АКЦІОНЕРНЕ ТОВАРИСТВО
«АКЦІОНЕРНИЙ БАНК «РАДАБАНК»

«ЗАТВЕРДЖЕНО»
Рішенням Правління АТ «АБ «РАДАБАНК»
Протокол від 15.09.2020 р. №15092020/1

Голова Правління

_____ А.В. Грігель

«ПОГОДЖЕНО»
Рішенням Ради з питань впровадження та функціонування СУІБ АТ «АБ «РАДАБАНК»
Протокол від 10.09.2020 р. №01/10092020

Голова Ради з питань впровадження та функціонування СУІБ АТ «АБ «РАДАБАНК»

_____ А.В. Грігель

ПОЛІТИКА

інформаційної безпеки
АТ «АБ «РАДАБАНК»

м. Дніпро
2020 р.

1. Загальні положення

1.1. Політика інформаційної безпеки АТ «АБ «РАДАБАНК» – це внутрішній нормативний документ, що декларує позицію АКЦІОНЕРНОГО ТОВАРИСТВА «АКЦІОНЕРНИЙ БАНК «РАДАБАНК» щодо інформаційної безпеки та кіберзахисту.

1.2. Політика розроблена відповідно до вимог Постанови Правління Національного банку України від 28.09.2017 №95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» та інших нормативно-правових актів Національного банку України щодо інформаційної безпеки та кібербезпеки у банках України, національних стандартів України з питань інформаційної безпеки ДСТУ ISO/IEC 27000:2017 «Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Огляд і словник термінів» (далі – ДСТУ ISO/IEC 27000:2017), ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги» (далі – ДСТУ ISO/IEC 27001:2015), ДСТУ ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки» (далі – ДСТУ ISO/IEC 27002:2015) та інших внутрішніх нормативних документів Банку.

1.3. Політика погоджується Радою з питань впровадження та функціонування системи управління інформаційною безпекою АТ «АБ «РАДАБАНК», затверджується рішенням Правління Банку та вводиться в дію наказом Голови Правління Банку.

1.4. Політика забезпечує підтримку стратегії розвитку інформаційної безпеки, яка узгоджується з основними стратегічними цілями Банку, що пов’язані із впровадженням нових бізнес-процесів/банківських продуктів з використанням технологій, які потребують захисту інформації, а також враховує планування розвитку інфраструктури Банку та заходів інформаційної безпеки для мінімізації ризиків інформаційної безпеки.

1.5. Політика доводиться до відома усіх працівників Банку та, за необхідністю, третіх сторін та контрагентів, та є обов’язковою для безумовного її виконання.

1.6. Для забезпечення реалізації цілей, принципів та вимог цієї Політики Банком розробляються та впроваджуються внутрішні нормативні документи , які поділяються на:

- документи вищого рівня – політики, які визначають та встановлюють вимоги інформаційної безпеки за окремими напрямками (питаннями);
- документи середнього рівня – положення та керівництва, які описують стан реалізації заходів безпеки інформації за відповідними напрямками або тематикою;
- документи нижнього рівня – інструкції, порядки, процедури, переліки, які описують та регламентують послідовність чи технологію виконання дій, опис пов’язаних об’єктів тощо у межах окремого процесу.

1.7. Внутрішні нормативні документи Банку розробляються з урахуванням вимог цієї Політики та не повинні суперечити нормативно-правовим актам України та іншим внутрішнім нормативним документам Банку.

1.8. У випадку суттєвих змін діючого законодавства, внутрішніх документів Банку в частині питань, що регламентуються цією Політикою, Банк здійснює свою діяльність у відповідності до вимог діючого законодавства та внутрішніх документів Банку, які застосовуються в частині, що не суперечить чинному законодавству.

1.9. У разі необхідності Політика переглядається із метою поліпшення ефективності банківських процесів та удосконалення системи внутрішнього контролю.

1.10. Відповідальність за внесення змін в Політику покладається на відділ інформаційної безпеки. Запропоновані зміни проходять процедуру узгодження, встановлену внутрішніми нормативними документами, погодження Радою з питань впровадження та

функціонування системи управління інформаційною безпекою АТ «АБ «РАДАБАНК», затвердження Правлінням Банку та введення в дію наказом по Банку.

1.11. Політика є обов'язковою для виконання всіма структурними підрозділами та співробітниками Банку, які беруть участь у цьому процесі. За порушення вимог Політики співробітники Банку несуть дисциплінарну відповідальність.

1.12. У разі зміни назв структурних підрозділів, які задіяні в процедурах, що описані в Політиці, при незмінності функцій, Політика вважається дійсною щодо їх нової назви.

1.13. Надання Політики третім особам відбувається у відповідності до внутрішніх процедур Банку.

2. Терміни та скорочення

В Політиці використовуються наступні терміни та визначення:

Банк – АКЦІОНЕРНЕ ТОВАРИСТВО «АКЦІОНЕРНИЙ БАНК «РАДАБАНК».

НБУ – Національний Банк України.

Політика – Політика інформаційної безпеки АТ «АБ «РАДАБАНК».

Рада СУІБ – Рада з питань впровадження та функціонування системи управління інформаційною безпекою АТ «АБ «РАДАБАНК».

СУІБ – Система управління інформаційною безпекою.

Інші терміни**,** що вживаються в цій Політиці, застосовуються в значеннях, визначених законами України, нормативно-правовими актами Національного банку України та ДСТУ ISO/IEC 27000:2017.

3. Ціль документа

Основною ціллю цієї Політики є визначення цілей, принципів та вимог щодо забезпечення належного рівня безпеки інформації та кіберзахисту, якими керується Банку при здійсненні своєї діяльності.

4. Сфера застосування

Політика інформаційної безпеки поширюється на всі підрозділи організаційної структури Банку у цілому. Дотримання Політики є обов'язковою умовою функціонування всіх процесів діяльності Банку, є обов'язковою для виконання працівниками Банку і враховується при відносинах з третіми сторонами - діловими партнерами, клієнтами Банку, контрагентами, постачальниками обладнання, матеріалів, послуг, провайдерами каналів зв'язку, уповноваженими органами, тощо.

5. Предмет документа та опис дій

5.1. Інформація та її безпека.

5.1.1. Інформація, що створюється, обробляється та використовується в Банку, є одним з цінних ресурсів, що забезпечує конкурентну перевагу Банку на ринку банківських послуг і тому потребує відповідного захисту від актуальних та потенційних загроз та вразливостей.

5.1.2. Основоположна мета інформаційної безпеки – це захист інформації та засобів оброблення інформації від несанкціонованого доступу, використання, розкриття, модифікації або знищення з метою забезпечення конфіденційності, цілісності та доступності.

5.1.3. Банк забезпечує належний рівень безпеки інформації за рахунок розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення СУІБ.

5.1.4. СУІБ Банку складається з організаційних структур, політик, процедур, настанов, відповідного набору заходів безпеки, пов'язаних процесів та ресурсів, якими колективно управляє Банк, для захисту своїх інформаційних ресурсів та досягнення бізнес-цілей.

5.1.5. СУІБ Банку застосовує ризик-орієнтований підхід до забезпечення інформаційної безпеки, який ґрунтується на розподілі обов'язків між підрозділами Банку із застосуванням моделі трьох ліній захисту:

- перша лінія - на рівні бізнес-підрозділів Банку та підрозділів інформаційних технологій та інформаційної безпеки. Ці підрозділи приймають ризики інформаційної безпеки та несуть відповідальність за них;
- друга лінія - на рівні підрозділу з управління ризиками та підрозділу контролю за дотриманням норм (комплаєнс);
- третя лінія - на рівні підрозділу внутрішнього аудиту щодо перевірки СУІБ для забезпечення того, що інформація чи СУІБ відповідає ідентифікованим вимогам та ефективно впроваджена і підтримується.

5.2. Принципи та вимоги інформаційної безпеки.

5.2.1. Постійний розвиток, вдосконалення та відповідність СУІБ сучасним загрозам, регуляторним та бізнес-вимогам, новітнім інформаційним технологіям забезпечується шляхом дотримання наступних принципів та вимог інформаційної безпеки:

- системного та комплексного підходу до забезпечення безпеки інформації;
- безперервного процесу удосконалення та розвитку інформаційної безпеки шляхом обґрунтування та реалізації раціональних засобів, методів, заходів із застосуванням найкращого міжнародного досвіду;
- своєчасних та адекватних заходів захисту від реальних та потенційних загроз і вразливостей інформаційній безпеці Банку;
- підтримці та контролю з боку керівництва Банку належного рівня інформаційної безпеки Банку;
- забезпечення достатніми ресурсами, у тому числі фінансовими, для сталого розвитку систем інформаційної безпеки;
- своєчасного моніторингу стану впровадження та ефективності функціонування СУІБ Банку з подальшою оцінкою можливостей вдосконалення та потреби проведення коригувальних дій.

5.3. Цілі та завдання СУІБ Банку.

5.3.1. Основними цілями та завданнями СУІБ Банку є:

- захист інформаційних ресурсів Банку та його клієнтів від випадкового або навмисного знищення, викривлення, розповсюдження або втрати інформації;
- забезпечення неперервності бізнесу та мінімізації можливих збитків Банку шляхом попередження можливих інцидентів інформаційної безпеки;
- нейтралізація та усунення наслідків від можливих реалізованих загроз;
- забезпечення відповідності системи захисту інформації бізнес-цілям Банку;
- підготовка та впровадження правил щодо захисту інформації та постійне підвищення обізнаності/ навчання персоналу Банку для підтримки належного рівня інформаційної безпеки;
- забезпечення відповідності СУІБ вимогам чинного законодавства України, нормативно-правовим актам Національного банку України та національних стандартів України з питань інформаційної безпеки.

5.3.2. Мінімальною сферою застосування СУІБ є всі критичні бізнес-процеси Банку щодо інформаційної безпеки. Банк може розширити сферу застосування СУІБ відповідно до особливостей своєї діяльності, характеру та обсягу банківських, фінансових послуг та інших видів діяльності Банку.

5.4. Плани щодо зменшення ризиків інформаційної безпеки.

5.4.1. Процес обробки ризиків інформаційної безпеки є інтегрований до комплексної системи управління ризиками Банку. Оцінка та обробка ризиків інформаційної безпеки здійснюється у відповідності у до вимог діючого законодавства, нормативно-правових актів Національного Банку України, внутрішніх нормативних документів Банку, з урахуванням принципів і рекомендацій Базельського комітету з банківського нагляду щодо корпоративного управління та управління ризиками в банках і банківських групах, та згідно рекомендацій міжнародних стандартів щодо забезпечення безперервності ISO 22301, ISO 22313, ISO 27031 та ISO 27005.

5.4.2. Обробка та фіксування подій інформаційного ризику здійснюється відповідно внутрішніх нормативних документів Банку щодо управління інформаційним та операційним ризиками.

5.5. Перегляд політики інформаційної безпеки.

5.5.1. Політика переглядається за появи істотних змін з метою забезпечення її постійної придатності, адекватності та ефективності. Зокрема перегляд охоплює оцінку можливостей вдосконалення Політики в разі змін інфраструктури Банку, бізнес-обставин, правових умов або технічної інфраструктури.

5.5.2. Перегляд Політики з боку керівництва Банку здійснюється на основі отриманої інформації, а саме:

- продуктивності критичних бізнес-процесів та відповідності Політиці інформаційної безпеки;
- тенденцій загроз та вразливостей (на основі постійного моніторингу подій та за результатами запланованої оцінки ризиків);
- зареєстрованих подій інформаційної безпеки;
- зворотнього зв‘язку від зацікавлених сторін (Ради СУІБ, власників критичних бізнес-процесів, іншої інформації);
- звітів аудиторів (отриманих як за результатами внутрішнього аудиту так і за результатами незалежних переглядів - зовнішній аудит);
- звітів за результатами проведення стрес-тестування інформаційних систем Банку;
- результатів попередніх переглядів з боку керівництва Банку;
- рекомендацій наданих відповідними повноваженими організаціями (рекомендації та нормативні документи НБУ, інших повноважних організацій - стосовно пожежної безпеки, будівельних чи санітарних норм, тощо).

5.5.3. За результатами перегляду Політики, керівництво Банку приймає управлінські рішення стосовно вдосконалення підходу до управління інформаційною безпекою, вдосконалення заходів безпеки інформації, вдосконалення розподілу ресурсів та/або обов‘язків.

5.5.4. Переглянута Політика обов‘язково затверджується керівництвом Банку.

6. Ролі та відповідальності

6.1. Для забезпечення реалізації цілей, принципів та вимог цієї Політики та ефективного функціювання СУІБ у Банку здійснюється наступний розподіл функцій (ролей) і відповідальності за забезпечення інформаційної безпеки:

6.1.1. Керівництво Банку (Голова та члени Наглядової Ради, Голова та члени Правління Банку) сприяє створенню, впровадженню, контролю та підтримці Стратегії та Політики інформаційної безпеки, а також приймає управлінські рішення для реалізації необхідних заходів з питань забезпечення безпеки інформації.

6.1.2. У Банку створений та постійно діє колективний керівний орган з питань впровадження та функціювання СУІБ – Рада з питань впровадження та функціонування

системи управління інформаційною безпекою АТ «АБ «РАДАБАНК», рішення якого є обов'язковими для виконання усіма працівниками Банку.

6.1.3. До складу Ради СУІБ входять Голова Правління Банку, що відповідає за інформаційну безпеку Банку (CISO), керівник підрозділу з інформаційної безпеки, керівник підрозділу з управління ризиками, керівники підрозділів Банку – власники критичних бізнес-процесів Банку, керівники підрозділів Банку – власники критичних ресурсів Банку тощо.

6.1.4. Рада СУІБ забезпечує та несе відповідальність за:

- погодження та перегляд Політики, стратегії розвитку інформаційної безпеки та інших внутрішніх нормативних документів Банку з питань інформаційної безпеки;
- узгодження впровадження нових проектів, напрямів, стратегічних завдань та заходів з питань інформаційної безпеки;
- визначення необхідних оптимальних ресурсів для впровадження заходів інформаційної безпеки;
- організація практичних заходів щодо підвищення обізнаності/навчання персоналу Банку та представників третіх сторін з питань інформаційної безпеки;
- забезпечення своєчасного моніторингу стану впровадження та ефективності функціонування СУІБ з подальшою оцінкою можливостей вдосконалення та потреби проведення коригувальних дій.

6.1.5. У Банку призначено відповідальну особу за інформаційну безпеку (Chief information security officer, CISO), яка має повноваження для прийняття управлінських рішень. Відповідальна особа за інформаційну безпеку забезпечує та несе відповідальність за:

- стратегічне керівництво з питань інформаційної безпеки;
- визначення напрямів розвитку інформаційної безпеки, їх відповідність стратегії розвитку Банку;
- відповідність методів та засобів забезпечення безпеки інформації потребам бізнес-процесів / банківських продуктів;
- контроль за впровадженням та реалізацією заходів забезпечення безпеки інформації у Банку.

6.1.6. З метою оперативного контролю за виконанням заходів щодо забезпечення безпеки інформації на всіх стадіях її життєвого циклу, у Банку сформований підрозділ з інформаційної безпеки зі складу штатних працівників Банку. Підрозділ з інформаційної безпеки безпосередньо підпорядковується відповідальній особі за інформаційну безпеку Банку.

6.1.7. Підрозділ інформаційної безпеки забезпечує та несе відповідальність за:

- ознайомлення з цією Політикою та дотримання її вимог;
- виконання вимог нормативно-правових актів України та внутрішніх нормативних документів Банку з питань інформаційної безпеки;
- розроблення вимог щодо методів та засобів забезпечення безпеки інформації;
- розроблення або участь у розробленні внутрішніх нормативних документів Банку щодо застосування методів та засобів забезпечення безпеки інформації;
- контроль за застосування засобів забезпечення безпеки інформації на всіх стадіях її життєвого циклу у Банку, та вимог цієї Політики;
- розслідування інцидентів безпеки інформації;
- спільно з підрозділом інформаційних технологій Банку відновлення функціонування інформаційних систем Банку після збоїв у роботі внаслідок інцидентів безпеки інформації.

6.1.8. Підрозділ інформаційних технологій забезпечує та несе відповідальність за:

- розроблення або участь у розробленні внутрішніх нормативних документів Банку щодо застосування безпечних методів та засобів оброблення інформації;
- безпечну розробку, тестування та впровадження нових інформаційних систем Банку та їх складових;

- належну експлуатацію, технічне обслуговування та підтримку інформаційних систем Банку та їх складових;
- своєчасне оновлення налаштувань безпеки інформаційних систем Банку та їх складових;
- безперервне функціонування інформаційних систем Банку та їх складових, встановлених елементів захисту інформації;
- відновлення функціонування інформаційних систем Банку після збоїв у роботі внаслідок інцидентів безпеки інформації.

6.1.9. Працівники Банку, які отримали та використовують доступ до інформації, забезпечують та несуть відповідальність за:

- ознайомлення з цією Політикою та дотриманням її вимог;
- ознайомлення та виконання вимог нормативно-правових актів України та внутрішніх нормативних документів Банку з питань інформаційної безпеки;
- виконання правил використання та зберігання інформації;
- дотримання технології оброблення та безпеки інформації;
- участь у впровадженні нових, модернізації/відновленні функціонування діючих методів та засобів використання та безпеки інформації;
- інформування про події (інциденти), пов'язані з використанням та зберіганням інформації.

6.1.10. Треті сторони, які отримали та використовують доступ до інформації під час взаємодії з Банком, забезпечують та несуть відповідальність за:

- ознайомлення з цією Політикою та дотриманням її вимог;
- виконання правил використання та зберігання інформації;
- дотримання технології оброблення та безпеки інформації;
- інформування про події (інциденти), пов'язані з використанням та зберіганням інформації;
- на вимогу Банку надавати відомості про порядок використання та зберігання інформації.

6.2. Наслідки недотримання цієї Політики, зловмисні дії або невідповідне поводження з інформацією та ресурсами інформаційної мережі Банку, тягнуть за собою:

- ініціювання застосування відповідних заходів впливу до порушників, згідно внутрішніх нормативних документів Банку;
- адміністративну або іншу відповідальність, передбачену чинним законодавством України.

7. Перегляд документу

Банк забезпечує підтримку Політики в актуальному стані та її перегляд не рідше ніж один раз на рік. Причинами внесення змін до Політики є зміни у Стратегії Банку, інформаційній інфраструктурі та/або впровадженні нових інформаційних технологій, зміни правових умов, виникнення нетипових інцидентів безпеки, а також зміни в нормативно-правових актах України в сфері інформаційної безпеки.

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