ЗАТВЕРДЖЕНО

Протокол засідання Правління
АТ «МОТОР-БАНК»
«07» жовтня 2022 р. № 02/10/22
Голова Правління АТ «МОТОР-БАНК»
_____Вадим ЧИХУН

ПОЛІТИКА

інформаційної безпеки АТ «МОТОР-БАНК»

ІІ-01-А5-0822
(нова редакція)

м.Запоріжжя – 2022

ЗМІСТ

1. Загальні положення

1.1. Політика інформаційної безпеки АТ «МОТОР-БАНК» (далі - Політика) описує та регламентує функціонування системи управління інформаційною безпекою АТ «МОТОР-БАНК» (далі – Банк) відповідно до Законів України «Про інформацію», «Про банки та банківську діяльність», «Про захист персональних даних», «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 року за №95, Положення про організацію системи управління ризиками в банках України та банківських групах, затвердженого Постановою Правління Національного банку України від 11.06.2018 № 64 (із змінами), Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг, затвердженого Постановою правління Національного банку України від 16.01.2021 р. № 4, Положення про організацію кіберзахисту в банківській системі України, затвердженого Постановою правління Національного банку України від 12.08.2022 р. № 178, настанов та вимог національних стандартів ДСТУ ISO/IEC 27000:2019 «Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів», ДСТУ ISO/IEC 27001:2015 “Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги”, ДСТУ ISO/IEC 27002:2015 “Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки”, ДСТУ ISO/IEC 27005:2019 «Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки», які прийняті наказами Державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 18.12.2015 №193 та від 16.10.2019 № 312, адаптованих для застосування в банківської системі України, відповідає вимогам чинного законодавства України в тому числі нормативно-правовим актам Національного банку України, а також вимогам міжнародних та внутрішньодержавних платіжних систем та систем переказу коштів. При цьому, також застосовуються інші міжнародні і національні стандарти щодо інформаційної безпеки, наприклад стандарт безпеки даних індустрії платіжних карток PCI DSS, стандарти групи ISO 27000 та інші, якщо вони не суперечать вищевказаним стандартам.

1.2. Політика визначає принципи, складові частини і зміст процесу управління безпекою інформаційних ресурсів Банку.

1.3. Політика є керівним документом і поширюється на всіх працівників Банку, допущених до роботи з інформаційною системою Банку, а також на фізичних та юридичних осіб, що працюють з інформаційними системами Банку або з інформацією, яка належить Банку. Політика також поширюється на організацію співпраці із зовнішніми партнерами, постачальниками, бізнес-партнерами тощо та з іншими юридичними або фізичними особами, що забезпечують сервіси, пов'язані з використанням інформаційних ресурсів Банку.

1.4. Відносини між працівниками Банку, а також сторонніми особами та третіми сторонами, що виникають під час реалізації механізмів забезпечення інформаційної безпеки, регулюються нормативними документами інформаційної безпеки, затвердженими керівництвом Банку. Нормативні документи інформаційної безпеки є одним з ключових елементів інфраструктури інформаційної безпеки, який забезпечує розуміння персоналом своїх обов'язків та відповідальності щодо виконання вимог інформаційної безпеки.

1.5. Всі посадові особи Банку зобов'язані виконувати вимоги, викладені у нормативно правових актах з питань забезпечення інформаційної безпеки, та несуть відповідальність за їх невиконання.

1.6. Політика є документом верхнього рівня Системи управління інформаційною безпекою (СУІБ) Банку.

2. Визначення термінів

2.1. В цій Політиці терміни вживаються в такому значенні:

CISO (Chief information security officer) – відповідальна особа за інформаційну безпеку Банку, яка має повноваження, достатні для прийняття управлінських рішень (посада не нижче заступника Голови Правління Банку)

Інформаційні активи Банку – активи Банку, що мають відношення до його інформаційної сфери.

Інформаційна безпека Банку – стан захищеності інформаційних активів Банку в умовах загроз в інформаційній сфері.

Керівний орган СУІБ – керівний орган з питань впровадження та функціонування СУІБ.

Політика інформаційної безпеки - це сукупність основних норм, правил, вимог, на основі яких будується система управління безпекою в сфері обігу, зберігання та розповсюдження інформаційних ресурсів Банку. Політика формується на основі аналізу поточного стану і перспектив розвитку інформаційної системи Банку, а також можливих загроз, і визначає:

- цілі, пріоритети та область дії системи інформаційної безпеки Банку;
- положення щодо намірів і підтримки реалізації цілей та принципів інформаційної безпеки Банку згідно з бізнес-стратегіями Банку;
- короткого пояснення важливих для Банку принципів, стандартів безпеки та вимог щодо відповідності;
- посилання на окремі документи, що підтримують Політику, визначають обов'язки персоналу з управління інформаційною безпекою, включаючи звітування щодо інцидентів інформаційної безпеки та спектру санкцій за порушення інформаційної безпеки.

Для реалізації Політики безпеки створюється система управління інформаційною безпекою, що включає в себе комплекс різних заходів.

Система управління інформаційною безпекою (СУІБ) - сукупність заходів і засобів захисту, ресурсів для забезпечення інформаційної безпеки та процесів управління інформаційною безпекою у повному обсязі.

Структурні підрозділи – підрозділи банку відповідно до Організаційної структури АТ «МОТОР-БАНК», в тому числі відокремлені підрозділи (відділення).

2.2. Інші терміни, що вживаються у цій Політиці, застосовуються в значеннях, визначених законодавчими актами України, нормативно-правовими актами Національного банку України та іншими внутрішніми документами Банку.

3. Цілі Політики інформаційної безпеки

3.1. Політика визначає цілі та засади забезпечення інформаційної безпеки в діяльності Банку та розподіл відповідальності за її дотриманням. Політика відображає позицію керівництва Банку за найбільш принциповими напрямками інформаційної безпеки та складена для формування цілісного уявлення про інформаційну безпеку в Банку.

3.2. Основною ціллю Політики Банку є ефективне функціонування СУІБ Банку, що забезпечує захист інформації та ресурсів Банку від зовнішніх і внутрішніх загроз та загроз, що пов’язані з навмисними та ненавмисними діями працівників Банку, забезпечувати безперервну роботу Банку, сприяти мінімізації ризиків операційної діяльності Банку та створювати позитивну репутацію Банку при роботі з клієнтами.

Цілі інформаційної безпеки:

- мінімізація бізнес-ризиків або зведення до мінімуму можливих збитків від зовнішніх та внутрішніх загроз та загроз, що пов’язані з операційною діяльністю Банку та навмисними чи ненавмисними діями працівників Банку;
- забезпечення безперервної роботи Банку;

- збільшення ефективності інвестицій та можливостей діяльності Банку;
- створення позитивної репутації Банку при роботі з клієнтами.

3.3.Пріоритетом при реалізації Політики вважаються такі цілі та заходи, що при мінімумі фінансових витрат створюють достатній рівень захисту інформаційних активів Банку.

4. Сфера застосування Політики інформаційної безпеки

4.1. Політика розповсюджується на:
- діяльність Банку у цілому;
- всі критичні бізнес-процеси/банківські продукти Банку;
- всі програмно-технічні засоби;
- працівників Банку;
- юридичних та фізичних осіб Банку, які працюють з інформаційними системами Банку, у частині взаємодії з Банком або з інформацією, яка належить Банку;
- зовнішніх партнерів, контрагентів, постачальників Банку у частину взаємодії з Банком;
- юридичних та фізичних осіб, які забезпечують інформаційні та інші сервіси Банку, дії яких можуть вплинути на забезпечення інформаційної безпеки Банку.

5. Засади Політики інформаційної безпеки

5.1. Інформаційна безпека підтримує бізнес-цілі (місію) Банку, а саме спрямована на підтримання прийнятного та достатнього рівня безпеки з огляду на існуюче оточення оскільки основною метою Банку є отримання прибутку, виходячи з фінансових витрат і цінності інформаційних ресурсів на базі аналізу та оцінки ризиків та використання відповідних засобів захисту.

5.2. Інформаційна безпека - інтегральний елемент системи управління і є частиною загальної політики безпеки Банку.

5.3. Ефективність інформаційної безпеки.

Витрати не повинні перевищувати вигоди від впровадження систем безпеки. Тому повинні бути визначені витрати та вигоди від безпеки, як у фінансовому, так і в інших аспектах. Заходи безпеки реалізуються пропорційне цінностям, надійності комп'ютерних систем та потенційним збиткам.

5.4. Відповідальність та звітність з питань інформаційної безпеки.

Під відповідальністю розуміються функціональні обов'язки та очікувані дії. На безпеку в цілому має вплив ступінь відповідальності та звітності власників системи і користувачів.

5.5. Ретельний і цілісній підхід.

Безпека повинна розглядатися на всіх етапах життєвого циклу інформації. Інформаційна безпека Банку використовує всі види контролю з оглядом на фінансові можливості, та існує поряд з іншими видами безпеки, такими як фізична безпека, безпека персоналу тощо.

5.6. Періодичний перегляд Політики.

Інформаційна система Банку є динамічною системою, в якої користувачі, дані та інформація знаходяться в постійній зміні, що у цілому впливає на інформаційну безпеку Банку.

Обов'язок Банку забезпечити підтримку Політики в актуальному стані та здійснювати її перегляд у строки визначені п. 11.2. цієї Політики.

5.7. Суперечливий і компромісний характер інформаційної безпеки.

Відносини між безпекою та прийнятими нормами у Банку можуть бути антагоністичними. Політика та процедури безпеки вступають в конфлікт з щоденною поточною діяльністю. Дозвіл компромісних ситуацій повинен вирішуватися керівництвом Банку.

6. Застосування властивостей інформації

6.1. СУІБ Банку з ціллю підтримання належного захисту інформації застосовує такі властивості інформації як цілісність, конфіденційність, доступність та спостережність:

- цілісність – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем та/або процесом. Щодо інформаційної системи, цілісність розглядається як властивість системи, при якій жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки;
- конфіденційність – властивість інформації, при якій інформація є недоступною для неавторизованих осіб та/або процесів;
- доступність – властивість інформаційного активу (ресурсу), при якій користувач та/або процес, володіючи відповідними повноваженнями, може використовувати інформаційний актив відповідно до правил, встановлених політикою безпеки;
- спостережність – властивість системи, яка покликана 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.

6.2. У Банку при необхідності застосовуються інші властивості такі як автентичність, відстежуваність, неспростовність та надійність, але властивості згідно п.6.1. вважаються головними.

6.3. Зазначені в п.6.1., цієї Політики, властивості інформації, в першу чергу, стосуються інформації з обмеженим доступом (банківська таємниця, комерційна таємниця, конфіденційна інформація, персональні дані).

7. Принципи Політики інформаційної безпеки

7.1. Для досягнення певного рівня інформаційної безпеки Банку використовуються наступні принципи організації та функціонування СУІБ:

7.1.1. Принцип законності, який передбачає здійснення, розробку і реалізацію заходів щодо інформаційної безпеки Банку відповідно до законодавства України та нормативно-правових актів Національного банку в області інформаційної політики, у тому числі захисту інформації, із застосуванням методів виявлення і припинення правопорушень при роботі з інформацією.

7.1.2. Принцип спеціалізації - експлуатація технічних засобів захисту та реалізація заходів інформаційної безпеки повинна здійснюватися виключно кваліфіковано підготовленими, в достатній кількості, фахівцями Банку, що забезпечують безпеку інформаційних активів Банку з можливістю залучення фірм та організацій, які підготовлені до такого виду діяльності, мають відповідний досвід та право на проведення цих робіт.

7.1.3. Принцип персональної відповідальності, який передбачає покладання відповідальності щодо забезпечення безпеки інформації та інформаційних систем на кожного працівника Банку в межах їх повноважень. Відповідно до цього принципу розподіл прав і обов'язків працівників Банку будується так, щоб у разі будь-якого порушення круг винуватців був чітко відомий або зведений до мінімуму.

7.1.4. Принцип поінформованості - користувачі інформаційної системи Банку повинні бути проінформовані про існування і загальний обсяг заходів, дій, процедур, що забезпечують безпеку інформаційних систем Банку. Поінформованість сприяє посиленню існуючих методів управління, дає можливість застосування додаткових заходів безпеки і веде до зниження конкретної загрози.

7.1.5. Принцип адекватності - застосовані захисні заходи повинні бути адекватними можливому рівню пошкодження інформаційних активів (ресурсів) Банку. Ці заходи потребують використання ресурсів Банку, мають певну ціну для розробки, придбання, виконання, безперервного контролю за заходами безпеки.

7.1.6. Принцип звітності - звітність про безпеку інформаційної системи Банку повинна бути точною і вичерпною. Цей принцип пов'язаний з необхідністю ясного визначення та розмежування ролей і дій всіх осіб, які працюють з інформацією.

7.1.7. Принцип своєчасності - для запобігання та швидкої реакції у разі виникнення проломів в безпеці інформаційної системи Банку, користувачі повинні діяти своєчасно і узгоджено. Цей принцип також визначає, що при прийнятті рішень щодо зниження ризику, принципи інформаційної безпеки Банку повинні ґрунтуватися на своєчасній та достовірній інформації про ступінь загрози та вразливості системи.

7.1.8. Принцип безперервної діяльності у сфері захисту. Забезпечення безпеки інформації - це процес, який повинен постійно підтримуватись у Банку і кожен працівник Банку повинен брати участь в цьому процесі.

7.1.9. Принцип внутрішнього контролю - безпека становить ядро системи внутрішнього інформаційного контролю Банку. Контроль передбачає обов'язковість і своєчасність виявлення і припинення спроб порушення встановлених правил інформаційної безпеки Банку, на основі використання легальних систем і засобів захисту інформації.

7.1.10. Принцип централізації політики безпеки – принцип, який передбачає самостійне функціонування системи безпеки за єдиними організаційними, функціональними і методологічними принципами з централізованим управлінням діяльністю системи безпеки.

8. Предмет та вимоги Політики інформаційної безпеки

8.1. Банк підтримує ризик-орієнтовний підхід, який забезпечує розуміння, моніторинг та зменшення ризиків операційної діяльності. Деталі ризик-орієнтовного підходу описані в Положенні про управління ризиками інформаційної безпеки АТ «МОТОР-БАНК».

8.2. Політика базується на реалізації засад забезпечення комплаєнсу та внутрішнього банківського контролю, виконанню вимог чинного національного законодавства та внутрішніх нормативних документів Банку.

8.3. Весь персонал Банку обізнаний та виконує вимоги інформаційної безпеки Банку у роботі згідно Порядку щодо забезпечення інформаційної безпеки людських ресурсів АТ «МОТОР-БАНК», у якому викладено спектр санкцій за порушення вимог інформаційної безпеки.

Звітування щодо інцидентів інформаційної безпеки Банку здійснюється згідно Порядку реєстрації та моніторингу подій операційного ризику АТ «МОТОР-БАНК».

Під час розроблення, впровадження та функціонування програмно-технічних комплексів враховуються вимоги інформаційної безпеки Банку.

8.4. Інформація щодо дій про надання, скасування чи зміни доступу до інформаційних систем банку, які безпосередньо забезпечують автоматизацію банківської діяльності, знаходиться у базах даних у захищених від несанкціонованої модифікації електронних журналах із забезпеченням їх збереження не менше ніж протягом трьох років, контроль цілісності якої здійснюється засобами системи управління базами даних.

8.5. Публічні сервіси Банку та внутрішні мережі Банку відповідають вимогам стандартів з інформаційної безпеки Банку.

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

8.7. Банк забезпечує виконання вимог інформаційної безпеки в угодах з третьої стороною. Політика або її основні засади додаються по можливості до кожного договору з третьою стороною та є його невід’ємною частиною.

9. Порядок ознайомлення з Політикою інформаційної безпеки

9.1. З Політикою ознайомлюються в обов'язковому порядку всі працівники Банку, яких підключено або підключаються до інформаційної мережі АТ «МОТОР-БАНК».

З Політикою також ознайомлюються клієнти, контрагенти, які мають з Банком договірні зобов'язання та інші треті особи. На запит третіх осіб сканована копія Політики в паперовому або електронному вигляді може бути направлена на їх адресу.

9.2. Ознайомлення працівників з Політикою здійснюється у разі прийняття їх на роботу або затвердження нової редакції Політики або внесення змін. Ознайомлення виконується засобами системи електронного діловодства «АСКОД». У разі, коли працівник не має можливості роботи з системою електронного діловодства, останній заповнює у вільній формі Аркуш узгодження з Політикою у паперовій формі та направляє його адміністратору інформаційної безпеки. Адміністратор інформаційної безпеки інформує таких працівників щодо появи нової редакції Політики засобами електронної пошти або іншими засобами інформування.

9.3. При прийнятті працівника на роботу, ознайомлення з Політикою проводиться після підключення його до системи електронного діловодства «АСКОД».

9.4. У разі відмови з боку працівника Банку провести ознайомлення з Політикою, адміністратор інформаційної безпеки повідомляє про це відповідальну особу за інформаційну безпеку Банку для прийняття відповідних адміністративних заходів впливу. Адміністратор інформаційної безпеки має право на відключення користувача, який не ознайомився з Політикою, від інформаційної мережі Банку.

9.5. Політика розміщується на загально доступних для користувачів інформаційних системах та ресурсах Банку.

9.6. Політика розміщується на офіційному сайті Банку та повинна бути доступна для відвідувачів сайту. На сайті Банку розміщується остання редакція Політики.

10. Визначення функцій (ролей) і відповідальності за забезпечення інформаційної безпеки

10.1. Керівництво Банку чітко розуміє, що інформаційна безпека Банку є одним із основних напрямів його життєдіяльності. У Банку сформовано та постійно працює колективний керівний орган СУІБ, а саме Комісія з питань інформаційної безпеки Банку (далі-Комісія), рішення якої є обов'язковими для виконання усіма працівниками Банку.

10.2. До складу комісії входить Голова Правління Банку, Перший заступник Голови Правління, Начальник інформаційної безпеки та керівники підрозділів.

10.3. Комісія підпорядковується Правлінню Банку, здійснює роботу під його керівництвом та контролем, має право приймати рішення в межах своєї компетенції.

10.4. Мета, функції та компетенція Комісії зазначені в п.2 та п.3 Положення про Комісію з питань інформаційної безпеки АТ «МОТОР-БАНК».

10.5. Банком призначено відповідальну особу за інформаційну безпеку банку (CISO), яка входить до складу Комісії і має повноваження, достатні для прийняття управлінських рішень та забезпечує:

1) стратегічне керівництво з питань інформаційної безпеки банку;

2) визначення напрямів розвитку інформаційної безпеки банку, їх відповідність стратегії розвитку банку;

3) відповідність заходів безпеки інформації потребам бізнес-процесів/банківських продуктів;

4) контроль за функціонуванням інформаційної структури Банку;

5) контроль за впровадженням заходів безпеки інформації в банку.

10.6. Документи, що є складовою Політики, розробляються Відділом інформаційної безпеки, здійснюючого реалізацію та контроль виконання цієї Політики, сумісно з іншими підрозділами за відповідними напрямками діяльності. Постійний контроль впровадження, виконання, вдосконалення та підтримки Політики в актуальному стані покладено на CISO Банку.

10.7. Керівництво Банку сприяє створенню, впровадженню, контролю та підтримці Політики.

10.8. Стратегія розвитку інформаційних технологій Банку, всі проекти, які пов’язані з інформаційними технологіями, узгоджуються з Політикою.

10.9. Кожен працівник Банку забезпечує підтримку відповідного рівня інформаційної безпеки Банку. В межах своїх службових обов’язків та повноважень працівники виконують та відповідають за виконання вимог цієї Політики, законодавчих, регуляторних і внутрішньобанківських норм і несуть відповідальність за їх порушення згідно із законодавством України та внутрішніми документами Банку.

10.10. З метою виникнення конфлікту інтересів в інформаційних системах Банку, які безпосередньо забезпечують автоматизацію банківських процесів/продуктів, забороняється суміщення в межах однієї функції таких повноважень: розроблення та супроводження (адміністрування), розроблення та експлуатація, супроводження (адміністрування) та експлуатація, виконання операцій в таких системах та подальшого контролю за їх виконанням.

10.11. Підрозділу інформаційних технологій (інформатизації, автоматизації) банку забороняється бути власником інформаційних систем банку, які безпосередньо забезпечують автоматизацію банківської діяльності.

10.12. Працівникам підрозділу інформаційної безпеки/CISO Банку забороняється мати повноваження з розроблення, упровадження, супроводження (адміністрування) та експлуатації інформаційних систем банку, крім тих, що використовуються для забезпечення безпеки інформації.

10.13. Документи, що є складовою Політики, доступні працівникам Банку у межах їх повноважень на доступних інформаційних ресурсах та призначені надавати допомогу у виконанні вимог інформаційної безпеки Банку.

10.14. Для зменшення ризиків виникнення інцидентів інформаційної безпеки керівництво Банку створює працівникам умови для систематичного вивчення норм та вимог до інформаційної безпеки Банку.

10.15. У Банку складаються, діють, тестуються та оновляються План забезпечення безперервної діяльності в АТ «МОТОР-БАНК» у цілому та Інструкції щодо забезпечення безперервної діяльності структурних підрозділів на випадок непередбачених ситуацій (дія стихійного лиха, нещасні випадки, відмова обладнання або зловмисні дії тощо).

10.16. Працівники Банку несуть персональну відповідальність за підтримку та додержання всіх політик, стандартів та інструкцій з питань інформаційної безпеки в Банку.

10.17. Працівники Банку несуть персональну відповідальність за порушення вимог інформаційної безпеки.

10.18. Працівники Банку несуть персональну відповідальність за порушення вимог звітування щодо інцидентів інформаційної безпеки.

10.19. Керівники структурних підрозділів Банку несуть персональну відповідальність за підтримання цілісності, доступності та конфіденційності інформаційних активів підпорядкованого структурного підрозділу.

10.20. Керівники структурних підрозділів Банку несуть персональну відповідальність за забезпечення виконання всіх політик, стандартів та інструкцій з питань інформаційної безпеки у структурному підрозділі.

10.21. Основні обов'язки працівників Відділу інформаційної безпеки Банку по виконанню цієї Політики визначаються Положенням про відділ інформаційної безпеки АТ «МОТОР-БАНК» та посадовими інструкціями, а також внутрішніми документами Банку, включених у склад Політики.

11. Прикінцеві положення

11.1. Ця Політика набирає чинності з дати її затвердження рішенням Правління Банку.

11.2. Ця Політика підлягає обов'язковому перегляду на предмет її відповідності поточній діяльності Банку та законодавству України. Політика може переглядатися згідно з планами перегляду Системи інформаційної безпеки Банку, але не рідше ніж один раз на рік або в неплановому порядку у разі істотних змін в управлінській та організаційній структурі Банку.

Якщо за результатами перегляду зміни до Політики інформаційної безпеки не вносяться, то повторне її затвердження не потрібно.

11.3. Перегляд та оновлення (актуалізація) Політики здійснюється Відділом інформаційної безпеки (власник процесу) сумісно з управлінням інформаційних технологій.

Постійний контроль впровадження, виконання, вдосконалення та підтримки Політики в актуальному стані покладається на CISO Банку.

11.4. Погодження та перегляд політики інформаційної безпеки покладається на керівний орган СУІБ

11.5. У разі внесення змін до Політики, вона викладається у новій редакції та їй присвоюється відповідний номер згідно прийнятої системи маркування у структурі документів СУІБ (додаток 2 до Політики управління інформаційною безпекою АТ «МОТОР-БАНК»), який повинен бути відображеним в інших внутрішніх документах Банку з питань інформаційної безпеки, у разі посилань на неї.

У разі затвердження нової редакції цієї Політики новий номер Політики вноситься в інші внутрішні документи Банку з питань інформаційної безпеки, в яких є посилання на цю Політику, під час їх актуалізації.

11.6. У разі зміни вимог нормативно-правових актів стосовно політики Банку ця Політика чинна в частині вимог, що не суперечать новим вимогам.

11.7. Питання, які не врегульовані цією Політикою, регулюються іншими нормативно-правовими актами України, іншими внутрішніми документами Банку (у т.ч. рішеннями Наглядової Ради та Правління, наказами/розпорядженнями Голови Правління Банку та службовим листуванням).

11.8. У разі невідповідності будь-якої частини цієї Політики чинному законодавству України або нормативним актам Національного банку, у тому числі у зв’язку з прийняттям нових актів законодавства України або нових нормативних актів Національного банку, ця Політика буде діяти лише в тій частині, яка не суперечитиме чинному законодавству України та/або нормативним актам Національного банку.

Виконуючий обов’язки начальника
Відділу інформаційної безпеки
АТ «МОТОР-БАНК» Володимир АНТОНЕНКО

Політика погоджена рішенням Комісії з питань інформаційної безпеки згідно протоколу від 04 жовтня 2022 № 3-2022