

ЗАТВЕРДЖЕНО

Протокол Комітету
з операційних, комплаєнс
ризиків та інформаційної
безпеки
АТ «БАНК КРЕДИТ ДНІПРО»
від 26.03.2025 №21.1

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АТ "БАНК КРЕДИТ ДНІПРО"

ВЕРСІЯ 4.0

ЗМІСТ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ	3
2. НОРМАТИВНА БАЗА	3
3. ОСНОВНІ ТЕРМІНИ, ВИЗНАЧЕННЯ ТА СКОРОЧЕННЯ	4
4. ЦІЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	5
5. СФЕРА ЗАСТОСУВАННЯ.....	6
6. ДОКУМЕНТИ ПОЛІТИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	6
7. ЗАГАЛЬНІ ЗАСАДИ ВПРОВАДЖЕННЯ ПОЛІТИКИ.....	7
8. ПРИНЦИПИ ПОБУДОВИ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	7
9. КОНТРОЛЬ ТА ВІДПОВІДАЛЬНІСТЬ	12
10. ПРИКІНЦЕВІ ПОЛОЖЕННЯ.....	14

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Політика інформаційної безпеки АТ «БАНК КРЕДИТ ДНІПРО» (далі - Політика) визначає основні принципи та розкриває основні напрямки забезпечення інформаційної безпеки, а також містить систематизоване викладення цілей, задач, базових правил захисту інформації та способів досягнення належного рівня інформаційної безпеки АТ «БАНК КРЕДИТ ДНІПРО» (далі — Банк). Спрямована на збереження конфіденційності, цілісності, доступності та спостережливості інформаційних активів.

1.2. Політика регламентує впровадження та ефективне управління системою інформаційної безпеки, спрямованої на захист інформаційних активів Банку, забезпечення безперервності діяльності Банку, мінімізації ризиків інформаційної безпеки, створення позитивної репутації Банку та довірчих відносин з клієнтами.

1.3. Забезпечення інформаційної безпеки Банку досягається реалізацією комплексу необхідних заходів, що підтримуються кожним працівником та постачальником Банку на своєму робочому місці - при виконанні своїх функціональних обов'язків в необхідних і визначених для нього межах відповідно до ВНД Банку щодо забезпечення інформаційної безпеки та кіберзахисту інформаційних ресурсів Банку.

2. НОРМАТИВНА БАЗА

2.1. При розробці Політики була використана така нормативна база зовнішнього та внутрішнього походження:

№	Найменування документа:
1.	ДСТУ ISO/IEC 27000:2019 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000:2018, IDT)
2.	ДСТУ ISO/IEC 27001:2023 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги
3.	ДСТУ ISO/IEC 27002:2023 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки
4.	Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затверджене Постановою Правління Національного банку України (далі – НБУ) від 28.09.2017р. №95
5.	Положення про порядок формування, зберігання та знищення відокремлених електронних даних, отриманих за результатами роботи інформаційних систем у Національному банку України і банках України, затверджене Постановою НБУ від 14.09.2018 № 99
6.	Положення про організацію бухгалтерського обліку в банках України, затверджене Постановою НБУ від 04.07.2018 № 75
7.	Положення про організацію кіберзахисту в банківській системі України, затверджене Постановою НБУ від 12.08.2022 № 178
8.	Положення про автентифікацію та застосування посиленої автентифікації на платіжному ринку, затверджене Постановою НБУ від 03.05.2023 № 58
9.	Положення про використання електронного підпису та електронної печатки, затверджене Постановою НБУ, від 20.12.2023 №172
10.	Правила з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи, затверджені Постановою НБУ від 17.08.2007 №243
11.	Положення про організацію системи управління ризиками в банках України та банківських групах, затверджене Постановою НБУ від 11.06.2018 № 64
12.	Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг, затверджене Постановою НБУ від 16.01.2021 № 4

13.	Постанова № 42 від 08.03.2022 «Про використання банками хмарних послуг в умовах воєнного стану в Україні»
-----	---

3. ОСНОВНІ ТЕРМІНИ, ВИЗНАЧЕННЯ ТА СКОРОЧЕННЯ

3.1. У межах застосування цієї Політики нижченаведені терміни вживаються у такому значенні:

- **Банківська група** – банківська група Кредит Дніпро, до складу якої входить група юридичних осіб, які мають спільного контролера, що складається з Банку та компаній, які є фінансовими установами або для яких надання фінансових послуг є переважним видом діяльності (посилання на склад Банківської групи «КРЕДИТ ДНІПРО» <https://bank.gov.ua/ua/supervision/registration/bankgroups/305749>).
- **Банк** – АТ «БАНК КРЕДИТ ДНІПРО».
- **Доступність** - властивість ресурсу системи, яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний.
- **Зниження ризиків** — процес впровадження контролів для зменшення виявлених ризиків до прийняттого рівня.
- **Інформаційна безпека (ІБ)** – сукупність організаційно-технічних заходів і засобів, спрямованих на захист інформаційного середовища Банку, його формування, використання і розвиток в інтересах Банку, конфіденційності, цілісності і доступності інформації, інформаційних активів і систем, з метою забезпечення стану стійкої життєдіяльності та динамічного розвитку Банку.
- **Інформаційна система/інформаційний актив(ІС/ІА)** – апаратно-програмний комплекс, який виконує збір, обробку, зберігання та передачу даних з метою забезпечення потреб Банку.
- **Інцидент інформаційної безпеки** — одна або кілька небажаних або несподіваних подій інформаційної безпеки, що мають істотну ймовірність порушення бізнес-операцій і загрожують інформаційній безпеці Банку.
- **Інцидент високого рівня** — це подія, пов'язана із загрозами інформаційній безпеці, яка має значний вплив на діяльність Банку, викликає серйозні ризики для захисту інформаційних активів та потребує негайного реагування.
- **ІТ** — інформаційні технології.
- **Контроль** — сукупність організаційних та/або технічних дій, спрямованих на управління ризиком.
- **Конфіденційність** — властивість інформації (або інформаційного активу), що полягає у тому, що доступ до інформації не може бути отриманий неавторизованою особою, об'єктом і/або процесом.
- **Користувач** – фізична або юридична особа, яка в установленому чинним законодавством або внутрішніми документами Банку порядку одержала право доступу до інформації в системі.
- **КОКРтаІБ** – колегіальний орган Банку, створений відповідно до чинного законодавства України та внутрішніх нормативних документів Банку, що має забезпечувати визначення та пріоритетність завдань інформаційної безпеки у Банку, їх відповідність вимогам законодавства України, нормативно-правових актів Національного банку України та внутрішніх документів Банку, інтегрованість у відповідні процеси/банківські продукти, перегляд ефективності впровадження та функціонування системи управління інформаційною безпекою, визначати ресурси,

що потрібні для інформаційної безпеки та навчання персоналу з питань інформаційної безпеки.

- **КЦДС** - Конфіденційність, Цілісність, Доступність та Спостережливість.
Постачальник – юридична особа, фізична особа-підприємець, фізична особа та/або співробітник юридичної особи, фізичної особи-підприємця, які підписали зобов'язання (договір) щодо нерозголошення конфіденційної інформації та/або договір надання послуг з Банком, який містить зобов'язання щодо нерозголошення конфіденційної інформації, та які отримують доступ до інформаційної системи Банку.
- **Ризик інформаційної безпеки** (складова операційного ризику) - імовірність виникнення збитків або додаткових втрат, або недоотримання запланованих доходів унаслідок порушення конфіденційності, цілісності, доступності даних в інформаційних системах банку, недоліків або помилок в організації внутрішніх процесів або настання зовнішніх подій, уключаючи кібератаки або неадекватну фізичну безпеку.
- **Система управління інформаційною безпекою (СУІБ)** — частина загальної системи управління, що ґрунтується на врахуванні ризиків інформаційної безпеки та призначена для безперервного процесу розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.
- **Спостережливість** - 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 і/або забезпечення відповідальності за певні дії.
- **Цілісність** - властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом. Цілісність системи - властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки.

3.2. Терміни, визначення та скорочення, не визначені у цьому розділі, вживаються у значеннях, наведених далі за текстом Політики, а у разі відсутності такого визначення – відповідно до законодавства та/або інших ВНД Банку. Якщо визначення у ВНД відрізняються від наведених у цій Політиці, для цілей тлумачення Політики превалюють значення, наведені у тексті Політики.

4. ЦІЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

4.1. Загальною метою Політики є визначення підходів та принципів забезпечення інформаційної безпеки Банку та інформаційних активів, впровадження і ефективне управління СУІБ, спрямованої на захист інформаційних активів Банку, забезпечення безперервності діяльності Банку, мінімізацію ризиків інформаційної безпеки, створення позитивної репутації Банку і довірчих стосунків з клієнтами.

4.2. Ціллю Політики інформаційної безпеки є впровадження та ефективне функціонування системи управління інформаційною безпекою, яка буде забезпечувати безпечність та надійність функціонування банківських 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.

4.3. Практична мета Політики полягає в тому, щоб оцінити усі можливі ризики, розробити, впровадити та підтримувати відповідний рівень захисту для кожного з

активів Банку від зовнішніх і внутрішніх, умисних і ненавмисних загроз для забезпечення стану стійкої життєдіяльності Банку.

4.4. Інформування працівників, клієнтів Банку та інших зацікавлених сторін щодо організації інформаційної безпеки у Банку.

5. СФЕРА ЗАСТОСУВАННЯ

5.1. Політика є внутрішнім нормативним документом Банку, поширюється на всі аспекти діяльності Банку та інформаційні активи, які можуть ефективно вплинути на кінцевий продукт своєю відсутністю або псуванням (тобто впливають на КЦДС) і є обов'язковою для застосування всіма працівниками Банку, а також третіми сторонами при обміні інформацією та використанні інформаційних ресурсів Банку в межах договірних відносин.

5.2. Більш детально область дії СУІБ описана в Положенні щодо області дії системи управління інформаційною безпекою АТ «БАНК КРЕДИТ ДНІПРО» (далі – Положення), яке регламентує межі напрямів та процесів діяльності, на які поширюється СУІБ. Це Положення визначає, що СУІБ використовується як засіб виконання функцій та надання послуг, які здійснюються АТ «БАНК КРЕДИТ ДНІПРО», відповідно до вимог стандарту ДСТУ ISO/IEC 27002:2023.

6. ДОКУМЕНТИ ПОЛІТИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

6.1. Банк розробляє та впроваджує внутрішні документи, що регламентують вимоги та процеси у сфері інформаційної безпеки, зокрема:

- порядок надання, зміни, скасування та контролю доступу до інформаційних систем банку, включаючи привілейовані облікові записи;
- вимоги до безпеки інформації під час використання змінних носіїв даних;
- заходи із захисту від зловмисного програмного забезпечення та порядок реагування на кіберзагрози;
- використання криптографічних засобів для забезпечення конфіденційності та цілісності інформації;
- процеси управління ключами криптографічного захисту;
- порядок управління оновленнями та внесення змін до інформаційних систем;
- вимоги до використання корпоративної електронної пошти та контролю її безпеки;
- правила вибору, впровадження та виведення з експлуатації апаратних і програмних засобів, що використовуються для обробки інформації;
- процеси управління інцидентами інформаційної безпеки, порядок їх реєстрації, аналізу та усунення наслідків.
- застосовує стандарти, рекомендації та методології відкритого проекту захисту додатків Open Web Application Security Project (OWASP) для забезпечення безпечної розробки програмного забезпечення;
- керується принципами безпечної розробки Secure Software Development Lifecycle (SSDLC) під час впровадження та розробки програмного забезпечення;
- забезпечує дотримання вимог інформаційної безпеки на всіх етапах життєвого циклу програмно-технічних комплексів – від розробки до експлуатації;

6.2. Внутрішні нормативні документи Банку, що детальніше описують вимоги Політики інформаційної безпеки, зокрема наведені в переліку пов'язаних ВНД, доступні всім працівникам Банку в межах їх повноважень. Вони спрямовані на підтримку реалізації Політики інформаційної безпеки та є обов'язковими для виконання.

6.3. Політика інформаційної безпеки має трирівневу структуру:

Рівень 1 – документи, що описують Стратегію інформаційної безпеки Банку, загальну Політику інформаційної безпеки Банку з основними поняттями і концепціями, які розміщуються на внутрішніх інформаційних ресурсах Банку і доступні всім без виключень;

Рівень 2 – документи, базуються на документах 1-го рівня, описують тактичні заходи, щодо реалізації Стратегії Інформаційної безпеки та регламентують організаційні питання і що містять рекомендації з питань інформаційної безпеки або роботи з активами;

Рівень 3 – документи, що містять практичне керівництво, довідники і шаблони, інструкції, принципи і моделі для реалізації і контролю практичного виконання документів 2-го рівня та досягнення мети документів 1-го рівня.

7. ЗАГАЛЬНІ ЗАСАДИ ВПРОВАДЖЕННЯ ПОЛІТИКИ

7.1. Загальні засади впровадження інформаційної безпеки базуються на:

7.1.1. Законності побудови інформаційної безпеки та врахування соціальних факторів.

7.1.2. Узгодженість головної мети та цілей інформаційної безпеки із стратегічними цілями та поточними завданнями діяльності Банку.

7.1.3. Єдність управління інформаційною безпекою та загального управління в Банку. Система управління інформаційною безпекою є інтегрованою частиною загального менеджменту Банку.

7.1.4. Відповідальність Банку за інформаційну безпеку перед зовнішніми сторонами. Якщо у Банку циркулює інформація, яка належить стороннім особам, організаціям або державі, то Банк забезпечує адекватний захист цієї інформації і несе відповідальність за порушення конфіденційності, цілісності та доступності даної інформації під час її обробки.

7.1.5. Персональна відповідальність вищого керівництва Банку, посадових осіб усіх рівнів управління та всього персоналу Банку за стан інформаційної безпеки. У Банку на всіх рівнях чітко визначаються права, обов'язки та відповідальність посадових осіб, що беруть участь у процесі обробки інформації стосовно вирішення задач інформаційної безпеки. З одного боку, це означає визначення правових та адміністративних норм, які регулюють взаємовідносини та обов'язки різних учасників щодо забезпечення інформаційної безпеки. З іншого – передбачає реалізацію спеціальних заходів нагляду, що дозволяють визначити порушення вимог з інформаційної безпеки та ідентифікувати особу, що причетна до дій, які призвели до порушення інформаційної безпеки.

7.1.6. Комплексність та системність забезпечення інформаційної безпеки. Створення надійної СУІБ та реалізація контролів здійснюється на правовому, адміністративному, процедурному та програмно-технічному рівнях, а також на основі комплексного застосування методів та засобів захисту інформації.

7.1.7. Адекватність забезпечення інформаційної безпеки. Рівень інформаційної безпеки має відповідати та бути адекватним цінності ресурсів, що захищаються, та рівню можливого збитку, який може бути нанесений у випадку порушення цілісності, конфіденційності та доступності інформації та інформаційних активів Банку.

7.1.8. Безперервність забезпечення інформаційної безпеки. Реалізація контролів здійснюється на постійній основі із проведенням періодичної оцінки рівня захищеності інформації та інформаційних активів Банку, адаптації СУІБ до умов експлуатації.

8. ПРИНЦИПИ ПОБУДОВИ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

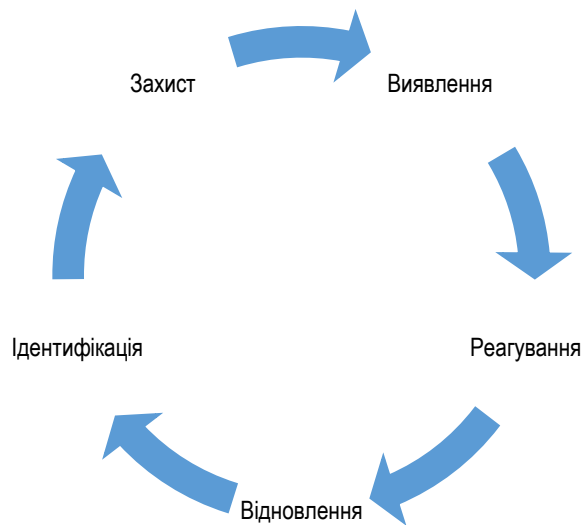
В Банку в питаннях інформаційної безпеки за замовчуванням діє правило – заборонено все, що явно не дозволено.

8.1. Для досягнення мети Політики Банк дотримується 10 основних принципів:

Принцип 1: Створення гнучкого управління інформаційною безпекою на основі ризик орієнтованого підходу

Визначення та реалізація системи управління інформаційною безпекою ґрунтується на дотриманні 6 підходів для забезпечення відповідності вимог законодавства України, нормативних актів НБУ з інформаційної безпеки та узгодження зі стратегічними цілями Банку:

- **Баланс** - система розподіляє навантаження на весь ланцюжок цінностей безпеки, як показано схематично нижче:



- **Узгодженість** - процес інтеграції взаємодії з підрозділами, відповідальними за захист даних, боротьба з шахрайством, безперервність бізнесу, безпека людей та інформаційних активів Банку тощо.
- **Обміркований та впорядкований підхід** - система сприяє досягненню цілей Банку завдяки дотриманню найкращих практик та зусиль для підтримки постійного балансу між прийнятими рівнями ризику та зробленими інвестиціями.
- **Витрати та прийняті ризики** - рішення, що стосуються прийнятих рівнів ризику, є частиною стандартизованого та задокументованого процесу прийняття ризику. У разі затверджених винятків Банк бере на себе пов'язані ризики та витрати в межах зобов'язань, визначених у Політиці управління ризиками інформаційної безпеки.
- **Безперервне покращення** – процеси та правила контролю та моніторингу надають показники для вимірювання рівня захищеності Банку та прогресу, досягнутого з часом.
- **Спостережливість** - підрозділ Банку, який відповідає за інформаційну безпеку відповідає за відстеження виконання цілей системи управління. У разі відхилення від цілей Стратегії розвитку інформаційної безпеки забезпечує контроль їх виконання.

Принцип 2: Підхід орієнтований на властивості інформаційних активів

Прийнятий в Банку підхід, орієнтований на забезпечення чотирьох основних властивостей безпеки, відносно яких кожен відповідальний працівник Банку повинен оцінювати кожен актив та проект на стадії усього його життєвого циклу Конфіденційність, Цілісність, Доступність та Спостережливість.

У зв'язку з тим, що вимоги безпеки і наслідки їх недотримання з часом можуть змінюватись, їх необхідно регулярно переглядати.

Кожен працівник Банку може направити запит на надання підтримки з боку фахівців підрозділів Управління ризик-менеджмент, Управління безпеки, Департамент з інформаційної безпеки, Управління компанс тощо.

Аналіз критичності активу/проекту, повинен проводити кожен керівник бізнес напряму/напряму підтримки, проекту у відповідності до вимог документу, що визначає порядок оцінювання критичності інформаційних активів.

Аналіз критичності безпеки проводиться за:

- Ступенем впливу на критерії безпеки КЦДС (вплив на діяльність Банку (зокрема, Бізнес та Інфраструктуру і існуючі системи));
- Характером впливу – фінансовий та нефінансовий.

Проекти з критичним рівнем по одному з цих напрямів, вважаються "критичними проектами" і підлягають систематичному моніторингу і повторному узгодженню з Департаментом з інформаційної безпеки Банку на усіх етапах проекту і життєдіяльності активу.

Принцип 3: Культура інформаційної безпеки побудована та адаптована до викликів інформаційної безпеки

Кожен працівник та постачальник Банку зобов'язаний брати участь в підтримці належного рівня інформаційної безпеки Банку, виконувати вимоги інформаційної безпеки.

Керівники усіх підрозділів Банку повинні постійно доводити до відома своїх підлеглих та постачальників інформацію про необхідність бездоганного дотримання норм Політики інформаційної безпеки.

Керівники усіх підрозділів Банку несуть відповідальність за те, що кожен працівник:

- достатньо поінформований про вимоги законодавства України, стандартів, внутрішніх правил та інструкцій в частині інформаційної безпеки;
- має необхідні навички здійснення захисних заходів та вміння реагувати та повідомляти про будь-які виявлені проблеми з інформаційної безпеки в рамках своїх компетенцій.

Усі підрозділи Банку мають бути забезпечені необхідною нормативною базою з питань інформаційної безпеки і/або мати доступ до таких ресурсів в електронному вигляді.

Всі працівники Банку під час прийому на роботу ознайомлюються з Політикою, а також не рідше одного разу на рік, проходять навчання з інформаційної безпеки.

Програма навчання/інформування повинна включати, як мінімум:

- інформацію про ризики використання ресурсів мережі Інтернет, пошти, зовнішніх носіїв інформації, критичних з точки зору безпеки засобів обчислювальної техніки та програмного забезпечення;
- керівництво щодо використання інформаційних активів, систем та сервісів;
- посилання на Політику інформаційної безпеки;
- інтеграція питань інформаційної безпеки у повсякденну діяльність працівників.

Питання інформаційної безпеки повинні бути інтегровані у внутрішні тренінги, призначені для персоналу Банку та бізнес напрямів/ліній підтримки та ІТ, а також для працівників/представників третіх сторін, що мають доступ до інформаційних активів Банку.

Принцип 4: Контроль «ризиків інформаційної безпеки», пов'язаних з аутсорсинговими послугами

Залучення аутсорсингових послуг до діяльності Банку призводять до підвищення загроз інформаційної безпеки пов'язаних з Доступністю, Цілісністю, Конфіденційністю, Спостережливістю. Загальне усвідомлення зовнішнього ризику, пов'язаного з аутсорсинговими послугами, полягає в тому, що Банк надає доступ зовнішнім контрагентам до інформаційних активів Банку.

Контроль ризиків інформаційної безпеки, пов'язаних з аутсорсинговими послугами охоплює різні етапи від укладання договору, початкового дослідження необхідності залучення аутсорсингу до завершального етапу – розірвання договору.

Принцип 5: Надання та контроль доступу до інформаційних активів Банку

Надання та контроль доступу до інформаційних активів базується на чотирьох засадах:

- Чутливі активи/дані повинні бути захищені пропорційно ризикам, які виникають при наданні доступу до них;
- За замовчуванням для всіх користувачів застосовується правило: "Заборонено все, що явно не дозволено";
- Користувачам можуть надаватись права в мінімально необхідному обсязі, достатньому для виконання їх обов'язків згідно матриці доступів;
- Для реалізації контролю доступу мають бути розроблені та впроваджені механізми фіксації дій користувача з інформаційними активами (спостережливість) згідно наданих прав доступу.

Контроль доступу, в першу чергу залежить від можливості надання індивідуального доступу на основі засобів ідентифікації, автентифікації та авторизації адаптованих до чутливості активів, що захищаються.

Принцип 6: Забезпечення технічними засобами захисту інформації

Для забезпечення належного рівня інформаційної безпеки необхідно, окрім організаційних процесів, використовувати технічні засоби, рекомендовані НБУ та міжнародними стандартами з інформаційної безпеки.

Безпека технічної бази забезпечується розгортанням та обслуговуванням апаратних засобів безпеки, конфігурація та адміністрування яких підлягають регулярному контролю зі сторони підрозділу Банку, який відповідає за інформаційну безпеку.

Вибір та використання технічних засобів захисту інформації має виконуватись згідно з законодавством України, в тому числі НБУ, та вимогами платіжних систем, що використовує Банк.

Принцип 7: Інтеграція інформаційної безпеки в проекти та управління інформаційними активами

Кожен проект протягом усього життєвого циклу повинен відповідати вимогам політик з інформаційної безпеки. Процес затвердження та контроль дотримання вимог інформаційної безпеки має бути інтегрований в управління проектами.

Впровадження засобів (механізмів забезпечення) в проекти безпеки інформації має включати як мінімум:

- регулярний аналіз критичності безпеки згідно **Принципу 2** та перегляд вимог інформаційної безпеки керівником бізнес-напрямку за сприяння Департаменту з інформаційної безпеки;
- регулярний аналіз можливих ризиків;
- механізми забезпечення його безпеки керівником проекту за сприяння підрозділу Банку, який відповідає за інформаційну безпеку Банку та підрозділів ІТ;
- аналіз відповідності проекту нормам Політики інформаційної безпеки та вимогам інформаційної безпеки;
- узгодження проекту або змін до нього з підрозділом Банку, який відповідає за інформаційну безпеку Банку.
- У кожного інформаційного активу повинен бути Власник ІС та Бізнес-відповідальний, що визначаються у відповідності до Порядку визначення Власників інформаційних активів – при цьому:
- підрозділу ІТ Банку забороняється бути власником інформаційних активів Банку, які безпосередньо забезпечують автоматизацію банківської діяльності;

- підрозділу Банку, який відповідає за інформаційну безпеку Банку, забороняється мати повноваження з розроблення, впровадження, супроводження (адміністрування) та експлуатації інформаційних активів Банку, крім тих, що використовуються для забезпечення безпеки інформації.

Принцип 8: Зміцнення культури відповідності

Всі вимоги законодавства України, зокрема НБУ, Політики інформаційної безпеки, а також правила платіжних систем, що використовує Банк, є обов'язковими до виконання в усіх процесах Банку.

Для зміцнення культури відповідності відповідальні підрозділи Банку розробляють та виконують періодичні контролю, які охоплюють:

- дотримання вимог законодавства України та нормативних актів НБУ;
- виконання внутрішніх політик та процедур з інформаційної безпеки;
- відповідність вимогам міжнародних стандартів безпеки та правил платіжних систем;
- оцінку рівня зрілості організації щодо галузевих стандартів та нормативних вимог;
- контроль надійності систем захисту інформації.

Будь-які виявлені невідповідності, а також плани вдосконалення підлягають моніторингу в рамках процесу управління, визначеного в Принципі 1.

Принцип 9: Забезпечення нагляду за «інформаційним середовищем» Банку

Моніторинг та спостереження повинні бути впровадженні відповідно до чинного законодавства щоб:

- контролювати та інтегрувати зміни в бізнесі та технологіях;
- забезпечити виявлення, як можна швидше, нових загроз, нападів чи "незвичайних подій" та, якщо необхідно, підвищення рівня захисту інформаційних активів.

Принцип 10: Реагування на інциденти інформаційної безпеки

Інцидентом інформаційної безпеки вважається порушення хоч би однієї з основних вимог Політики інформаційної безпеки - Доступність, Цілісність, Конфіденційність, Спостережливність.

Процес реагування на інциденти інформаційної безпеки, їх виявлення та документування, оповіщення відповідальних осіб проводиться відповідно до затвердженої в Банку Політики управління інцидентами інформаційної безпеки АТ "БАНК КРЕДИТ ДНІПРО" та окремими планами реагування, в залежності від типу інциденту.

Політика інформаційної безпеки передбачає відповідну реакцію на той або інший тип інциденту. Інцидент має бути локалізований для запобігання його можливому поширенню, також повинні бути визначені пов'язані активи, максимально розмежовані зони функціонування пов'язаних критичних активів, зокрема щоб обмежити вплив інциденту на інші активи.

При виникненні інциденту «Високого рівня» необхідно здійснити усі заходи для його ліквідації. Має бути зроблене вивчення ІТ систем і сервісів, активів і систем/механізмів забезпечення безпеки, складений і реалізований коригуючий План дій.

Причини кожного інциденту мають бути досліджені і встановлені. За результатами розслідування інциденту мають бути вжиті необхідні заходи, спрямовані на мінімізацію вірогідності в майбутньому повторення подібного.

Працівники Банку повинні нести відповідальність за порушення Політики, що призвели до інциденту з інформаційної безпеки.

Клієнт Банку, відносно своїх активів в Банку, має право звернутися в Банк з метою встановлення причин виникнення інциденту та/або усунення причин інциденту, що пов'язаний безпосередньо з активом клієнта Банку.

9. КОНТРОЛЬ ТА ВІДПОВІДАЛЬНІСТЬ

9.1. Відповідно до нормативних актів НБУ, стандарту ДСТУ ISO/IEC 27001:2015, міжнародного стандарту платіжних карт PCI DSS та рішень вищого керівництва Банку в Банку створений та функціонує Комітет з операційних, комплаєнс ризиків та інформаційної безпеки (далі – Комітет). Діяльність Комітету регулюється Положенням про функціонування системи колегіальних органів виконавчого рівня АТ «БАНК КРЕДИТ ДНІПРО». Рішення Комітету є обов'язковими для виконання всіма працівниками Банку та контрагентами в рамках договірних відносин.

9.2. Голова Правління, члени Правління Банку та керівники структурних підрозділів Банку сприяють у створенні, впровадженні, постійному контролю й супроводі Політики та Стратегії розвитку інформаційної безпеки Банку.

9.3. Керівництво Банку несе загальну відповідальність за забезпечення інформаційної безпеки, визначає стратегію та політику у цій сфері, а також забезпечує надання необхідних ресурсів для їх реалізації.

9.4. Відповідальний за інформаційну безпеку призначається відповідним наказом Голови Правління та:

- Забезпечує стратегічне керівництво з питань інформаційної безпеки Банку.
- Визначає напрямки розвитку інформаційної безпеки банку, їх відповідність стратегії розвитку Банку.
- Забезпечує відповідність заходів безпеки інформації потребам бізнес-процесів та банківських продуктів.
- Контролює впровадження заходів безпеки інформації в Банку

9.5. Керівники структурних підрозділів Банку :

- Відповідають за впровадження та дотримання вимог інформаційної безпеки у межах своїх підрозділів.
- Забезпечують виконання працівниками підпорядкованих підрозділів встановлених політик та процедур інформаційної безпеки.

9.6. Працівники Банку:

- Зобов'язані дотримуватися політик та процедур інформаційної безпеки, негайно повідомляти про інциденти або підозри на порушення інформаційної безпеки відповідним відповідальним особам.

9.7. Розробка, підтримка в актуальному стані або ініціювання перегляду Політики інформаційної безпеки входить в межі відповідальності підрозділу Банку, який відповідає за інформаційну безпеку Банку.

9.8. Рішення та рекомендації Департаменту з інформаційної безпеки, підрозділу Банку, який відповідає за інформаційну безпеку Банку щодо застосування заходів та методів захисту з інформаційної безпеки є безперечними і обов'язковими до виконання всіма працівниками Банку.

9.9. Стратегія інформаційної безпеки Банку та Стратегія розвитку інформаційних технологій Банку включаючи всі проекти, що пов'язані з інформаційними активами, не повинні суперечити даній Політиці.

9.10. Кожен працівник Банку або співробітник постачальника (в рамках договірних зобов'язань) бере участь в підтримці високого рівня інформаційної безпеки Банку. В межах своїх посадових обов'язків та повноважень, працівники Банку та/або постачальники, яким надається доступ до ІС банку зобов'язані:

- ознайомлюватися під підпис з Політикою інформаційної безпеки Банку та вимогами інформаційної безпеки, що зазначені у посадових інструкціях або контрактах/договорах (перед початком виконання робіт);
- дотримуватися вимог даної Політики, законодавчих та міжнародних норм, міжнародних стандартів в області інформаційної безпеки, вимог інформаційної безпеки Банку, а також несуть відповідальність за їх порушення в межах, встановлених законодавством України, Кримінальним кодексом України, внутрішньобанківськими нормативними документами, договорами тощо.

9.11. Для мінімізації ризиків виникнення інцидентів інформаційної безпеки через необізнаність користувачів (працівник Банку або співробітник контрагента), Департамент з інформаційної безпеки систематично, доступними методами, повідомляє про ризики інформаційної безпеки працівників, постачальників та клієнтів Банку, навчає працівників Банку і його постачальників нормам та вимогам інформаційної безпеки.

9.12. Для забезпечення ефективного управління інформаційною безпекою Банк проводить регулярний моніторинг і оцінку ефективності заходів безпеки, а також здійснює внутрішні аудиту для виявлення та виправлення можливих порушень або слабких місць у системі захисту інформації.

9.13. На випадок різних непередбачених критичних ситуацій і надзвичайних подій, в Банку складаються, діють, систематично тестуються і оновлюються План забезпечення безперервної діяльності Банку та План аварійного відновлення.

9.14. Ризики, притаманні процесу та процедури контролю за ними:

№ з/п	Короткий опис процедур контролю	Вид ризику	Опис ризику (ідентифікатор ризику)	Періодичність контролю	Рівні контролю			Вид контролю
					1-й рівень контролю	2-й і 3-й рівні контролю	Колегіальний контроль	
1	Забезпечення процедур внутрішнього контролю щодо забезпечення заходів інформаційної безпеки	Операційний ризик Ризик інформаційної безпеки	Порушення конфіденційності, цілісності, доступності даних в інформаційних системах банку	Постійно	Управління інформаційної безпеки	Управління ризик-менеджменту; Управління внутрішнього аудиту	Комітет з операційних, комплаєнс ризиків та інформаційної безпеки	Попередній; Поточний; Подальший
2	Забезпечення процедур внутрішнього контролю щодо забезпечення заходів інформаційної безпеки	Операційний ризик Ризик інформаційної безпеки	Недоліки, помилки або неналежне виконання обов'язків в організації внутрішніх процесів щодо побудови системи забезпечення інформаційної безпеки	Постійно	Управління інформаційної безпеки	Управління ризик-менеджменту; Управління внутрішнього аудиту	Комітет з операційних, комплаєнс ризиків та інформаційної безпеки	Попередній; Подальший
3	Забезпечення процедур внутрішнього контролю щодо забезпечення заходів інформаційної безпеки	Операційний ризик Ризик інформаційної безпеки	настання зовнішніх подій, включаючи кібератаки або неадекватний фізичний вплив на системи інформаційної безпеки	Постійно	Управління інформаційної безпеки	Управління ризик-менеджменту; Управління внутрішнього аудиту	Комітет з операційних, комплаєнс ризиків та інформаційної безпеки	Попередній; Подальший
4	Ризик нечіткого розподілу обов'язків/відповідальності працівників Банку, контрольних функцій	Комплаєнс ризик Операційний ризик	Розподіл обов'язків працівників Банку у внутрішніх нормативних документах Банку, положеннях про підрозділи та посадових інструкціях; наявність контролю перерозподілу	Постійно Періодично	Керівники відповідальних підрозділів /ризик координатори; Управління по роботі з персоналом	Управління комплаєнс; Управління ризик-менеджменту; Управління внутрішнь	Правління та комітети Правління; Рада та комітети Ради	Попередній; Поточний; Подальший

			функцій; контроль актуалізації зазначених документів; проведення навчань працівників, тощо.			ого аудиту		
--	--	--	---	--	--	------------	--	--

10. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

10.1. Ця Політика є безстроковою, затверджується Комітетом (КОКРтаІБ) і набуває чинності з дати, визначеної рішенням Комітету. У разі незазначення дати набрання чинності Політики у протоколі рішення Комітету — Політика набирає чинності з наступного робочого дня з дати затвердження.

10.2. Зміни та доповнення до Політики затверджуються Комітетом та оформлюються у письмовій формі шляхом викладення вимог у новій редакції або шляхом викладення безпосередньо змін до Політики (у випадку, якщо такі зміни є не багаточисленними і таке викладення змін не призводить до ускладнення сприйняття їх суті). Прийняття нової редакції Політики автоматично припиняє дію попередньої версії/ редакції документа.

10.3. У разі невідповідності будь-якої частини Політики чинному законодавству України, нормативно-правовим актам Національного банку України, у тому числі у зв'язку з прийняттям нових актів законодавства України, Політика діє лише у тій частині, що не суперечить чинному законодавству України.

10.4. Надання Політики зовнішнім органам, третім особам відбувається за обов'язковим погодженням з управлінням комплаєнс та з юридичним управлінням відповідно до діючого законодавства України.

10.5. У разі зміни назв структурних підрозділів, які задіяні у процедурах, що описані у Політиці, при незмінності функцій, даний документ вважається дійсним щодо їх нової назви.

10.6. Політика переглядається управлінням інформаційної безпеки не рідше ніж один раз на рік із метою підтримки в актуальному стані та за необхідності – поліпшення ефективності банківських процесів та удосконалення системи внутрішнього контролю.