабінет міністрів України (як вищий орган Банку):**

1. Визначає основні (стратегічні) напрями діяльності Банку;
2. Схвалює стратегію розвитку Банку;
3. Вносить зміни до Статуту Банку;
4. Призначає та припиняє повноваження членів Наглядової ради.

**Державні структури (Мінфін, ДССЗЗІ, СБУ та інших, державні органи):**

1. Визначають умови функціонування Банку, як об’єкта критичної інфраструктури України;
2. Сприяють покращенню захисту інформаційних ресурсів та участі у центрах з ІТ/ІБ координації.

**Національний банк України:**

1. Визначає умови роботи банківських систем;
2. Висуває вимоги щодо архітектури ІТ і ІБ;
3. Впроваджує нові або вносить зміни у поточні інформаційні системи НБУ;
4. Здійснює перевірку стану впровадження СУІБ банку та повноту виконання заходів з безпеки інформації.

**Надавачі хмарних послуг:**

1. Надають хмарні послуги відповідно до визначеного рівня інформаційної безпеки/кібербезпеки;

**Кримінальні структури, комп'ютерні злочинці, хакери, шахраї:**

1. Прагнуть розкрити/викрасти інформацію з обмеженим доступом за допомогою технічних або програмних засобів, людського фактору, та вчинення спроб негативного впливу на репутацію банку;
2. Підбурюють/залучають співробітників Банку з метою отримання власної вигоди та сприяють на вчинення протиправних дій.

**Конкуренті організації:**

1. Сприяють/стимулюють на пошук та створення нових конкурентно спроможних рішень/продуктів, покращення діючих процесів та збільшення привабливості на ринку.

**Клієнти**:

1. Досвід використання продуктів клієнтами сприяє визначенню подальшого розвитку СУІБ, впровадженню заходів з безпеки інформації.

**Держави-агресори, держави-спонсори тероризму (ворожі країни):**

1. Такі країни як РФ, Республіка Білорусь та інші країни, які підтримують їх в збройній агресії проти України впливають на розвиток СУІБ через розгортання інформаційної війни у кіберпросторі, а також військових дій, актів тероризму на території України;
2. Виступають спонсорами кримінальних структур, комп'ютерних злочинців та хакерів.

## 6. ПІДХОДИ ЩОДО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

### 6.1. Підходи до визначення цілей СУІБ

Для підтримання належного захисту інформації (насамперед інформації з обмеженим доступом) із забезпеченням її цілісності, конфіденційності, доступності та спостережності визначаються цілі інформаційної безпеки. Цілі інформаційної безпеки виражаються у вигляді характеристик і параметрів, для досягнення яких впроваджуються заходи інформаційної безпеки, та встановлюються якісні та кількісні показники в системі внутрішнього контролю процесів СУІБ.

Джерелами для формування цілей інформаційної безпеки є зовнішні та внутрішні фактори, що визначають діяльність Банку, а саме:

- закони України;
- стандарти інформаційної безпеки;
- нормативно-правові акти Національного банку України;
- правила платіжних систем та систем переказу коштів, учасником яких є Банк;
- угоди з третіми сторонами;
- результати оцінки ризиків, які враховують загальну бізнес-стратегію та цілі діяльності Банку;
- внутрішні нормативні документи Банку, що регламентують принципи обміну та обробки інформації відповідно до бізнес-потреб.

Цілі інформаційної безпеки затверджуються окремим розділом у внутрішньому нормативному документі Банку з управління СУІБ.

### 6.2. Управління ризиками інформаційної безпеки

При управлінні ризиками інформаційної безпеки банк керується основними принципами системи управління ризиком в Банку:

1. Дотримання трирівневої моделі управління ризиками.

2. Створення та впровадження процедури управління ризиком інформаційної безпеки з метою ефективного управління ризиком інформаційної безпеки/кіберризиком.

3. Забезпечення своєчасного виявлення загроз інформаційної безпеки та усунення ризиків інформаційної безпеки.

4. Виявлення і врахування факторів ризику, які загрожують доступності, цілісності, конфіденційності інформації в банку.

5. Забезпечення обізнаності працівників Банку щодо ризиків інформаційної безпеки.

### 6.3. Управління інцидентами інформаційної безпеки

1. Виявлення і фіксація подій ІБ найбільш ефективним шляхом, підтвердження їх класифікації як інцидентів ІБ/кіберінцидентів;

2. Послідовна оцінка і безперервне реагування на виявлені інциденти ІБ/кіберінциденти найбільш сприятливим та ефективним чином;

3. Застосування ефективної системи управління інцидентами, для зведення до мінімуму несприятливих наслідків для Банку;

4. Використання своєчасного інформування відповідальних осіб за інформаційну безпеку про інциденти ІБ/кіберінциденти, за допомогою процесу ескалації;

5. Впровадження моніторингу, оцінки та усунення вразливостей ІБ, для скорочення кількості інцидентів;

6. Швидке вилучення досвіду за результатами управління інцидентами ІБ.

### 6.4. Підходи до управління та моніторингу ІБ

Для управління інформаційною безпекою в Банку використовується ефективне поєднання технічних та організаційних рішень, що дозволяє досягти високої якості моніторингу стану СУІБ.

1. Технічні рішення є сукупністю засобів для збору відомостей про стан елементів інформаційних систем, а також засобів впливу на їх поведінку. Зокрема засоби моніторингу шкідливого ПЗ, а також системи управління подіями і інцидентами інформаційної безпеки (SIEM).

2. Організаційні рішення використовуються у вигляді налагодження процесів взаємодії людей (співробітників), спрямованих на забезпечення необхідного рівня моніторингу ІТ-систем і підсистем ІБ. Це дозволяє формувати групи реагування на інциденти, що складаються з експертів різного рівня, та обумовлює створення операційного центру безпеки (Security Operation Centre).

## 7. ПРИНЦИПИ ТА ВИМОГИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

7.1. Основним принципом інформаційної безпеки є підтримання належного захисту інформації (насамперед інформації з обмеженим доступом) із забезпеченням її цілісності, конфіденційності, доступності та спостережності.

7.2. Принципами забезпечення інформаційної безпеки є:

- системний (комплексний) підхід до забезпечення інформаційної безпеки банку;
- безперервність процесу удосконалення та розвитку інформаційної безпеки та його здійснення шляхом обґрунтування та реалізації раціональних засобів, методів, заходів із

застосуванням найкращого міжнародного досвіду;

- своєчасність та адекватність заходів захисту від реальних та потенційних загроз інформаційній безпеці банку;
- контроль та забезпечення підтримки належного рівня інформаційної безпеки з боку керівників банку;
- забезпечення достатності ресурсів, у тому числі фінансових, для сталого розвитку систем інформаційної безпеки.

7.3. Підрозділ з інформаційної безпеки банку безпосередньо підпорядковується відповідальній особі за інформаційну безпеку банку (CISO).

7.4. Керівництво банку всіляко підтримує впровадження інформаційної безпеки та забезпечує її фінансування на достатньому рівні.

7.5. Документи з питань інформаційної безпеки/кіберзахисту розробляються підрозділом з інформаційної безпеки та іншими підрозділами за відповідними напрямками діяльності. Постійний контроль впровадження, виконання, вдосконалення та підтримки Політики в актуальному стані покладений на підрозділ з інформаційної безпеки.

7.6. Банк розробляє внутрішні документи, які визначають, зокрема:

- вимоги щодо використання, надання, скасування та контролю доступу до інформаційних систем банку;
- вимоги щодо безпеки інформації під час використання змінних носіїв інформації;
- вимоги до забезпечення захисту від зловмисного коду та організації захисту від зловмисного коду;
- використання криптографічних засобів для захисту інформації;
- процес управління ключами;
- процес управління оновленнями;
- вимоги щодо безпеки інформації, технічного обслуговування, експлуатації факсимільних апаратів, багатофункціональних пристроїв, телефонів та/або телефонних систем;
- вимоги щодо використання електронної корпоративної пошти;
- вимоги щодо підбору, застосування або модернізації програмних та апаратних засобів обробки інформації або в разі придбання, а також порядок виведення з експлуатації обладнання інформаційних систем банку;
- вимоги щодо процесу управління інцидентами інформаційної безпеки.

7.7. У банку діє принцип надання мінімального рівня повноважень під час надання доступу до інформаційних систем банку (включаючи доступ привілейованих користувачів).

7.8. В інформаційних системах банку, які безпосередньо забезпечують автоматизацію банківської діяльності, забороняється суміщення в межах однієї функції (ролі) таких повноважень: розроблення та супроводження (адміністрування), розроблення та експлуатація, супроводження (адміністрування) та експлуатація, виконання операцій в таких системах та подальшого контролю за їх виконанням.

7.9. Банк використовує стандарти, документи та настанови відкритого проекту захисту додатків "Open web application security project" (OWASP) для розроблення безпечних додатків.

7.10 Банк при впровадженні та розробці програмного забезпечення керується

принципами та підходами безпеки з дотриманням методик S-SDLC.

7.11. Під час розроблення, впровадження та функціонування програмно-технічних комплексів обов'язково враховуються вимоги інформаційної безпеки.

7.12. Публічні сервіси банку та внутрішні мережі банку мають відповідати вимогам стандартів з інформаційної безпеки.

7.13. Банк забезпечує виконання вимог з інформаційної безпеки, які наявні в угодах з третіми сторонами стосовно участі у міжнародних платіжних системах та системах переказу коштів.

7.14. Банк підтримує високий рівень безпеки інформації, яка обробляється, зберігається та передається за допомогою хмарних технологій зберігання даних.

7.15. У банку розроблено та затверджено план забезпечення безперервності діяльності банку, у якому враховано безперервність функціонування заходів інформаційної безпеки в рамках процесу управління безперервністю діяльності банку.

7.16. Стратегія розвитку інформаційних технологій, проекти, які пов'язані з інформаційними технологіями, узгоджуються з Політикою.

7.17. Відповідальність структурних підрозділів банку в частині інформаційної безпеки визначається внутрішніми документами банку.

7.18. Кожен працівник банку під час виконання своїх посадових обов'язків і повноважень повинен забезпечувати виконання вимог інформаційної безпеки банку. Працівники банку несуть відповідальність за невиконання вимог інформаційної безпеки, встановлених внутрішніми документами банку та нормами чинного законодавства.

7.19. Банк підтримує програму підвищення обізнаності/навчання працівників банку з питань безпеки інформації/кіберзахисту з урахуванням досвіду, отриманого за результатами вирішення інцидентів безпеки інформації.

7.20. Зміст Політики доводиться до відома всього персоналу банку та, за необхідності, представникам третіх сторін. Банк зобов'язаний ознайомити з Політикою працівників під час прийняття на роботу. Кожен працівник банку зобов'язаний ознайомитися з Політикою під підпис та надати зобов'язання про дотримання конфіденційності.

7.21. Банк впроваджує заходи щодо дотримання законодавства про захист персональних даних, а також договірних умов, узгоджених з партнерами, підрядниками та відповідними третіми сторонами. Банк визнає свою відповідальність за захист приватності та конфіденційності персональних даних, а також за забезпечення безпечної обробки та зберігання таких даних.

## 8. ЗВІТНІСТЬ

8.1. Напрямок Інформаційної безпеки надає на розгляд керівному органу СУІБ звіт з оцінки впливу інформаційних систем на діяльність Банку, один раз на рік.

8.2. Звіти, щодо моніторингу ефективності впровадження СУІБ, надаються на розгляд керівному органу СУІБ раз на квартал.

8.3. Звіти, щодо стану впровадження системи управління інформаційною безпекою, моніторингу досягнення цілей з інформаційної безпеки, аналіз змін факторів зовнішнього та внутрішнього середовища, які важливі для функціонування СУІБ, розгляду можливостей щодо постійного вдосконалення та потреби внесення змін до системи управління інформаційною безпекою, звіти зі стану процесів забезпечення безперервності діяльності

банк та управління ризиками інформаційної безпеки надаються Комітету з управління операційними ризиками та інформаційною безпекою один раз на півріччя.

8.4. Напрямком інформаційної безпеки надається підсумковий місячний звіт відповідальному за інформаційну безпеку в Банку (CISO), щодо виконаних заходів з забезпечення інформаційної безпеки у Банку.

## 9. ПЕРЕГЛЯД ДОКУМЕНТА

9.1. Політика затверджується Правлінням банку.

9.2 Політика підтримується в актуальному стані та переглядається не рідше ніж один раз на рік. Якщо за результатами перегляду зміни до Політики не вносяться, то повторне її затвердження не потрібно.

9.3. Підставами внесення змін до Політики є зміни в інформаційній інфраструктурі та/або впровадженні нових інформаційних технологій, зміни в законодавстві, стандартах з інформаційної безпеки та інших нормах, або за появи істотних змін.

9.4. Зміни та доповнення до Політики погоджуються з керівним органом СУІБ та затверджуються Правлінням банку.