ЗАТВЕРДЖЕНО
Протокол Наглядової Ради
АБ «УКРГАЗБАНК»
від «01» жовтня 2019 року №18
Голова Наглядової Ради
_____ Давда Ш.Д.

ПОГОДЖЕНО
Протокол Правління
АБ «УКРГАЗБАНК»
від «12» вересня 2019 року №41
Голова Правління Шевченко К.Є.
_____

ПОГОДЖЕНО
Протокол Комітету з питань
управління інформаційною
безпекою АБ «УКРГАЗБАНК»
від «23» липня 2019 року №8
Голова Комітету
_____ Савощенко Т.Ю.

ПОЛІТИКА інформаційної безпеки АБ «УКРГАЗБАНК»

Київ - 2019

Зміст

Розділ І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Політика інформаційної безпеки АБ «УКРГАЗБАНК» (далі - Політика) розроблена відповідно до Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затвердженого постановою Правління Національного банку України від 28.09.2017 №95 (далі – Положення); національних стандартів України з питань інформаційної безпеки ДСТУ ISO/IES 27000:2015 «Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник», ДСТУ ISO/IES 27001:2015 «Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги.», ДСТУ ISO/IES 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки» (далі – державні стандарти); та з урахуванням міжнародних стандартів з питань інформаційної безпеки, загальноприйнятих у міжнародній практиці принципів забезпечення інформаційної безпеки і кіберзахисту, вимог актів внутрішнього регулювання АБ «УКРГАЗБАНК» (далі - Банк).

1.2. Ця Політика описує прийняту та впроваджену Банком політику щодо інформаційної безпеки.

1.3. Перелік взаємопов’язаних документів:

- Положення про управління інформаційною безпекою в АБ «УКРГАЗБАНК»;
- Положення про інформацію з обмеженим доступом АБ «УКРГАЗБАНК»;
- Положення щодо захисту персональних даних у АБ «УКРГАЗБАНК»;
- Перелік вимог з інформаційної безпеки АБ «УКРГАЗБАНК»;
- Правила управління інцидентами інформаційної безпеки в АБ «УКРГАЗБАНК».

Розділ ІІ. ВИЗНАЧЕННЯ ТЕРМІНІВ

Керівництво Банку (керівництво) (в межах цієї Політики) – Голова та Члени Правління Банку, Голова та Члени Наглядової Ради.

Бізнес-процес – це систематичне і послідовне виконання певних операцій (функцій), направлених на одержання конкретного результату (продукту).

Загроза (threat) – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків автоматизованій системі.

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

Інформація з обмеженим доступом – відомості, що становлять банківську таємницю, комерційну таємницю, персональні дані та службову інформацію.

Клієнт (Клієнт Банку) – будь-яка фізична особа чи суб’єкт господарювання (в т.ч. банківська установа), що користується послугами банку.

Критичний бізнес-процес – бізнес-процес, який обробляє інформацію з обмеженим доступом, розголошення якої може нанести шкоду Банку.

Несанкціонована особа, об'єкт або процес – особа, об’єкт або процес, які не контролюються Банком та/або не задовольняють вимоги, які до них висуваються.

Ресурси СУІБ (asset) – все, що має цінність для Банку.

Санкціонований об'єкт – об’єкт, який контролюється Банком та/або задовольняє вимоги, які до нього висуваються.

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

Розділ ІІІ. ЦІЛЬ ДОКУМЕНТА ТА СФЕРА ЙОГО ЗАСТОСУВАННЯ

3.1. Ціллю цієї Політики є впровадження та ефективне функціонування системи управління інформаційною безпекою та кіберзахисту, яка буде забезпечувати безпечність та надійність функціонування бізнес-процесів, захист інформації та ресурсів Банку від зовнішніх та внутрішніх загроз та загроз, які 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.

3.2. Дія цієї Політики поширюється на весь Банк в цілому та представників (користувачів) третіх сторін. Всі працівники Банку, представники (користувачі) третіх сторін, незалежно від рівнів доступу до інформації та ресурсів Банку, мають дотримуватись вимог цієї Політики.

3.3. Ця Політика використовується для усіх критичних бізнес-процесів/банківських продуктів/програмно-технічних комплексів Банку.

3.4. Банк керується ризик-орієнтованим підходом, який забезпечує розуміння, моніторинг та зменшення ризиків операційної діяльності включаючи інформаційні ризики.

3.5. Банк контролює дотримання вимог цієї Політики при наданні послуг третіми особами, які в процесі надання таких послуг одержують доступ до інформаційних ресурсів Банку. Представники (користувачі) третіх сторін мають негайно повідомляти Банк про події порушення інформаційної безпеки Банку та/або слабкі місця інформаційної безпеки Голові Правління або Заступнику Голови Правління Банку.

3.6. Банк захищає власні інформаційні ресурси фізичними, апаратними, програмними, нормативними та цивільно-правовими шляхами. Банк розмежовує інформацію з обмеженим доступом від іншої інформації.

Розділ IV. ПРЕДМЕТ ДОКУМЕНТУ ТА ОПИС ДІЙ

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

- **Цілісності** - властивість захищеності, безпомилковості та повноти ресурсів СУІБ.
- **Конфіденційності** - властивість інформації не ставати доступною та розкритою для несанкціонованих осіб, об'єктів або процесів.
- **Доступності** - властивість доступності та можливості використання ресурсів СУІБ на вимогу санкціонованого об'єкта.
- **Спостережності** - властивість системи (автоматизованої, контролю доступу, моніторингу тощо) фіксувати діяльність ідентифікованих користувачів і процесів.

4.2. Це в першу чергу стосується інформації з обмеженим доступом, перелік відомостей яких представлено в ***Положенні про інформацію з обмеженим доступом АБ «УКРГАЗБАНК»*** та в ***Правилах щодо захисту персональних даних у АБ «УКРГАЗБАНК».***

4.3. Серед основних об'єктів, на які розповсюджується дія інформаційної безпеки Банку, розглядаються наступні види ресурсів:

- **інформаційні ресурси** - інформація та дані у будь-якому вигляді, що отримуються, зберігаються, обробляються, передаються, оголошуються, у тому числі знання працівників, партнерів Банку, бази даних та файли, документація, посібники користувача, навчальні матеріали, описи процедур, архівована інформація тощо;
- **програмне забезпечення** - прикладне програмне забезпечення, системне програмне забезпечення, сервісне програмне забезпечення та будь-яке інше програмне забезпечення, незалежно від форми отримання (придбання, власної розробки, таке, що вільно розповсюджується), яке використовується у Банку працівниками та системами для роботи та взаємодії з Клієнтами та іншими внутрішніми та зовнішніми системами тощо;
- **фізичні ресурси** - працівники, апаратні засоби IT (сервери, робочі станції, міжмережеві екрани, принтери, копіювальні апарати, телекомунікаційне обладнання, обладнання зв'язку, маршрутизатори, АТС, факси, модеми тощо), носії даних (стрічки, диски тощо), меблі, приміщення, виробниче обладнання, інші технічні засоби тощо;
- **сервісні ресурси** - обчислювальні та комунікаційні сервіси (Інтернет, електронна пошта, канали зв'язку тощо), інші технічні сервіси (опалення, освітлення, енергозбереження, кондиціювання повітря, системи сигналізації та моніторингу), усі послуги, пов'язані з отриманням, наданням, використанням, передачею та знищенням ресурсів, усі юридичні та фізичні особи, організації, установи та підприємства (а також їх працівники), послугами яких користується Банк для отримання, використання, передачі та знищення ресурсів.

4.4. Для кожного ресурсу визначаються можливі ризики інформаційної безпеки, критерії їх прийняття та шляхи їх мінімізації, тобто Банк використовує ризик-орієнтований підхід, який забезпечує розуміння, моніторинг та зменшення ризиків операційної діяльності. Деталі ризик-орієнтовного підходу описані в діючій редакції ***Положення про управління інформаційною безпекою в АБ «УКРГАЗБАНК».***

4.5. Політика базується на вимогах законодавчих, регуляторних та актах внутрішнього регулювання з інформаційної безпеки.

4.6. Всі працівники Банку / представники (користувачі) третіх сторін до того, як вони приступають до виконання свої обов’язків дають Зобов’язання про зберігання банківської, комерційної таємниці, персональних даних та службової інформації / Зобов’язання про зберігання інформації з обмеженим доступом АБ «УКРГАЗБАНК», яке залишається чинним протягом всього періоду роботи в Банку/або дії договору с третіми сторонами та після звільнення/закінчення дії договору, необмежений час.

4.7. Банком використовуються наступні підходи щодо забезпечення інформаційної безпеки:

- створено та затверджено перелік відомостей, що містять інформацію з обмеженим доступом;
- створено та затверджено перелік критичних бізнес-процесів за якими проводиться оцінка ризиків інформаційної безпеки та подальша їх обробка;
- встановлено правила доступу до інформаційних ресурсів та програмно-технічних комплексів;

- забезпечується контроль фізичного та логічного доступу до всіх визначених ресурсів;
- забезпечується парольний захист програмних та сервісних ресурсів;
- забезпечується антивірусний захист програмних та сервісних ресурсів;
- забезпечується захист мережі;
- забезпечується захищений віддалений доступ до ресурсів мережі (локальної, мережі Інтернет, мереж інших організацій);
- забезпечується ідентифікація та автентифікація всіх визначених ресурсів;
- забезпечується криптографічний захист інформації;
- проводяться внутрішні аудити СУІБ та аналіз СУІБ з боку керівництва Банку;
- моніторинг та вдосконалення СУІБ.

4.8. Банк дотримується наступних правил в частині забезпечення ІБ та безперебійної діяльності:

- Працівники Банку та третіх сторін беруть участь у підтримці відповідного рівня ІБ в межах своїх обов'язків та повноважень і несуть відповідальність за його порушення в межах, встановлених чинним законодавством України та актами внутрішнього регулювання Банку.
- Під час розроблення, впровадження та функціонування програмно-технічних комплексів враховуються вимоги інформаційної безпеки (відповідно до діючої редакції ***Переліку вимог з інформаційної безпеки АБ «УКРГАЗБАНК»***).
- Публічні сервіси Банку та внутрішні мережі Банку відповідають вимогам інформаційної безпеки (відповідно до діючої редакції ***Переліку вимог з інформаційної безпеки АБ «УКРГАЗБАНК»***).
- Банк забезпечує встановлення та моніторинг виконання усіх вимог інформаційної безпеки, які наявні в угодах з третіми сторонами стосовно участі у міжнародних платіжних системах та системах переказу коштів (вимоги зацікавлених сторін).
- Стратегія розвитку інформаційних технологій Банку, всі проекти, які пов'язані з інформаційними технологіями, відповідають діючій редакції ***Положення про управління інформаційною безпекою в АБ «УКРГАЗБАНК».***
- Керівництво Банку створює працівникам Банку умови для систематичного навчання нормам та заходам інформаційної безпеки, для зменшення ризиків виникнення інцидентів ІБ.
- У банку складаються, діють, систематично тестуються та оновлюються плани на випадок різних непередбачуваних критичних ситуацій:
  - План забезпечення безперервності діяльності АБ «УКРГАЗБАНК»;
  - План відновлення функціонування інформаційних систем в АБ «УКРГАЗБАНК»;
  - Плани забезпечення безперервного функціонування критичних бізнес-процесів;
  - План забезпечення безперервного функціонування Дирекцій та відділень АБ «УКРГАЗБАНК».

4.9. Про кожний інцидент інформаційної безпеки працівники Банку зобов'язані негайно сповістити свого безпосереднього керівника та управління інформаційної безпеки департаменту банківської безпеки. Банком відповідно до діючої редакції ***Правил управління інцидентами інформаційної безпеки в АБ «УКРГАЗБАНК»*** передбачено аналіз та реакція (в тому числі на рівні комунікації) на той чи інший інцидент. За результатами аналізу вживаються заходи, направлені на недопущення повторення подібних інцидентів.

Розділ V. ВІДПОВІДАЛЬНІСТЬ

5.1. Керівництво Банку чітко розуміє, що інформаційна безпека Банку є основою життєдіяльності Банку та забезпечує (організаційно та фінансово) впровадження, підтримку та контроль належного рівня інформаційної безпеки та кіберзахисту.

5.2. Керівництво Банку активно підтримує безпеку в межах Банку шляхом чіткого регулювання, підтверджених зобов'язань, чітких призначень та визнання відповідальності за ІБ.

5.3. Кожний працівник, структурний підрозділ Банку бере участь у підтримці відповідного рівня інформаційної безпеки Банку в межах своїх обов'язків та повноважень, несе відповідальність за їх порушення в межах, встановлених чинним законодавством України, актами внутрішнього регулювання та нормативно-методичними документами Банку. Представники третіх сторін несуть відповідальність за виконання цієї Політики.

5.4. У Банку створений та постійно працює Комітет з питань управління інформаційною безпекою АБ «УКРГАЗБАНК» (далі – Комітет), рішення якого є обов'язковими для виконання усіма працівниками Банку. Керівником Комітету рішенням Правління Банку призначено Заступника Голови Правління Банку.

5.5. Документи системи управління інформаційною безпекою розробляються управлінням інформаційної безпеки департаменту банківської безпеки та іншими структурними підрозділами Банку за відповідними напрямками діяльності.

5.6. Документи системи управління інформаційною безпекою доступні працівникам Банку у межах їх повноважень і призначені надавати допомогу у виконанні вимог інформаційної безпеки.

5.7. Постійний контроль впровадження, виконання, вдосконалення та підтримки цієї Політики в актуальному стані покладається на управління інформаційної безпеки департаменту банківської безпеки.

Розділ VI. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

6.1. Ця Політика затверджується Наглядовою Радою Банку.

6.2. Зміни до цієї Політики затверджуються рішенням Наглядової Ради Банку та оформлюються окремим документом або шляхом його викладення в новій редакції. Прийняття нової редакції Політики автоматично призводить до припинення дії попереднього документа.

6.3. У разі невідповідності будь-якої частини цієї Політики чинному законодавству України, у тому числі нормативно-правовим актам Національного банку України, зокрема, у зв'язку з прийняттям нових чи внесенням змін до діючих нормативно- правових актів, ця Політика буде діяти лише в тій частині, яка не суперечитиме чинному законодавству України.