АТ «Ощадбанк»

ЗАТВЕРДЖЕНО

Постановою правління АТ „Ощадбанк”
від 07 жовтня 2015р. №905
зі змінами внесеними рішенням комітету СУІБ
від 28.03.2019 р. протокол № 3

зі змінами, внесеними постановою правління АТ «Ощадбанк» від 19.07.2019 № 485

ПОЛІТИКА

ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В АТ «ОЩАДБАНК»

Київ – 2019

ЗМІСТ

1. ВСТУП

Політика інформаційної безпеки (далі – Політика) є внутрішнім нормативно-правовим документом Банку, який формулює та висловлює позицію керівництва в АТ «Ощадбанк» (далі – Банк) щодо інформаційної безпеки, а також визначає основні принципи та завдання забезпечення інформаційної безпеки в Банку.

2. ТЕРМІНИ ТА СКОРОЧЕННЯ

Терміни та скорочення в Політиці визначаються згідно з чинним законодавством України та за прийнятою внутрішньобанківською термінологією.

3. ЦІЛЬ ДОКУМЕНТА

Мета Політики - визначення базових засад та принципів забезпечення інформаційної безпеки Банку.

Основними завданнями забезпечення інформаційної безпеки Банку є:

- захист інформаційних активів Банку від зовнішніх та внутрішніх навмисних та ненавмисних загроз;
- впровадження та забезпечення ефективного функціонування системи управління інформаційною безпекою;
- попередження, виявлення і усунення загроз безпеки Банку, причин та умов, які призводять до матеріальних втрат;
- забезпечення безперервної та надійної роботи інформаційних систем Банку;
- створення умов для зменшення негативного впливу наслідків порушення вимог інформаційної безпеки Банку;
- управління інформаційною безпекою на основі ризик-орієнтованого підходу, ідентифікація та оцінювання ризиків;
- координація діяльності всіх працівників Банку, визначення ролей та обов’язків щодо управління та забезпечення інформаційної безпеки Банку;
- навчання та підвищення обізнаності працівників Банку у сфері інформаційної безпеки.

Політика є основою для захисту інформаційних ресурсів Банку з метою забезпечення їх конфіденційності, цілісності, доступності та спостережності.

4. СФЕРА ЗАСТОСУВАННЯ

Дія Політики поширюється на всі аспекти та процеси операційної діяльності Банку, інформаційні ресурси та автоматизовані системи Банку.

Вимоги, встановлені в цьому документі, є загальними та призначені для застосування:

- працівниками Банку;

- користувачами інформаційних ресурсів Банку;
- у взаємовідносинах з клієнтами, партнерами, постачальниками та іншими контрагентами Банку.

Політика є основою для розробки нормативно-правових актів Банку в частині інформаційної безпеки. Будь-які внутрішні нормативно-правові акти Банку не можуть суперечити вимогам Політики.

5. РОЛІ ТА ВІДПОВІДАЛЬНОСТІ

Керівництво Банку розуміє важливість інформаційної безпеки Банку та розглядає її як обов'язковий механізм унеможливлення несанкціонованого доступу до інформаційних активів. У зв'язку з цим у Банку створений та постійно діє Комітет СУІБ з питань впровадження, забезпечення та контролю системи управління інформаційної безпеки.

Керівництво Банку сприяє створенню, впровадженню, вдосконаленню, контролю та підтримці цілей та принципів інформаційної безпеки, зазначених в цій Політиці, згідно з бізнес-стратегією та цілями Банку.

Крім цієї політики інформаційної безпеки СУІБ також має включати інші документи, більш детальні політики та процедури або правила безпеки, які користувачі повинні знати та виконувати, як складову частину політики інформаційної безпеки.

Для забезпечення прийнятного рівня інформаційної безпеки в Банку впроваджуються заходи та засоби безпеки, цілі яких ґрунтуються на результатах оцінки ризиків та формуються в процесі управління ризиками. Процес управління ризиками ІБ у складі СУІБ є невід'ємною частиною загальної банківської політики управління ризиками і ґрунтується на системі класифікації інформаційних активів, прийнятій у Банку.

Головною метою процесу управління ризиками ІБ є забезпечення адекватного захисту інформаційних активів Банку від можливих загроз, як навмисних, так і випадкових. Застосовуваний рівень безпеки для протидії потенційним загрозам ґрунтується на принципах ефективності та економічної доцільності, та рівні прийнятного ризику, що визначається керівництвом Банку.

Для забезпечення ефективного управління інформаційною безпекою Банку необхідна активна підтримка і безперервна участь працівників всіх підрозділів на всіх рівнях управління. Кожен підрозділ у межах компетенції несе відповідальність за виконання вимог нормативно-правових актів Банку з інформаційної безпеки як частини своїх службових завдань. У межах своїх обов'язків та повноважень працівники зобов'язані виконувати та відповідати за дотримання вимог Політики, законодавчих та міжнародних норм, внутрішньобанківських вимог та вимог договорів, укладених Банком, а також несуть

відповідальність за їх порушення в межах, встановлених законодавством України та внутрішньобанківськими нормативно-правовими актами.

З метою забезпечення ефективності та підтримки інформаційної безпеки Банку керівництво Банку забезпечує систематичне навчання кожного працівника Банку. Навчання охоплює інформацію щодо правил та процедур забезпечення безпеки, відомих загроз, належних каналів звітування щодо інцидентів інформаційної безпеки, коректного та безпечного використання засобів оброблення інформації тощо.

У рамках системи управління інформаційною безпекою в Банку учасниками інформаційної безпеки є:

Керівництво Банку (голова правління або його заступник, який відповідає за інформаційну безпеку):

- визначає принципи і завдання інформаційної безпеки;
- визначає рівень прийнятного ризику інформаційної безпеки та здійснює формалізоване, об’єктивне та інформоване прийняття залишкових ризиків;
- організовує періодичний перегляд заходів інформаційної безпеки, враховуючи результати аудитів безпеки, інциденти, результати вимірювань ефективності, пропозиції і зворотній зв'язок з усіма зацікавленими сторонами, а також забезпечує вжиття коригувальних та запобіжних заходів за результатами переглядів;
- забезпечує необхідні та достатні ресурси (включаючи персонал та фінансування) для управління інформаційною безпекою та відповідності правовим та нормативним вимогам;
- затверджує нормативні документи Банку з питань інформаційної безпеки;
- сприяє розслідуванню інцидентів інформаційної безпеки.

Комітет СУІБ:

Діяльність комітету СУІБ регламентується Положенням про комітет СУІБ.

Адміністратор інформаційного ресурс/системи – відповідальний працівник служби інформатизації, який згідно наказу керівника установи:

- забезпечує експлуатацію та технічне обслуговування інформаційного ресурсу/системи;
- забезпечує проведення заходів з модернізації, тестування, оперативного відновлення функціонування інформаційного ресурсу/системи після збоїв, відмов, аварій окремих його компонентів;

- забезпечує резервування технічних засобів, програмного забезпечення інформаційного ресурсу, а також встановлює та налагоджує програмне забезпечення підсистеми резервного копіювання;
- бере участь у впровадженні та забезпечує безперервне функціонування засобів захисту інформації на інформаційному ресурсі/системі;
- своєчасно повідомляє керівництво Банку про факти виявлення несправностей в роботі апаратного та програмного забезпечення інформаційного ресурсу/системи;
- виконує налаштування реєстрації подій безпеки на інформаційному ресурсі/системи, регулярний перегляд та моніторинг відповідних журналів подій;
- бере участь у процедурі надання, зміни або скасування прав доступу користувачів до інформаційного ресурсу;
- забезпечує технічну підтримку користувачів інформаційного ресурсу по каналах зв'язку;
- бере участь у розслідуванні інцидентів інформаційної безпеки у складі групи реагування на інциденти інформаційної безпеки.

Адміністратор захисту інформації – відповідальний працівник служби захисту електронної інформації, який згідно з наказом керівника установи:

- забезпечує поточний контроль за станом захисту інформації;
- бере участь у процедурі надання, зміни або скасування прав доступу користувачів до інформаційного ресурсу;
- здійснює періодичний аналіз вразливостей інформаційних систем;
- узгоджує, контролює надання та періодично переглядає права доступу користувачів інформаційних ресурсів/систем;
- бере участь у процесі обробки інцидентів інформаційної безпеки у складі групи реагування на інциденти інформаційної безпеки;
- супроводжує засоби захисту інформації в підпорядкованих бізнес процесах.

Керівники філій та територіально відокремлених безбалансових відділень Банку:

- у рамках своїх повноважень організують процеси СУІБ у підпорядкованих підрозділах;
- контролюють виконання політики інформаційної безпеки та інших вимог СУІБ працівниками підпорядкованих підрозділів;
- узгоджують права доступу до інформаційних систем працівників підпорядкованих підрозділів.

Власники інформаційних активів (керівник профільного підрозділу центрального апарату, регіонального управління, територіально відокремленого безбалансового відділення Банку, який є головним користувачем інформаційного активу та погоджує проведення дії з аналізу захищеності інформаційного активу):

- беруть участь у класифікації інформаційних активів;
- беруть участь у процесі оцінки ризиків інформаційної безпеки;
- узгоджують права доступу користувачів інформаційних активів;
- несуть відповідальність за забезпечення захисту інформації в інформаційних активах.

За одним інформаційним активом може бути закріплено декілька власників.

Керівники самостійних структурних підрозділів:

- організовують роботу із забезпечення політики інформаційної безпеки;
- своєчасно доповідають службі захисту електронної інформації про інциденти інформаційної безпеки та виявлені порушення вимог політики безпеки Банку;
- контролюють дотримання вимог діючої в Банку політики інформаційної безпеки, вимог СУІБ та інших нормативно-правових актів працівниками підпорядкованого підрозділу.

Усі працівники Банку та користувачі інформаційних активів Банку:

- мають знати та виконувати вимоги нормативно-правових актів щодо інформаційної безпеки;
- повинні сприяти попередженню, виявленню та розслідуванню інцидентів інформаційної безпеки;
- повинні вживати всіх можливих заходів безпеки з метою запобігання чи зменшення втрат і збитків.

Партнери, постачальники, інші контрагенти:

- мають виконувати договірні вимоги та вимоги нормативно-правових актів Банку щодо інформаційної безпеки;
- відповідають за попередження та виявлення, а також повинні сприяти розслідуванню інцидентів інформаційної безпеки, які виникають під час виконання договорів з Банком.

Управління окремими процесами СУІБ, впровадження та експлуатації засобів захисту, виконання заходів безпеки в Банку забезпечують відповідні служби:

Служба банківської безпеки (департамент банківської безпеки, підрозділи банківської безпеки регіональних управлінь, відповідальні працівники банківської безпеки територіально відокремлених безбалансових відділень Банку) забезпечує:

- захист від загроз фізичного середовища,
- контроль персоналу,
- захист фізичних складових інформаційних ресурсів.

Служба захисту електронної інформації (управління захисту інформації, підрозділи захисту інформації регіональних управлінь, відповідальні працівники захисту інформації територіально відокремлених безбалансових відділень Банку):

- визначає та впроваджує в Банку єдину політику технічного захисту інформації та криптографічного захисту інформації в інформаційних активах Банку;
- відповідає за впровадження та підтримку засобів захисту ресурсів СУІБ;
- забезпечує впровадження та експлуатацію систем керування ключовими даними Банку;
- виконує методологічне забезпечення питань інформаційної безпеки в інформаційних активах Банку;
- виконує нагляд за дотриманням вимог СУІБ в установах Банку.

Служба інформатизації (департамент інформатизації, підрозділи інформатизації регіональних управлінь, відповідальні працівники інформатизації територіально відокремлених безбалансових відділень Банку):

- забезпечує експлуатацію та технічне обслуговування інформаційних активів;
- виконує встановлення оновлень безпеки для інформаційних активів;
- забезпечує безперервне функціонування інформаційних активів та елементів захисту інформації, встановлених на них;
- забезпечує технічну підтримку користувачів інформаційних активів по каналах зв’язку.

Стосовно працівників Банку, виконання наведених вище функцій повинно бути зафіксовано у посадових інструкціях або відповідних наказах керівників установ банку.

6. ЦІЛІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

До основних цілей забезпечення інформаційної безпеки належать забезпечення наступних властивостей інформації:

- конфіденційність (confidentiality) – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем та/або процесом;

- цілісність (integrity) – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем та/або процесом. Цілісність системи (system integrity) – властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки;
- доступність (availability) – властивість ресурсу системи, яка полягає в тому, що користувач та/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний;
- спостережність (accountability) – властивість системи, що дає можливість фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно встановлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки та/або забезпечення відповідальності за певні дії.

7. ПРИНЦИПИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Забезпечення інформаційної безпеки Банку ґрунтується на наступних фундаментальних принципах:

- **Мінімальність повноважень.** Доступ працівників Банку та користувачів інформаційних систем до інформаційних ресурсів обчислювальної мережі Банку повинен бути організований таким чином, щоб надавати тільки ті повноваження, що необхідні для виконання службових завдань.
- **Явне санкціонування дій.** Дії працівників Банку, що явно не дозволені внутрішніми розпорядчими або нормативними документами, є забороненими.
- **Законність.** Система управління інформаційною безпекою Банку бере до уваги вимоги чинного законодавства України, а також вимоги міжнародних нормативних вимог у галузі інформаційної безпеки.
- **Узгодженість.** Цілі та завдання інформаційної безпеки відповідають стратегічним цілям та завданням Банку.
- **Єдність.** Управління інформаційної безпекою є невід'ємною частиною управління Банком.
- **Ефективність.** Засоби захисту інформаційних ресурсів впроваджуються відповідно до їхньої критичності, тобто категорії класифікації та рівня ризику інформаційного ресурсу, ґрунтуючись на засадах оцінки ризику та управління ризиком
- **Практичність.** Засоби захисту інформаційних ресурсів повинні бути практичними та підтримувати баланс між працездатністю та захищеністю інформаційних систем.

- **Безперервність.** Інформаційна безпека є безперервним процесом протистояння загрозам та управління ризиками, характерними для сфери діяльності Банку.
- **Відповідальність.** Керівництво Банку всіх рівнів, працівники, постачальники та інші треті сторони, які мають доступ до інформаційних ресурсів Банку, повинні дотримуватися вимог нормативно-правових актів Банку в області інформаційної безпеки та несуть персональну відповідальність за їхнє виконання.
- **Принцип постійного удосконалення.** Забезпечення інформаційної безпеки передбачає засоби контролю кожного процесу та показники ефективності, за якими можна реєструвати зміни й визначати тенденції, усувати причини негативних факторів та заохочувати поліпшення.
- **Потайність.** Виключає ознайомлення сторонніх осіб з організаційними та технічними засобами забезпечення інформаційної безпеки.
- **Принцип захисту в глибину.** Забезпечення інформаційної безпеки передбачає створення наступного ряду послідовних рівнів захисту інформаційних ресурсів та персоналу Банку від ймовірних загроз:
  - Організаційно-правовий рівень, який визначає нормативно-правові вимоги та зобов'язання персоналу, користувачів інформаційних ресурсів та контрагентів Банку щодо інформаційної безпеки;
  - Фізичний рівень захисту, який запобігає неавторизованому фізичному доступу, ушкодженню та вторгненню до службових приміщень Банку та втручання в його інформацію;
  - Рівень прикладного програмного забезпечення, який відповідає за взаємодію з користувачем інформаційних активів;
  - Рівень системи управління базами даних, який відповідає за зберігання та оброблення даних;
  - Рівень операційної системи, який відповідає за безпечне та надійне обслуговування прикладного програмного забезпечення та систем управління базами даних;
  - Рівень мережі, який відповідає за взаємодію вузлів інформаційної системи Банку.
- **Комплексність та системність.** Інформаційна безпека Банку забезпечується на правовому, адміністративному, організаційному та програмно-технічному рівнях, а також на підставі комплексного застосування засобів захисту інформації та взаємодії всіх підрозділів Банку.

Принципи інформаційної безпеки повинні бути інтегровані в усі аспекти управління операційною діяльністю та інформаційними технологіями Банку.

8. ПЕРЕЛІК ВЗАЄМОПОВ'ЯЗАНИХ ДОКУМЕНТІВ

Політика розроблена відповідно до вимог таких чинних документів:

- законів України Про інформацію, Про захист інформації в інформаційно-телекомунікаційних системах, Про електронні документи та електронний документообіг, Про електронні довірчі послуги, Про захист персональних даних, Про Національний банк України, Про банки і банківську діяльність, Кодексу України про адміністративні правопорушення, Кримінального кодексу України, Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму;
- нормативно-правових актів НБУ з інформаційної безпеки, в тому числі Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України (затверджено постановою правління НБУ від 28 вересня 2017 року № 95), стандартів 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";
- стандарту безпеки даних індустрії платіжних карток PCI DSS.

9. ПЕРЕГЛЯД ПОЛІТИКИ

Перегляд Політики ініціюється та здійснюється Комітетом СУІБ щонайменше один раз на рік та в разі впровадження нових або зміни існуючих інформаційних систем та технологій в Банку, а також у зв'язку з прийняттям нових нормативно-правових актів або змін у чинному законодавстві України.

Відповідальність за внесення змін в Політику несе голова Комітету СУІБ.

10. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

Цей документ набуває чинності з дати його затвердження постановою правління Банку.

У подальшому відповідальність за супроводження Політики покладається на управління захисту інформації.

Зміни та доповнення до даного документу затверджуються рішенням Комітету СУІБ та можуть оформлюватись у тому числі шляхом викладення Політики в новій редакції.

У разі невідповідності будь-якої частини даної Політики чинному законодавству України, в тому числі у зв'язку з прийняттям нових нормативно-правових актів, ця Політика буде діяти лише в тій частині, яка не суперечитиме чинному законодавству України.

11. ІСТОРІЯ ЗМІН

Дата	Автор	Зміст змін
28.03.2019	Нікітюк Д.В.	Враховані зміни у законодавстві України
19.07.2019	Нікітюк Д.В.	В частині зміни повного найменування Банку