ЗАТВЕРДЖЕНО

Протокол Правління АБ «УКРГАЗБАНК»
«14» грудня 2017 р. № 81
Голова Правління
_____ Шевченко К.Є.

ПОГОДЖЕНО
Протокол Комітету з питань управління інформаційною безпекою
АБ «УКРГАЗБАНК»
«01» грудня 2017 р. № 20
Голова Комітету
_____ Савощенко Т.Ю.

ПОЛІТИКА
інформаційної безпеки
АБ «УКРГАЗБАНК»

Київ 2017

Зміст

1. Вступ

Політика інформаційної безпеки АБ «УКРГАЗБАНК» (далі - Політика) розроблена відповідно до вимог чинного законодавства України, нормативно-правових актів Національного банку України (в тому числі стандартів СОУ Н НБУ 65.1 СУІБ 1.0:2010 Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD) та СОУ Н НБУ 65.1 СУІБ 2.0:2010 Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD)), постанови Правління Національного банку України від 28.09.2017 №95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» (з дати набрання чинності), вимог 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), вимог міжнародних та внутрішньодержавних платіжних систем та систем переказу коштів, вимог актів внутрішнього регулювання АБ «УКРГАЗБАНК» (далі - Банк).

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

2. Терміни та скорочення

Керівництво Банку (керівництво) – Голова та Члени Правління Банку, Голова та Члени Наглядової Ради.

Бізнес-процес – послідовність логічно зв'язаних процедур, що має кілька входів і виходів, яка призначена для одержання заданого кінцевого результату (результатів).

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.

3. Ціль документу

Ціллю 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.

4. Сфера застосування

Дія 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.

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

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.

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

5. Предмет документу та опис дій

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.

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

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.

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 ***Політики управління інформаційною безпекою в АБ «УКРГАЗБАНК».***

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

Всі працівники Банку, представники (користувачі) третіх сторін до того, як вони приступають до виконання свої обов'язків дають зобов'язання про нерозголошення банківської таємниці, яке залишається чинним протягом всього періоду роботи в Банку/або дії договору с третіми сторонами та після звільнення/закінчення дії договору, необмежений час.

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.

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 ***Політики 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 безперервності діяльності, та дій на випадок надзвичайних ситуацій;
    - план відновлення працездатності інформаційних систем у разі виникнення надзвичайних ситуацій в автоматизованих системах;
    - план забезпечення безперервності функціонування заходів інформаційної безпеки.

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 ***Процедури 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.

6. Ролі та відповідальності

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.

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

Кожний працівник, 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 та актами внутрішнього регулювання. Представники третіх сторін несуть відповідальність за виконання цієї Політики.

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.

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

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

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

7. Перегляд документу

Політика підтримується в актуальному стані та переглядається один раз на рік та/або за необхідності та набуває чинності з моменту її затвердження Правлінням Банку.

Причинами внесення змін до Політики є зміни в законодавчих, регуляторних та інших нормах, а також зміни в інфраструктурі Банку та/або впровадження нових інформаційних технологій.

8. Перелік взаємопов’язаних документів

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

9. Лист погодження

Посада	**Прізвище**	**Особистий підпис**	**Дата**
Заступник директора департаменту банківської безпеки	Медведський В.І.		
Заступник директора департаменту банківської безпеки	Машошин О.В.		
Директор департаменту інформаційних технологій	Романов М.П.		
Заступник директора департаменту інформаційних технологій	Бережний О.А.		
Директор департаменту роздрібного банкінгу	Мороз Ю.А.		
Заступник головного бухгалтера	Сліпченко Б.І.		
Директор департаменту ризик-менеджменту	Пономарьов В.М.		
Заступник директора департаменту карткових продуктів та альтернативних каналів продажів	Широчин С.В.		
Начальник управління інформаційної безпеки департаменту банківської безпеки	Недзельський С.О.		
Начальник управління комплаєнсу та методології	Приходько Б.А.		
Директор юридичного департаменту	Пришко І.А.		

10. Історія змін

Дата	Автор	Зміст змін