ЗАТВЕРДЖЕНО
Протокол Наглядової ради
АБ «УКРГАЗБАНК»
від «30» 12 2024 № 46
Голова Наглядової Ради

_____ Санела ПАШІЧ

ПОГОДЖЕНО
Протокол Правління
АБ «УКРГАЗБАНК»
від 19.12.2024 №109
В.о. Голови Правління

_____ Родіон МОРОЗОВ

ПОГОДЖЕНО
Протокол комітету з питань
управління інформаційною
безпекою АБ «УКРГАЗБАНК»
від 13.12.2024 №13
Голова Комітету

_____ Андрій САМОХВАЛОВ

Політика
інформаційної безпеки АБ «УКРГАЗБАНК»

Київ - 2024

ЗМІСТ

Розділ І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Політика інформаційної безпеки АБ «УКРГАЗБАНК» (далі — Політика) є внутрішнім документом АБ «УКРГАЗБАНК» (далі – Банк), який визначає ціль, мету, завдання; сферу застосування інформаційної безпеки та кіберзахисту Банку; загальні принципи, вимоги, правила (організаційних і технічних заходів), що направлені на захист інформаційних активів Банку; визначення функцій і відповідальності за забезпечення інформаційної безпеки та кіберзахисту Банку.

1.2. Банк відноситься до об'єктів критичної інфраструктури в банківській системі України, що враховується Банком в частині забезпечення кіберзахисту в Банку.

1.3. Політика базується на вимогах законодавчих актів України, нормативно-правових актів Національного банку України з питань інформаційної безпеки та кібербезпеки та розроблена з урахуванням вимог:

- Закону України «Про основні засади забезпечення кібербезпеки України»;
- Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затвердженого постановою Правління Національного банку України від 28.09.2017 №95;
- Положення про захист інформації та кіберзахист учасниками платіжного ринку, затвердженого постановою Правління Національного банку України від 19.05.2021 №43;
- Положення про організацію кіберзахисту в банківській системі України, затвердженого постановою Правління Національного банку України від 12.08.2022 №178;
- національних стандартів України з питань інформаційної безпеки ДСТУ EN ISO/IEC 27000:2022 «Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів», ДСТУ ISO/IEC 27001:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги», ДСТУ ISO/IEC 27002:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки»;
- міжнародних стандартів з питань інформаційної безпеки, загальноприйнятих у міжнародній практиці принципів забезпечення інформаційної безпеки і кіберзахисту;
- інших внутрішніх документів Банку.

Розділ ІІ. ВИЗНАЧЕННЯ ТЕРМІНІВ

Бізнес-процес — це систематичне і послідовне виконання певних операцій (функцій), направлених на одержання конкретного результату (продукту/послуги), що має цінність для внутрішніх (посадові особи/структурні підрозділи/працівники Банку) і зовнішніх (клієнти Банку, інші компанії, державні органи і т.д.) споживачів.

Відповідальна особа за інформаційну безпеку Банку (Chief information security officer, CISO) (далі — ВО ІБ) — особа, яка призначена наказом Голови Правління Банку та має повноваження, достатні для прийняття управлінських рішень.

Загроза (threat) — будь-які обставини або події, що можуть бути причиною порушення конфіденційності, цілісності, доступності даних в Системах ІСТ Банку і/або нанесення збитків Системам ІСТ Банку.

Інформаційна безпека — багаторівневий комплекс організаційних заходів Банку, програмних, технічних засобів, що забезпечують захист інформації від випадкових та навмисних загроз, у результаті реалізації яких можливе порушення принципів безпеки: доступності, цілісності та конфіденційності.

Інформація з обмеженим доступом — інформація, що становить державну таємницю, інформацію для службового користування, банківську таємницю, професійну таємницю, таємницю страхування, комерційну таємницю, персональні дані, службову інформацію, дані ЕПЗ.

ІСТ (Information and communication technology) - інформаційно-комунікаційні технології, які охоплюють будь-які технології та засоби, що використовуються для обробки, передачі, отримання, зберігання та обміну інформацією за допомогою електронних засобів комунікації. До складу ІСТ входять Системи ІСТ та окремі програмні (системне, прикладне програмне забезпечення), апаратні засоби (серверне обладнання, комп'ютери, периферійні пристрої) та комунікаційні мережі.

Керівники Банку - Голова, його заступники та члени Наглядової ради Банку, Голова, його заступники та члени Правління Банку, головний бухгалтер Банку.

Клієнт (клієнт Банку) — будь-яка фізична чи юридична особа, що користується послугами Банку.

Надзвичайна ситуація – порушення штатного режиму функціонування Банку, що викликане стихійним лихом, недоступністю Сервісів ІСТ, вірусними загрозами, кібератаками, поширенням епідемії/пандемії, ескалацією військових конфліктів, небезпечним явищем природного чи техногенного характеру, діями людей, яке може нанести шкоду здоров'ю людей та/або призвести до значних матеріальних втрат, настає з моменту прийняття рішення групою відновлення діяльності щодо настання надзвичайної ситуації.

Ресурси критичних бізнес-процесів (КБП)/критичних бізнес-напрямів (КБН) — це Системи ІСТ, які використовуються у рамках КБП/КБН.

Система ІСТ - система, що створена для зберігання, пошуку та обробки інформації, яка є організаційною сукупністю ресурсів (людських, програмних, технічних), що надають та розповсюджують інформацію.

Сервіси ІСТ - сервіси, що надаються через системи інформаційно-комунікаційних технологій внутрішнім або зовнішнім користувачам, включаючи введення даних, зберігання даних, послуги з обробки даних та звітності, а також моніторинг та сервіси з підтримки бізнесу та прийняття рішень.

СУІБ — система управління інформаційною безпекою — перелік цілей, принципів керування, методів, заходів з захисту інформації та забезпечення стійкості бізнес-процесів в інформаційній інфраструктурі Банку.

Третя сторона — (компанія, постачальник, підрядник, провайдер, партнер, клієнт-юридична особа) - юридична або фізична особа, яка володіє достатнім рівнем знань та кваліфікації для надання необхідних послуг Банку або юридична особа, що отримує/має намір отримати послугу Банку, з якою відбувається або може відбуватись обмін інформацією в процесі взаємодії або намірів про взаємодію.

Інші терміни, що вживаються у цій Політиці, використовуються в значеннях, визначених законами України, нормативно-правовими актами Національного банку України (далі - НБУ).

Розділ ІІІ. ЦІЛЬ, МЕТА, ЗАВДАННЯ ТА СФЕРА ЗАСТОСУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КІБЕРЗАХИСТУ БАНКУ

3.1. Ціллю забезпечення захисту інформації, кіберзахисту та інформаційної безпеки Банку є збереження конфіденційності, цілісності даних, доступності інформації та систем, управління ризиками інформаційної безпеки та кіберризиками, захист від кіберзагроз, виконання нормативних вимог, захист репутації банку, фінансова безпека, підвищення кіберстійкості, навчання та усвідомлення персоналу.

3.2. Метою забезпечення захисту інформації, кіберзахисту та інформаційної безпеки Банку є забезпечення комплексного захисту інформаційних активів банку, підтримка довіри клієнтів і дотримання високих стандартів безпеки в умовах сучасних кіберзагроз, надійність функціонування КБП/КБН, захист інформації та ресурсів КБП/КБН від загроз. Джерелами загроз можуть бути навмисні/випадкові людські дії та/або джерела, що не ґрунтуються на людських діях. Банком визначено зовнішні та внутрішні обставини, які важливі для виконання мети забезпечення захисту інформації, кіберзахисту, інформаційної безпеки Банку та впливають на можливість досягнення запланованого результату СУІБ. Зовнішні та внутрішні обставини більш детально регламентовано документами з питань системи управління інформаційною безпекою Банку.

3.3. Завданнями забезпечення захисту інформації, кіберзахисту та інформаційної безпеки Банку є забезпечення безперервної роботи Банку, сприяння мінімізації ризиків операційної діяльності Банку, створення позитивної репутації Банку при роботі з клієнтами.

3.4. Сферою застосування захисту інформації, кіберзахисту та інформаційної безпеки Банку є усі КБП/КБН/ продукти Банку/Системи ІСТ/Сервіси ІСТ.

Розділ IV. ПРИНЦИПИ, ПРАВИЛА, ВИМОГИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КІБЕРЗАХИСТУ БАНКУ

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

- **Цілісності** — властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом;
- **Конфіденційності** — властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом;
- **Доступності** — це властивість інформації при її обробці технічними засобами, що забезпечує безперешкодний доступ до неї для проведення санкціонованих операцій ознайомлення, модифікації або знищення.

4.2. Принципами кіберзахисту, яких дотримується Банк, є:

- пропорційність та адекватність заходів кіберзахисту, що впроваджуються, реальним та потенційним кіберзагрозам;
- пріоритетність запобіжних заходів;
- мінімізація кіберризиків у діяльності Банку;
- дотримання вимог нормативно-правових актів/рекомендацій НБУ з питань інформаційної безпеки та кіберзахисту, рекомендацій Національного банку, уключаючи такі, що можуть бути надані Національним банком за результатами контролю;
- постійної підтримки з боку органів управління Банку кіберстійкості Банку шляхом організації ефективного управління кіберризиками.

4.3. Об'єктами, що підлягають захисту є:

- Системи ІСТ/сервіси ІСТ, обладнання, носії інформації, канали передачі даних, щодо яких Банк забезпечує належний рівень захисту інформації;

- ВДБ/НМДБ щодо обробки, збереження, передачі інформації, власником яких є Банк, або які є предметом професійного, ділового, виробничого, комерційного та інших інтересів Банку.

4.4. Банк розмежовує інформацію з обмеженим доступом від іншої інформації. Перелік інформації, що відноситься до інформації з обмеженим доступом, визначено документами з питань системи управління інформаційною безпекою Банку.

4.5. Серед ресурсів КБП/КБН, на які розповсюджується дія інформаційної безпеки та кіберзахисту, розглядаються наступні типи ресурсів КБП/КБН:

- **Системи ІСТ** — Системи ІСТ, що використовуються структурними підрозділами Банку для виконання своїх функцій, що визначені у переліку Систем ІСТ;
- **інженерна інфраструктура** — електроживлення, заземлення, система кондиціювання та вентиляції, система контролю доступу та відеоспостереження, пожежної сигналізації тощо;
- **об'єкти** — режимні приміщення, такі як (спеціалізовані) приміщення з обмеженим доступом, серверні приміщення, комутаційні кімнати тощо, в яких розміщена інженерна інфраструктура, серверне та мережеве обладнання;
- **персонал** — керівники самостійних структурних підрозділів, що забезпечують прийняття рішень та загальний процес управління ресурсами КБП/КБН; працівники Банку, які забезпечують функціонування Систем ІСТ та Сервісів ІСТ; працівники ДІБ, які забезпечують належний рівень функціонування інформаційної безпеки/кіберзахисту, Систем ІСТ та Сервісів ІСТ; працівники Банку, які використовують Системи ІСТ та Сервіси ІСТ (до цієї категорії відносяться усі працівники Банку, які не належать до керівників самостійних структурних підрозділів та працівники Банку, які забезпечують функціонування Систем ІСТ та Сервісів ІСТ).

4.6. Банк захищає інформацію і ресурси КБП/КБН фізичними, апаратними, програмними, нормативними та цивільно-правовими шляхами.

4.7. Банк дотримується наступних правил та вимог в частині забезпечення інформаційної безпеки, кіберзахисту та безперервності діяльності:

- працівники Банку та працівники третіх сторін беруть участь у підтримці відповідного рівня інформаційної безпеки та кіберзахисту в межах своїх обов'язків та повноважень і несуть відповідальність за його порушення в межах, встановлених законодавством України та документами Банку;
- дотримання вимог інформаційної безпеки та кіберзахисту під час розроблення, впровадження та функціонування Систем ІСТ/Сервісів ІСТ;
- публічні сервіси Банку та внутрішня мережа Банку відповідають вимогам інформаційної безпеки та кіберзахисту;

• Банк встановлює та моніторить виконання усіх вимог інформаційної безпеки та кіберзахисту, які наявні в угодах з третіми сторонами, зокрема стосовно участі у міжнародних платіжних системах та системах переказу коштів (вимоги зацікавлених сторін);

• працівники Банку систематично проходять навчання нормам та заходам інформаційної безпеки та кіберзахисту, з захисту персональних даних, інформаційних технологій;

• працівники Банку в межах своїх повноважень ознайомлюються з документами з питань системи управління інформаційною безпекою Банку, які містять вимоги та правила інформаційної безпеки та кіберзахисту в Банку;

• у Банку складаються, діють, систематично тестуються та оновлюються плани на випадок надзвичайних ситуацій та кібератак:

- План відновлення діяльності АБ "УКРГАЗБАНК";
- План забезпечення безперервності діяльності АБ «УКРГАЗБАНК»;
- Плани забезпечення безперервного функціонування критичних бізнес-напрямів;
- План забезпечення безперервності та відновлення функціонування Систем ІСТ АБ "УКРГАЗБАНК";
- План забезпечення безперервного функціонування Дирекцій та відділень АБ «УКРГАЗБАНК».

4.8. Про кожний інцидент інформаційної безпеки/кіберінцидент працівники Банку зобов'язані негайно сповістити свого безпосереднього керівника та департамент інформаційної безпеки Банку. Банком відповідно до документів з питань системи управління інформаційною безпекою Банку передбачено аналіз та реакцію (в тому числі на рівні комунікації) на той чи інший інцидент інформаційної безпеки/кіберінцидент. За результатами аналізу вживаються заходи, направлені на недопущення повторення подібних інцидентів інформаційної безпеки/кіберінцидентів.

4.9. Зміст Політики доводиться до відома всіх працівників Банку у встановленому в Банку порядку.

4.10. Зміст Політики є доступним, за потреби, зацікавленим сторонам. Політика розміщена на веб-сайті Банку https://www.ukrgasbank.com, в розділі «Про банк» — «Внутрішні документи».

4.11. Всі працівники Банку підписують зобов'язання про зберігання інформації з обмеженим доступом Банку та зобов'язання про дотримання вимог з інформаційної безпеки АБ «УКРГАЗБАНК». Ці зобов'язання залишаються чинними протягом всього періоду роботи працівника в Банку та необмежений час після його звільнення.

4.12. Всі працівники третіх сторін, які мають доступ до Систем ІСТ/Сервісів ІСТ, на виконання вимог угоди про нерозголошення інформації з обмеженим доступом (далі - Угода), до того, як вони приступають до виконання своїх обов'язків, підписують Зобов'язання про нерозголошення інформації з обмеженим доступом АБ «УКРГАЗБАНК», яке залишається чинним протягом всього періоду дії Угоди з третьою стороною та після закінчення дії Угоди протягом терміну, що визначений цією Угодою.

4.13. Всі працівники Банку, працівники третіх сторін, незалежно від рівнів доступу до інформації, Систем ІСТ, Сервісів ІСТ та ресурсів КБП/КБН, мають дотримуватись вимог цієї Політики.

4.14. Банк, при отриманні послуг, що надаються третіми сторонами, яким надано доступ до Систем ІСТ/Сервісів ІСТ, вимагає дотримання вимог третіми сторонами норм цієї Політики.

4.15. Банком використовуються наступні підходи щодо забезпечення інформаційної безпеки та кіберзахисту:

- створено та затверджено перелік інформації, що містить інформацію з обмеженим доступом;
- створено та затверджено перелік КБП/КБН, за якими проводиться оцінка ризиків інформаційної безпеки та подальша їх обробка;
- встановлено правила доступу до Систем ІСТ/Сервісів ІСТ;
- забезпечується контроль фізичного та логічного доступу до всіх визначених Систем ІСТ/Сервісів ІСТ;
- забезпечується парольний захист Систем ІСТ/Сервісів ІСТ;
- забезпечується антивірусний захист Систем ІСТ/Сервісів ІСТ;
- забезпечується захист мережі Банку;
- забезпечується захищений віддалений доступ до ресурсів мережі (локальної, мережі Інтернет);
- забезпечується захист від кібератак електронних інформаційних ресурсів, що доступні з мережі Інтернет та інших глобальних мереж передачі даних;
- забезпечується інвентаризація визначених ресурсів КБП/КБН;
- забезпечується криптографічний захист інформації;
- проводяться внутрішні аудити СУІБ та аналіз СУІБ з боку керівників Банку;
- здійснюється моніторинг та вдосконалення СУІБ.

4.16. Дотримання вимог цієї Політики та вимог інформаційної безпеки та кіберзахисту Банку дозволить мінімізувати ризики інформаційної безпеки, які можуть мати негативні наслідки для Банку.

4.17. Банк керується ризик-орієнтованим підходом, який забезпечує розуміння, моніторинг та зменшення ризиків в тих сферах діяльності Банку, яким притаманні більші ризики, зокрема операційний ризик, включаючи ризики інформаційної безпеки/кіберризики. Принцип ризик-орієнтовного підходу більш детально регламентовано внутрішніми документами Банку з питань системи управління інформаційною безпекою Банку.

4.18. З метою реалізації ризик-орієнтованого підходу у Банку діють модель порушника та модель загроз кіберзахисту/інформаційній безпеці Банку (Додаток 1 до Політики). Модель порушника складається на основі аналізу типу зловмисника, рівня його повноважень, знань, теоретичних та практичних можливостей.

Модель порушника та модель загроз кіберзахисту/інформаційній безпеці Банку використовуються у оцінці ризиків інформаційної безпеки Банку.

Розділ V. ФУНКЦІЇ УЧАСНИКІВ ПРОЦЕСУ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КІБЕРЗАХИСТУ БАНКУ

5.1. ВО ІБ:

- забезпечує виконання заходів, передбачених Положенням №95, в тому числі стратегічне керівництво з питань інформаційної безпеки Банку, визначення напрямів розвитку інформаційної безпеки Банку, їх відповідність стратегії розвитку Банку, відповідність заходів безпеки інформації потребам бізнес-процесів/продуктів Банку та контроль за впровадженням заходів безпеки інформації в Банку;

- забезпечує виконання заходів, передбачених Положенням №178, в тому числі пріоритетної реалізації заходів кіберзахисту критичної інформаційної інфраструктури Банку;

- забезпечує виконання заходів, передбачених Положенням № 43, в тому числі захист інформації та кіберзахист учасниками платіжного ринку.

5.2. Комітет з питань управління інформаційною безпекою АБ «УКРГАЗБАНК» (далі - Комітет) є колегіальним органом Банку з питань впровадження та функціонування СУІБ, який здійснює координацію діяльності структурних підрозділів Банку щодо функціонування СУІБ та на який покладено обов'язок виконання таких основних завдань:

1) перегляд та погодження Політики, та Стратегії розвитку інформаційної безпеки АБ «УКРГАЗБАНК» на 2023-2025 роки;

2) узгодження впровадження нових проектів, напрямів, стратегічних завдань з питань інформаційної безпеки/кіберзахисту Банку та заходів інформаційної безпеки;

3) розгляд, затвердження та контроль за виконанням проектів щодо розроблення, упровадження, функціонування, моніторингу, перегляду, підтримання та вдосконалення СУІБ Банку;

4) визначення необхідних оптимальних ресурсів для впровадження заходів інформаційної безпеки/кіберзахисту;

5) організація практичних заходів щодо підвищення обізнаності/ навчання персоналу Банку з питань інформаційної безпеки/кіберзахисту (в тому числі стандартів ISO/IEC групи 27000), стандартів Payment Card Industry Data Security Standard (PCI DSS) та VISA PCI PIN Security (PIN Security) та Концепції забезпечення безпеки користувачів SWIFT і принципам забезпечення інформаційної безпеки;

6) забезпечення своєчасного моніторингу стану впровадження та ефективності функціонування СУІБ Банку з подальшою оцінкою можливостей вдосконалення та потреби проведення коригувальних дій.

Детально завдання, функції та відповідальність Комітету визначені Положенням про комітет з питань управління інформаційною безпекою АБ°«УКРГАЗБАНК».

5.3. Департамент інформаційної безпеки виконує функції із забезпечення режиму інформаційної безпеки/кіберзахисту, основними завданнями якого є:

1) забезпечення та контроль розроблення вимог щодо налаштувань безпеки Систем ІСТ Банку;

2) розроблення або участь у розробленні документів з питань системи управління інформаційною безпекою;

3) організація та контроль за виконанням заходів щодо забезпечення безпеки інформації на всіх стадіях життєвого циклу Систем ІСТ Банку;

4) організація та контроль процесу управління інцидентами інформаційної безпеки/кіберінцидентами;

5) взаємодія із структурними підрозділами в процесі відновлення функціонування Систем ІСТ Банку після збоїв у роботі внаслідок інцидентів інформаційної безпеки/кіберінцидентів.

Детально завдання, функції та відповідальність департаменту інформаційної безпеки визначені Положенням про департамент інформаційної безпеки АБ «УКРГАЗБАНК».

5.4. Працівники Банку усвідомлюють важливість і необхідність уваги до напрямку інформаційної безпеки/кіберзахисту Банку, дотримуються та беззаперечно виконують всі правила, процедури та вимоги документів з питань системи управління інформаційною безпекою, вказівки/рішення Керівників Банку/Комітету та департаменту інформаційної

безпеки щодо підтримки належного стану інформаційної безпеки/кіберзахисту, а також сприяють розвитку інформаційної безпеки/кіберзахисту в Банку, у разі необхідності.

Розділ VI. КОНТРОЛЬ ТА ВІДПОВІДАЛЬНІСТЬ

6.1. Опис системи внутрішнього контролю бізнес-процесу "Методологія інформаційної безпеки" визначається в Додатку 2 до Політики.

6.2. Керівники Банку чітко розуміють, що інформаційна безпека та кіберзахист Банку є основою життєдіяльності Банку та забезпечують (організаційно та фінансово) впровадження, підтримку та контроль належного рівня інформаційної безпеки та кіберзахисту Банку.

6.3. Керівники Банку підтримують інформаційну безпеку та кіберзахист в межах Банку шляхом чіткого регулювання, підтверджених зобов'язань, чітких призначень та визнання відповідальності.

6.4. ВО ІБ є відповідальним за інформаційну безпеку та кіберзахист Банку.

6.5. Кожний працівник несе відповідальність за дотримання норм інформаційної безпеки та кіберзахисту Банку.

6.6. Кожен структурний підрозділ Банку бере участь у підтримці відповідного рівня інформаційної безпеки та кіберзахисту Банку в межах своїх функцій та повноважень, несе відповідальність за їх порушення в межах, встановлених чинним законодавством України та внутрішніми документами Банку.

6.7. Суб'єкти СУІБ несуть відповідальність за виконання своїх функцій, передбачених Розділом 5 цієї Політики. Відповідальність суб'єктів СУІБ визначається відповідно до законодавства України та документів Банку.

Розділ VII. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

7.1. Ця Політика набирає чинності з дати її затвердження Наглядовою радою Банку.

7.2. Зміни та доповнення до цієї Політики затверджуються Наглядовою радою та набирають чинності з дати їх затвердження.

7.3. У разі внесення змін до законодавства України або нормативно-правових актів Національного банку України ця Політика діє у тій частині, що не суперечить законодавству України, до моменту внесення відповідних змін, актуалізації або видання нової її редакції, згідно встановленого в Банку порядку.

7.4. Ця Політика підлягає періодичному перегляду не рідше 1 (одного) разу на рік.

7.5. У разі, якщо при здійсненні перегляду цієї Політики у строк, зазначений у пункті 7.4. цієї Політики, власником Політики встановлена відповідність чинної версії Політики

законодавству України, у тому числі нормативно-правовим актам Національного банку України, дія яких поширюється на Банк, ця Політика вважається актуальною та підлягає наступному перегляду не пізніше строку, зазначеного в пункті 7.4 цієї Політики.

ПІДГОТОВЛЕНО:

Директор департаменту інформаційної безпеки Сергій НЕДЗЕЛЬСЬКИЙ

ПОГОДЖЕНО:

Заступник Голови Правління Андрій САМОХВАЛОВ

Директор юридичного департаменту Ігор ПРИШКО

Директор департаменту комплаєнс Раджамі ДЖАН