ЗАВЕРДЖЕНО
В.о. заступника Голови
Ричаківська В.І.

_____
“ 01 ” березня 2011

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України

1. Вступ

Система управління інформаційною безпекою є сучасним процесом забезпечення безпеки інформаційних ресурсів організації, яка побудована на кращих світових практиках. Стандарти Національного банку України основані на міжнародних стандартах ISO 27001 та ISO 27002 з додаванням вимог із захисту інформації, зумовлених конкретними потребами сфери банківської діяльності і правовими вимогами, які вже висунуто в нормативних документах Національного банку України.

Відповідність системи управління інформаційною безпекою стандартам Національного банку України СОУ Н НБУ 65.1 СУІБ 1.0:2010 та СОУ Н НБУ 65.1 СУІБ 2.0:2010 гарантує банку відповідність міжнародним стандартам ISO 27001 та ISO 27002 і надає можливість отримати відповідний сертифікат.

Необхідність впровадження в банках України стандартів з управління інформаційною безпекою продиктована вимогами Базельського комітету Basel II з управління та зменшення операційних ризиків банків.

Впровадження в банках України стандартів з управління інформаційною безпекою дозволить:

- оптимізувати вартість побудови та підтримання системи інформаційної безпеки;
- постійно відслідковувати та оцінювати ризики з урахуванням цілій бізнесу;
- ефективно виявляти найбільш критичні ризики та знижати ймовірність їх реалізації;
- розробити ефективну політику інформаційної безпеки та забезпечити її якісне виконання;
- ефективно розробляти, впроваджувати та тестувати плани відновлення бізнесу;

- забезпечити розуміння питань інформаційної безпеки керівництвом та всіма працівниками банку;
- забезпечити підвищення репутації та ринкової привабливості банків;
- знизити ризики рейдерських та інших шкідливих для банку атак;
- тощо.

Слід зазначити, що наведені вище переваги не будуть досягнуті шляхом лише "формального" підходу до розроблення, впровадження, функціонування системи управління інформаційною безпекою та незацікавленості керівництва і працівників банку в підвищенні рівня інформаційної безпеки.

2. Загальні положення

Ці Методичні рекомендації щодо впровадження системи управління інформаційною безпекою розроблені на основі міжнародного стандарту ISO/IEC 27003:2010 "Information technology – Security techniques – Information security management system implementation guidance" (Настанова з впровадження системи управління інформаційною безпекою) з урахуванням особливостей банківської діяльності, стандартів та вимог Національного банку України з питань інформаційної безпеки.

Впровадження стандартів з питань управління інформаційною безпекою не може бути разовою акцією. Це фактично є безперервним процесом розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення системи управління інформаційною безпекою (СУІБ). Для процесів СУІБ застосована модель ПВПД (плануй-виконуй-перевіряй-дій), наведена у вступі до стандарту СОУ Н НБУ 65.1 СУІБ 1.0:2010.

Зрозуміло, що для проведення цих робіт потрібні ресурси, у тому числі наявність фахівців з питань інформаційної безпеки, наявність з боку керівництва банку повної підтримки та контролю, а також розуміння проблем, що виникають.

Система інформаційної безпеки повинна забезпечити безпечність та надійність функціонування бізнес-процесів/банківських продуктів банку. Впровадження та функціонування СУІБ стосується всіх підрозділів банку і, у першу чергу, керівників підрозділів – власників бізнес-процесів/банківських продуктів. Тому ці відповідальні особи повинні брати участь у вирішенні питань, що належать до сфери їх відповідальності, під час упровадження та функціонування СУІБ.

Цілі СУІБ та заходи безпеки, що вже існують і ті, що будуть додатково впроваджені в разі необхідності, а також відповідна документація, що описує функціонування СУІБ, повинні бути зрозумілими для всіх, кого це стосується. Тому обов'язковою умовою успішного функціонування СУІБ є також проведення відповідних навчань з питань інформаційної безпеки.

3. Підготовка до впровадження СУІБ

3.1. Зобов’язання керівництва щодо управління інформаційною безпекою

Відповідно до розділу 5 стандарту СОУ Н НБУ 65.1 СУІБ 1.0:2010 та пункту 6.1.1 стандарту СОУ Н НБУ 65.1 СУІБ 2.0:2010 керівництво банку повинно забезпечити визначення завдань інформаційної безпеки, їх відповідність вимогам законодавства України, нормативно-правових актів Національного банку України та банку, інтегрованість у відповідні бізнес-процеси/банківські продукти, переглядати ефективність впровадження та функціонування СУІБ, надавати ресурси, які потрібні для інформаційної безпеки та навчання персоналу з питань інформаційної безпеки.

Для вирішення цих завдань необхідно визначити організаційну структуру управління інформаційною безпекою, повноваження та відповідальність щодо розроблення, впровадження та функціонування СУІБ.

Керівництво СУІБ може здійснювати керівник банку або його заступник, або існуючий керівний орган, наприклад, рада з питань інформатизації з обов’язковим включенням до складу спеціалістів з питань інформаційної безпеки. В залежності від розміру банку ці обов’язки можуть бути покладені на створений спеціальний керівний орган з питань інформаційної безпеки з керівників підрозділів, відповідальних за критичні бізнес-процеси та банківські продукти. Формування такого керівного органу тільки з фахівців з питань інформаційної безпеки є недоцільним, оскільки в такому випадку питання інформаційної безпеки будуть за межами уваги керівників, відповідальних за критичні бізнес-процеси, або питання інформаційної безпеки будуть вирішуватися окремо для кожного бізнес-процесу, що створить додаткові умови для несанкціонованого доступу до інформації та порушення конфіденційності, а також призведуть до додаткових фінансових витрат. У разі необхідності до роботи з окремих питань в цьому керівному органі можуть долучатися зовнішні спеціалісти з питань інформаційної безпеки за умови підписання угоди про конфіденційність.

Відповідно до пункту 6.1.2 стандарту СОУ Н НБУ 65.1 СУІБ 2.0:2010 діяльність щодо інформаційної безпеки повинна бути узгоджена між представниками різних підрозділів банку, які відповідають та забезпечують функціонування критичних бізнес-процесів/банківських продуктів. Банки мають створювати єдину систему інформаційної безпеки для всіх бізнес-процесів та координувати дії різних підрозділів для забезпечення виконання загальних вимог щодо інформаційної безпеки. Для виконання цих обов’язків може бути створена окрема група з перехресними функціями з фахівців різних підрозділів. Якщо банк не створює окрему групу з перехресними функціями, то ці обов’язки повинні виконуватися спеціальним керівним органом або окремим керівником.

Зазвичай, координація інформаційної безпеки повинна стосуватися

співробітництва і координації спільної діяльності менеджерів, користувачів, адміністраторів, розробників прикладних програм, аудиторів і персоналу безпеки, а також фахівців у таких галузях, як страхування, правові питання, людські ресурси, управління ІТ або ризиками.

3.2. Призначення відповідальних осіб за впровадження та функціонування СУІБ

Для забезпечення впровадження, функціонування СУІБ та контролю за функціонуванням СУІБ наказом має бути призначений керівник СУІБ відповідно до рекомендацій пункту 3.1, а саме керівник банку або його заступник, який відповідає за питання інформаційної безпеки та в оперативному підпорядкуванні якого знаходиться підрозділ інформаційної безпеки. Керівник СУІБ повинен мати повноваження долучати до впровадження та функціонування СУІБ усіх потрібних фахівців і в першу чергу керівників підрозділів – власників бізнес-процесів/банківських продуктів.

Заступником керівника СУІБ може бути призначений керівник підрозділу, який відповідає за інформаційну безпеку в банку.

У наказі рекомендується зазначити, що керівники підрозділів – власників бізнес-процесів/банківських продуктів мають сприяти впровадженню і функціонуванню СУІБ та своєчасно надавати необхідну інформацію керівникові СУІБ або його заступнику.

3.3. Визначення вимог з інформаційної безпеки банку

Для впровадження та подальшого вдосконалення СУІБ необхідно чітко визначити вимоги з інформаційної безпеки банку.

Джерелами вимог з інформаційної безпеки є:

- Закони України;
- нормативно-правові акти Національного банку України;
- вимоги платіжних систем та систем переказу коштів;
- внутрішні нормативні документи банку;
- умови угод та договорів з третіми сторонами тощо.

Слід звернути увагу на те, що вимоги з інформаційної безпеки для платіжних систем та систем переказів коштів висуваються платіжною організацією платіжної системи та системи переказу коштів, тому вони можуть відрізнятися від вимог Національного банку України (крім Системи електронних платежів (СЕП) та Національної системи масових електронних платежів (НСМЕП), платіжними організаціями яких є Національний банк України). Однак, облік коштів повинен здійснюватися в системах автоматизації банку відповідно до вимог нормативно-правових актів Національного банку України.

Особливу увагу слід звернути на умови угод та договорів з третіми сторонами. Відповідно до пункту 6.2 стандарту СОУ Н НБУ 65.1 СУІБ 2.0:2010

безпека інформації та засобів оброблення інформації банку не повинна знижуватися через уведення в експлуатацію продуктів або послуг зовнішньої сторони. Якщо є бізнес-потреба в роботі із зовнішніми сторонами, яка може вимагати доступу до інформації або засобів оброблення інформації банку, або в отриманні від зовнішньої сторони чи наданні їй продукту та послуги, тоді банк повинен виконувати оцінку ризику для визначення вимог щодо заходів безпеки та наслідків порушення безпеки. Заходи безпеки повинні бути погоджені та визначені в угоді із зовнішньою стороною. Ці питання повинні розглядатися не тільки для договорів про надання послуг клієнтам банку (системи типу "клієнт-банк", інтернет-банкінг, мобільний банкінг тощо), а також при отриманні послуг зовнішніх сторін (розробка та супроводження програмного забезпечення, придбання та технічне обслуговування обладнання, надання послуг зв'язку тощо).

Аналіз вимог з наведених вище джерел допоможе правильно визначити цілі СУІБ та заходи безпеки, які можуть забезпечити зменшення ризиків операційної діяльності банку з урахуванням особливостей роботи банку.

Перелік вимог з інформаційної безпеки повинен бути задокументованим та затвердженим керівництвом банку.

4. Опис існуючої інфраструктури та заходів безпеки

4.1. Класифікація інформації

Відповідно до Закону України "Про інформацію" вся інформація з обмеженим доступом повинна бути надійно захищена. Відповідно до законів України "Про захист інформації в інформаційно-телекомуникаційних системах", "Про банки та банківську діяльність", "Про захист персональних даних" у банках можна визначити такі категорії інформації з обмеженим доступом:

- банківська таємниця;
- комерційна таємниця;
- персональні дані;
- інша конфіденційна інформація.

Банк має створити максимально докладний та зрозумілий перелік відомостей, які відносяться до інформації з обмеженим доступом. У цьому переліку повинні бути описані види інформації, які відносяться до кожної з категорій інформації з обмеженим доступом, що надасть можливість полегшити працівнику банку визначення відношення певної інформації до відповідної категорії.

Відповідно до "Правил зберігання, захисту, використання та розкриття банківської таємниці", затверджених постановою Правління Національного банку України від 14.07.2006 № 267, зареєстрованих в Міністерстві юстиції України 03.08.2006 за № 935/12809, працівники банку під час прийому на роботу повинні власноруч підписувати зобов'язання щодо збереження

банківської таємниці. Ці зобов'язання банк може поширити на всі категорії інформації з обмеженим доступом.

Банк зобов'язаний у внутрішніх положеннях встановити спеціальний порядок поводження та ведення діловодства з документами, що містять інформацію з обмеженим доступом, зокрема визначити порядок підготовки і реєстрації вихідних документів, роботи з документами, відправлення та зберігання документів, а також особливості роботи з електронними документами, які містять інформацію з обмеженим доступом, зокрема з урахуванням вимог, що викладені в наведеному вище нормативно-правовому акті Національного банку України.

Особливу увагу слід звернути на маркування документів з обмеженим доступом. Скорочені позначки грифу інформації з обмеженим доступом повинні бути загально відомими, наприклад, банківська таємниця – БТ, комерційна таємниця – КТ тощо. Не рекомендується використовувати інші літери для скорочених позначок грифу інформації, які не пов'язані із повною назвою грифу та не є інтуїтивно зрозумілими.

4.2. Опис критичних бізнес-процесів та програмно-технічних комплексів, які забезпечують їх функціонування

Відповідно до вимог стандартів Національного банку України сферою застосування СУІБ, яка має бути впроваджена, є банк у цілому. Тому дуже важливо чітко визначити бізнес-процеси/банківські продукти, які працюють з інформацією з обмеженим доступом і повинні бути захищеними.

Відповідно до Положення про організацію операційної діяльності в банках України, затвердженого постановою Правління Національного банку України від 18.06.2006 № 254 банківський продукт – це стандартизовані процедури, що забезпечують виконання банками операцій, згрупованих за відповідними типами та ознаками.

Поняття бізнес-процесу є багатозначним і не існує загально прийнятого його визначення. Під бізнес-процесом у широкому значенні розуміється структурована послідовність дій з виконання певного виду діяльності на всіх етапах життєвого циклу предмета діяльності. Кожен бізнес-процес має початок (вхід), вихід та послідовність процедур, які забезпечують виконання операцій, згрупованих за відповідними типами.

Не існує стандартного набору бізнес-процесів/банківських продуктів для будь-якого банку. Тому банк має самостійно визначити відповідні бізнес-процеси/банківські продукти, які використовуються всередині банку.

Для визначення бізнес-процесів/банківських продуктів, які має охоплювати СУІБ, необхідно проаналізувати всі бізнес-процеси/банківські продукти банку та створити перелік критичних процесів, функціонування яких має великий вплив на успішну роботу банку. Оскільки в банку бізнес-процеси/банківські продукти взаємопов'язані, то рекомендується створити їх блок-схему з визначенням усіх взаємозв'язків. Така візуалізація значно спростить розуміння всього обсягу робіт, що виконуються банком.

Банк повинен створити перелік критичних бізнес-процесів/банківських продуктів, які обробляють інформацію з обмеженим доступом, розголошення якої може нанести шкоду банку. До цього переліку повинні бути включеними всі бізнес-процеси/банківські продукти, що обробляють:

- платіжні документи,
- внутрішні платіжні документи,
- кредитні документи,
- документи на грошові перекази,
- персональні дані клієнтів та працівників банку,
- статистичні звіти,
- інші документи, які містять інформацію з обмеженим доступом.

Для кожного критичного бізнес-процесу/банківського продукту рекомендується надати перелік бізнес-процесів/банківських продуктів, з якими взаємодіє цей бізнес-процес/банківський продукт.

Перелік критичних бізнес-процесів/банківських продуктів повинен супроводжуватися коротким описом кожного бізнес-процесу/банківського продукту з наданням інформації про програмно-технічні комплекси, які забезпечують його функціонування.

Короткий опис кожного бізнес-процесу/банківського продукту повинен містити таку інформацію:

- назва бізнес-процесу/банківського продукту;
- цілі бізнес-процесу/банківського продукту;
- гриф інформації з обмеженим доступом, яка обробляється бізнес-процесом/банківським продуктом;
- власник бізнес-процесу/банківського продукту;
- підрозділи банку, які забезпечують функціонування бізнес-процесу/банківського продукту;
- наявність зобов'язань перед третіми сторонами (угоди на розроблення, доопрацювання, супроводження та технічне обслуговування);
- вхідні та вихідні дані бізнес-процесу/банківського продукту;
- перелік процедур бізнес-процесу та блок-схема послідовності їх виконання з визначенням взаємозв'язків (у тому числі додаткової вхідної інформації з інших бізнес-процесів);
- вимоги щодо забезпечення безперервності бізнес-процесу/ банківського продукту (максимально допустимий час простою);
- типи ролей(груп) для бізнес-процесу/банківського продукту;
- існування забороненого суміщення типів ролей;
- програмно-технічний(ні) комплекс(и), що забезпечує(ють) функціонування бізнес-процесу;
- кількість користувачів програмно-технічного комплексу;

- архітектура і технологія роботи (зокрема, файловий обмін або режим реального часу, в тому числі й для обміну інформацією з іншими програмно-технічними комплексами в разі наявності);
- операційна система та тип бази даних програмно-технічного комплексу, які використовуються для функціонування бізнес-процесу/банківського продукту;
- географічне розміщення (серверів та робочих місць) програмно-технічного комплексу;
- засоби захисту, які вже існують у програмно-технічному комплексі;
- взаємодія з іншими програмно-технічними комплексами;
- принципи резервування обладнання та інформації програмно-технічного комплексу (за наявності окремих принципів для цього програмно-технічного комплексу).

Зазначимо деякі аспекти формування цієї інформації.

Дуже важливо визначити власника бізнес-процесу/банківського продукту, який повинен також бути власником програмно-технічного комплексу. Саме власник бізнес-процесу/банківського продукту/програмно-технічного комплексу повинен приймати рішення щодо надання доступу до інформації, яка обробляється в цьому бізнес-процесі/банківському продукту/програмно-технічному комплексі. Власником програмно-технічного комплексу не може бути підрозділ банку, який відповідає за інформаційні технології і забезпечує технічну підтримку роботи комплексу.

Перелік процедур бізнес-процесу та блок-схема послідовності їх виконання з визначенням взаємозв’язків (у тому числі додаткової вхідної інформації з інших бізнес-процесів) буде дуже корисним під час аналізу та визначення вразливостей, притаманних цьому бізнес-процесу/банківському продукту. Цей перелік та блок-схема мають бути у достатньому ступені узагальненими. Дуже детальний перелік може призвести до ускладнення під час визначення вразливостей. Однак, якщо цей перелік та блок-схема будуть занадто узагальненими, то це може призвести до пропуску небезпечних вразливостей, які можуть створювати великі ризики.

У разі якщо функціонування одного бізнес-процесу/банківського продукту забезпечується декількома програмно-технічними комплексами, тоді короткі описи кожного комплексу та їх взаємозв’язків повинні також бути надані.

У разі якщо один програмно-технічний комплекс забезпечує функціонування декількох бізнес-процесів/банківських продуктів, тоді визначається єдиний власник програмно-технічного комплексу (але не підрозділ, який відповідає за інформаційні технології) або група власників бізнес-процесів, які надають та контролюють доступ до інформації, що обробляється різними модулями комплексу.

У разі відсутності централізованих програмно-технічних комплексів мають бути надані короткі описи програмно-технічних комплексів у

структурних підрозділах банку (обласних дирекціях, філіях тощо) та описаний взаємозв’язок між ними.

Для більшого розуміння зв’язків між бізнес-процесами/банківськими продуктами/програмно-технічними комплексами рекомендується створити блок-схему цих зв’язків із додаванням структурних підрозділів банку, які забезпечують ці бізнес-процеси/банківські продукти/програмно-технічні комплекси вхідною інформацією, та підрозділів банку, які використовують вихідні дані.

Типи ролей(груп) для бізнес-процесу/банківського продукту фактично означають різні рівні доступу до інформації, яка обробляється цим бізнес-процесом/банківським продуктом. При цьому слід пам’ятати про необхідність надання мінімальних прав доступу, необхідних для виконання службових обов’язків. Обов’язковим також є визначення заборонених суміщень прав доступу (ініціювання та подальше виконання операції) для запобігання підготовки фальсифікованих банківських документів або несанкціонованої модифікації документів. Наприклад, для платіжних документів забороненим є суміщення обов’язків операціоніста та бухгалтера.

4.3. Опис організаційної структури банку, яку охоплює СУІБ

На основі вихідних документів попереднього пункту банк має визначити всі підрозділи, які відносяться до сфери застосування СУІБ. Це підрозділи, які є власниками та учасниками критичних бізнес-процесів, підрозділи, які супроводжують та забезпечують технічну підтримку програмно-технічних комплексів, користувачі програмно-технічних комплексів, служба безпеки, яка забезпечує фізичну безпеку приміщень банку, тощо. Наявність такого переліку підрозділів дозволить чітко визначити обов’язки та відповідальності всіх причетних до виконання вимог безпеки сторін та планувати їх навчання у разі необхідності. Такий перелік може створюватися на основі структурної схеми підрозділів банку.

Окрім того, у разі наявності передавання частини послуг, що пов’язані з критичними бізнес-процесами/банківськими продуктами/програмно-технічними комплексами, третім сторонам, ці організації також повинні бути включені до опису організаційної структури банку з поміткою, що вони не є структурними підрозділами банку.

4.4. Опис структури мережі банку

Для подальшого аналізу захищеності мережі банку необхідно зробити опис структури мережі банку, засобів захисту та управління, які вже існують. Банк повинен мати внутрішнє положення про мережу банку, у якому надається така інформація:

- принципи побудови мережі з описом принципів резервування мережевого обладнання;

- принципи розподілу мережі на сегменти (підмережі) – за наявності;
- принципи розподілу адресного простору;
- система управління мережею;
- побудова вузла доступу до ресурсів мережі Інтернет;
- принципи доступу до мереж інших організацій – за наявності;
- наявність та правила роботи через канали зв'язку зовнішніх провайдерів телекомунікаційних послуг, у тому числі опис принципів резервування каналів зв'язку;
- засоби захисту мережі від зовнішнього та внутрішнього несанкціонованого доступу, у тому числі антивірусного захисту;
- принципи надання доступу працівникам банку до мережі та ресурсів мережі Інтернет;
- принципи та процедура надання віддаленого доступу працівникам банку до мережі банку – за наявності;
- принципи та процедура надання бездротового доступу до мережі банку – за наявності;
- принципи резервного копіювання інформації.

Для спрощення розуміння особливостей побудови мережі банку рекомендується створити окремі внутрішні положення (політики) за різними питаннями управління мережею, а в загальному положенні про мережу описати основні принципи побудови та функціонування мережі з наданням посилань на окремі політики.

4.5. Опис фізичного середовища

Питання захисту інфраструктури банку також входять до СУІБ.

Банк повинен мати такі документи:

- опис географічного та територіального розташування приміщень банку, включаючи відокремлені підрозділи банку (обласні дирекції, філії, відділення тощо) для визначення загроз з боку навколишнього середовища;
- опис принципів пропускного режиму;
- наказ із визначення приміщень з обмеженим доступом та опис відповідного захисту цих приміщень із забезпеченням контролю доступу до таких приміщень;
- опис принципів побудови систем відео спостереження;
- опис системи електроживлення та заземлення;
- опис охоронної та пожежної сигналізації;
- опис умов зберігання магнітних, оптомагнітних, паперових та інших носіїв інформації, у тому числі електронних архівів.

Вимоги до приміщень банків наведені у Правилах технічного захисту приміщень банків, де обробляються електронні банківські документи, затверджені постановою Правління Національного банку України від

04.07.2007 № 243, зареєстрованою в Міністерстві юстиції України 17.08.2007 за № 955/14222 та інших нормативно-правових актах Національного банку України.

4.6. Опис принципів забезпечення безперервності роботи

Однією з основних функцій банку є забезпечення безперервності його роботи. Основні вимоги до банку з цього питання викладені у Положенні про забезпечення безперервного функціонування інформаційних систем Національного банку України та банків України, затвердженому постановою Правління Національного банку України від 17.06.2004 № 265, зареєстрованою в Міністерстві юстиції України 09.07.2004 за № 857/9456.

Банк повинен мати опис принципів та заходів щодо забезпечення безперервності роботи, в якому надати опис процедур та обладнання, а також обов'язків працівників банку, в тому числі методи резервування інформації для відновлення роботи в разі виникнення надзвичайних ситуацій. У цьому документі повинні бути визначені терміни відновлення роботи банку та необхідні ресурси (зокрема програмно-технічні засоби, обладнання, резервне електроживлення тощо).

Банк повинен регулярно проводити тестування всіх складових, що потрібні для виконання плану забезпечення безперервної діяльності та дій у разі виникнення надзвичайних ситуацій, у тому числі можливість відновлення резервної інформації, яка зберігається у віддаленому резервному пункті.

5. Аналіз ризиків

5.1. Загальні положення

Методичні рекомендації щодо управління ризиками інформаційної безпеки розроблені на основі міжнародного стандарту ISO/IEC 27005 "Information technology – Security techniques – Information security risk management" (Управління ризиками інформаційної безпеки) з урахуванням особливостей банківської діяльності, стандартів та вимог Національного банку України з питань інформаційної безпеки.

Ризиком інформаційної безпеки вважається ймовірність того, що визначена загроза, впливаючи на вразливості ресурсу або групи ресурсів, може спричинити шкоду банку.

Управління інформаційними ризиками повинно включати:

- аналіз і ідентифікацію ризиків;
- оцінку ризиків з точки зору їх впливу на бізнес та ймовірності їх появи;

- інформування особи, яка вправі приймати рішення та акціонерів банку про ймовірності та впливи цих ризиків; ймовірність і наслідки ризику мають бути зрозумілими;
- встановлення порядку та пріоритетів оброблення ризиків;
- встановлення пріоритетів виконання дій щодо зниження ризиків;
- участь керівництва в процесі прийняття рішень щодо управління ризиками та його поінформованість щодо стану справ в управлінні ризиками;
- ефективний моніторинг та регулярний перегляд ризиків і процесу управління ризиками;
- інформування керівництва та персоналу щодо ризиків і дій щодо управління ними.

Процес управління ризиками інформаційної безпеки повинен здійснюватися для банку в цілому.

Процес управління ризиками інформаційної безпеки є безперервним процесом і до нього може бути застосована модель ПВПД (плануй-виконуй-перевіряй-дій), яка наведена у Вступі стандарту СОУ Н НБУ 65.1 СУІБ 1.0:2010.

Порівняння СУІБ та процесу управління ризиками інформаційної безпеки можна описати у вигляді таблиці:

Фаза СУІБ	*Процес управління ризиками інформаційної безпеки*
Плануй	Аналіз ресурсів СУІБ Оцінка ризиків План оброблення ризиків Прийняття залишкових ризиків
Виконуй	Впровадження плану оброблення ризиків
Перевіряй	Постійний моніторинг та перегляд ризиків
Дій	Підтримка та покращення процесу управління ризиками інформаційної безпеки

Процес управління ризиками інформаційної безпеки стосується всіх підрозділів банку і, у першу чергу, керівників підрозділів – власників бізнес-процесів/банківських продуктів. Тому ці відповідальні особи повинні брати участь у вирішенні питань, що належать до сфери їх відповідальності.

5.2. Аналіз ресурсів СУІБ та бізнес-процесів/банківських продуктів

Аналіз ресурсів СУІБ та бізнес-процесів/банківських продуктів виконується на основі даних, які були отримані та систематизовані на етапі опису існуючої інфраструктури та заходів безпеки (див. розділ 4). На цьому етапі рекомендується розглянути критичні бізнес-процеси/банківські продукти/програмно-технічні комплекси, які були визначені та описані раніше, з точки зору інформаційної безпеки та можливих втрат у разі порушень

інформаційної безпеки. Цей аналіз виконується тільки на якісному рівні, але дозволить в подальшому більш докладно виконати оцінку ризиків та визначити план оброблення ризиків. Для кожного бізнес-процесу/банківського продукту/програмно-технічного комплексу необхідно розглянути наскільки виконуються та як можуть впливати на бізнес основні сервіси інформаційної безпеки: цілісність, конфіденційність, доступність та спостережність. Такий аналіз повинен виконуватися власниками бізнес-процесів/банківських продуктів/програмно-технічних комплексів разом з фахівцями з питань інформаційної безпеки.

Нагадаємо визначення термінів основних сервісів інформаційної безпеки:

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

цілісність (integrity) – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/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 і/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 дозволяє 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.

Слід зазначити, що для різних бізнес-процесів/банківських продуктів можуть бути виявлені однакові ризики втрати основних сервісів безпеки, що буде свідчити про те, що певним питанням інформаційної безпеки не приділяється необхідної уваги. У такому випадку рекомендується вирішувати питання зменшення ризиків однаково для всіх бізнес-процесів/банківських продуктів банку.

Однак, найбільш поширеним випадком буде наявність в різних бізнес-процесах/банківських продуктах різних за рівнем небезпеки питань, які потребують впровадження конкретних заходів безпеки для конкретного бізнес-процесу/банківського продукту.

Тому докладна оцінка ризиків не може бути загальною для банку в цілому та потребує розгляду як загальних для банку питань, так і конкретних питань для кожного бізнес-процесу/банківського продукту. Крім того, особливу

увагу слід приділити розгляду обміну інформацією між різними бізнес-процесами/банківськими продуктами/програмно-технічними комплексами.

Після виконання такого аналізу з точки зору впливу порушень інформаційної безпеки на бізнес-процеси/банківські продукти/програмно-технічні комплекси можна переходити до більш докладної оцінки ризиків інформаційної безпеки.

5.3. Ідентифікація загроз та вразливостей

Загрози потенційно можуть завдати шкоди ресурсам СУІБ, зокрема інформації, персоналу, клієнтам, обладнанню, процесам і програмно-технічним комплексам, бізнес-процесам/банківським продуктам і, відповідно, банку. Загрози можуть мати природні та людські джерела і можуть бути випадковими або навмисними. Повинні бути ідентифіковані як випадкові, так і навмисні джерела загроз. Загрози можуть бути ідентифіковані в загальному вигляді або за типами (наприклад, неавторизовані дії, фізичне пошкодження, технічні пошкодження тощо).

Деякі загрози можуть впливати на декілька ресурсів СУІБ. У такому випадку вони можуть викликати різний вплив на різні ресурси.

До ідентифікації загроз необхідно залучати власників бізнес-процесів/банківських продуктів та користувачів, підрозділи управління персоналом та фізичної безпекою, спеціалістів з інформаційної безпеки, юридичні підрозділи тощо.

Приклади загроз наведені у додатку 1. Цей перелік не є вичерпаним і повинен доповнюватися в залежності від ситуації в банку, технологій, що використовуються, організаційної структури, процедур тощо.

Вразливості, які можуть бути використані загрозами для впливу на ресурси СУІБ/бізнес-процеси/банківські продукти, також повинні бути ретельно розглянути та ідентифіковані.

Вразливості можуть бути ідентифіковані в таких областях:

- банк у цілому;
- процеси та процедури;
- системи управління;
- персонал;
- фізичне середовище;
- конфігурація програмно-технічних комплексів, обладнання, програмне забезпечення або телекомунікаційне обладнання;
- залежність від зовнішніх організацій.

Наявність вразливостей не може впливати на ресурси та бізнес-процеси/банківські продукти самостійно, оскільки має бути наявна загроза, яка буде використовувати ці вразливості. Для вразливості, якій не відповідає відповідна загроза, не потрібно впровадження заходів безпеки, але вона повинна бути ідентифікована та відслідковуватися під час внесення будь-яких

змін, які пов’язані з цим ресурсом СУІБ і бізнес-процесом/банківським продуктом.

Некоректно запроваджені чи недієві заходи безпеки є одним з видів вразливостей.

Вразливості можуть бути пов’язаними із властивостями ресурсу СУІБ.

Приклади вразливостей наведені у додатку 2. Цей перелік не є вичерпаним і повинен доповнюватися в залежності від ситуації в банку, технологій, що використовуються, організаційної структури, процедур тощо.

Для виявлення вразливостей в залежності від критичності інформації та бізнес-процесу/банківського продукту, а також від інформаційно-телекомунікаційних технологій можуть використовуватися різні проактивні методи тестування. Такі методи тестування включають:

- спеціальний автоматичний інструментарій для сканування вразливостей;
- тестування та оцінку безпеки;
- тести на проникнення;
- перегляд коду програмно-технічних комплексів;
- аналіз відомих порушень безпеки;
- аналіз відомих вразливостей (наприклад, операційних систем, баз даних, телекомунікаційних технологій та протоколів тощо).

Такі методи допоможуть ідентифікувати вразливості.

Слід зазначити, що іноді ці методи можуть надавати інформацію про вразливості, які не представляють реальної загрози. Тому необхідно чітко задавати параметри програмно-технічних комплексів та їх конфігурацію для тестування.

5.4. Ідентифікація наслідків реалізації загроз

Наслідками реалізації загроз можуть бути втрати ефективності, бізнес-процесів, зниження репутації тощо. Необхідно проаналізувати негативні наслідки для банку, які можуть виникати якщо ідентифіковані загрози будуть використовувати відповідні вразливості або набір вразливостей і призведуть до інциденту інформаційної безпеки. Такий інцидент інформаційної безпеки може впливати на один або більше ресурсів СУІБ/бізнес-процес/банківський продукт. Таким чином, ресурсам СУІБ можуть бути приписані значення їх фінансової вартості, а також бізнес наслідків, якщо ці ресурси будуть пошкоджені або скомпрометовані.

6 Оцінка ризиків

6.1. Методологія оцінювання ризиків

Аналіз ризиків може бути виконаний з різним ступенем деталізації в залежності від критичності ресурсів СУІБ/бізнес-процесів/банківських

продуктів, відомих вразливостей і попередніх інцидентів інформаційної безпеки. Методологія оцінки ризиків може бути кількісною або якісною, або їх комбінацією. На практиці якісна оцінка часто використовується спочатку для визначення загального рівня ризику і визначення основних ризиків. Далі може виникнути необхідність виконання більш специфічного або кількісного аналізу стосовно основних ризиків. Кількісна оцінка ризиків є більш складною та потребує більше часу та ресурсів. Однак така оцінка буде дуже корисною у випадках, коли рішення щодо оброблення ризиків буде залежати від вартості заходів безпеки, які можуть бути більшими, ніж фінансові втрати інциденту інформаційної безпеки.

Якісна методика оцінки ризиків використовує шкалу атрибутів для опису величини потенціальних наслідків реалізації загроз і вірогідність того, що такі наслідки виникнуть. Перевагою якісної методики є її простота розуміння всім персоналом; недоліком такої методики є залежність від суб'єктивного вибору шкали атрибутів.

Для отримання якісної оцінки ризиків необхідно розглянути оцінки наслідків реалізації загроз разом із вразливостями, з використанням яких ці загрози можуть реалізуватися, та оцінки ймовірності їх реалізації для кожного бізнес-процесу/банківського продукту, мережі, обладнання, програмного забезпечення, які забезпечують функціонування цього бізнес-процесу/банківського продукту, мережі банку в цілому, фізичного середовища, персоналу тощо, як описано в додатку 2, з урахуванням попереднього аналізу.

Для виконання оцінки ризиків необхідно визначити шкалу для різних параметрів: оцінки величини наслідків реалізації загрози на сервіси безпеки (цілісність, конфіденційність, доступність, спостережність), оцінки ймовірності реалізації загрози. Загальний рівень оцінки величини наслідків реалізації кожної загрози на сервіси безпеки визначається як максимальна величина з окремих оцінок впливу на цілісність, конфіденційність, доступність, спостережність. Звертаємо увагу на те, що оцінка ймовірності не є математичною величиною вірогідності, яка не може перевищувати 1.

Рівень ризику за окремою парою загроза/вразливість, яка може використовуватися для реалізації цієї загрози, визначається перемноженням загального рівня оцінки величини наслідків на оцінку ймовірності реалізації загрози.

Загальний рівень ризику для бізнес-процесу/банківського продукту, персоналу, фізичного середовища тощо дорівнює максимальної величині з усіх ризиків за кожною парою загроза/вразливість.

Рекомендується використовувати такі шкали для оцінки ризиків:

Для оцінки ймовірності реалізації загроз:

Оцінка ймовірності	*Опис*
1	Виникнення інциденту практично неможливо

2	Виникнення інциденту малоймовірне (не частіше ніж 1 раз на 1 рік)
3	Виникнення інциденту ймовірне до 1 разу на 3 місяці
4	Виникнення інциденту ймовірне до 1 разу на тиждень
5	Виникнення інциденту ймовірне до 1 разу на добу

Для величини наслідків реалізації загрози: вплив на цілісність:

Оцінка рівня наслідків	*Опис*
1	Практично не призводить до наслідків з фінансовими втратами
2	Призводить до незначних фінансових втрат (визначити суму) та має незначний вплив на репутацію банку
3	Призводить до значних фінансових втрат (визначити суму) та має значний вплив на репутацію банку
4	Призводить до великих фінансових втрат (визначити суму), має значний вплив на репутацію банку і може призвести до зупинки роботи бізнес-процесу/банківського продукту
5	Призводить до зупинки бізнес-процесу/банківського продукту і порушує законодавство України

Для величини наслідків реалізації загрози: вплив на конфіденційність:

Оцінка рівня наслідків	*Опис*
1	Практично не призводить до розкриття конфіденційної інформації
2	Призводить до розкриття окремих документів, які відносяться до “банківської таємниці”, “комерційної таємниці”, персональних даних і не призводить до фінансових втрат
3	Призводить до розкриття окремих документів, які відносяться до “банківської таємниці”, “комерційної таємниці”, персональних даних і призводить до незначних фінансових втрат (визначити суму)
4	Призводить до розкриття документів, які відносяться до “банківської таємниці”, “комерційної

	таємниці", персональних даних і призводить до значних фінансових втрат (визначити суму), має значний вплив на репутацію банку і може призвести до зупинки роботи бізнес-процесу/банківського продукту
5	Призводить до зупинки бізнес-процесу/банківського продукту і порушує законодавство України

Для величини наслідків реалізації загрози: вплив на доступність:

Оцінка рівня наслідків	*Опис*
1	Практично не впливає на доступність
2	Вплив на доступність незначний (не більше 1/10 від максимально допустимого часу простою для цього бізнес-процесу/банківського продукту)
3	Вплив на доступність середній (не більше S від максимально допустимого часу простою для цього бізнес-процесу/банківського продукту)
4	Вплив на доступність значний (до максимально допустимого часу простою для цього бізнес-процесу/банківського продукту)
5	Призводить до зупинки бізнес-процесу/банківського продукту на тривалий час, який перевищує максимально допустимий час простою)

Для величини наслідків реалізації загрози: вплив на спостережність:

Оцінка рівня наслідків	*Опис*
1	Практично не впливає
2	Вплив незначний
3	Призводить до неможливості відстежити частину дій виконавців бізнес-процесу/банківського продукту
4	Призводить до неможливості відстежити дії виконавців і адміністраторів бізнес-процесу/банківського продукту/ програмно-технічного комплексу
5	Призводить до неможливості відстежити дії виконавців і адміністраторів бізнес-процесу/банківського продукту/ програмно-технічного комплексу, може призвести до зупинки бізнес-процесу/банківського продукту, має вплив на репутацію банку і порушує законодавство України

Визначення конкретних величин для параметрів оцінки повинно виконуватися з урахуванням досвіду працівників банку, вимог нормативно-правових актів Національного банку України, історії попередніх інцидентів інформаційної безпеки, відомих випадків порушення інформаційної безпеки, досвіду інших фінансових установ тощо.

Рекомендується оцінку ризиків документувати у вигляді таблиці для кожного бізнес-процесу/банківського продукту, приклад якої наданий у додатку З.

Такий підхід до оцінки ризиків дозволить чітко виявити найбільші ризики у бізнес-процесах/банківських продуктах і найбільш критичні загрози.

6.2. Оброблення ризиків

Відповідно до пункту 4.2.1 стандарту Національного банку України СОУ Н НБУ 65.1 СУІБ 1.0:2010 після виконання оцінки ризиків банк має оцінити альтернативні варіанти оброблення ризиків. Можливими варіантами оброблення ризиків можуть бути:

- зниження ризиків шляхом застосування належних заходів безпеки;
- свідоме та об'єктивне прийняття ризиків за умови, що вони чітко задовольняють політику організації та критерії прийняття ризиків;
- уникнення ризиків;
- перенесення відповідних бізнес-ризиків на інші сторони, наприклад, страхувальників, постачальників.

Для прийняття рішення щодо оброблення конкретних ризиків рекомендується визначити такі критерії стосовно кожного окремого ризику:

- низький ризик - 1 – 6;
- середній ризик - 7 - 14;
- високий ризик - 15 - 25.

Застосування належних заходів безпеки дозволить зменшити ризики. Під час вибору цих додаткових заходів безпеки повинні бути враховані всі вимоги законодавства України, нормативно-правових актів Національного банку України, внутрішніх документів, політики та стратегії банку. Крім того, цей вибір також повинен враховувати вартість додаткових заходів безпеки, час їх впровадження, вплив на технологію операційної роботи, інтерфейс користувача тощо. З урахуванням цих факторів складається план оброблення ризиків. У разі необхідності тривалої підготовки до впровадження додаткових заходів безпеки деякі ризики можуть бути тимчасово прийняти як залишкові з включенням до наступного плану оброблення ризиків після перегляду оцінки ризиків.

Прийняття всіх залишкових ризиків повинно бути задокументовано і затверджено керівництвом банку. Це стосується середніх та високих ризиків і повинно бути ретельно розглянуто. У документах стосовно прийняття

залишкових ризиків має бути надана причина прийняття ризику та, за необхідністю, строки впровадження додаткових заходів безпеки для зниження ризику. Наприклад, якщо банком використовується програмно-технічний комплекс із застарілими технологіями, який має великий ризик реалізації однієї або декількох загроз і який планується замінити на новий більш сучасний комплекс протягом 2 років, то ці ризики можуть бути прийняти як тимчасове рішення до заміни цього програмно-технічного комплексу з наданням терміну впровадження нового.

Деякі ризики є властивістю існуючого бізнес-процесу/банківського продукту/програмно-технічного комплексу. Особливу увагу слід звернути на вразливості саме програмно-технічних комплексів, які використовують застарілі або новітні незахищені технології. В деяких випадках слід розглянути питання щодо уникнення ризиків за рахунок зміни операційного середовища, баз даних, програмно-технічного комплексу, технології оброблення та зберігання інформації, оскільки це буде вимагати менших витрат, ніж впровадження додаткових заходів безпеки.

6.3. Визначення цілей додаткових заходів безпеки та плану впровадження заходів безпеки

Після вибору варіанту оброблення ризиків у разі необхідності впровадження додаткових заходів безпеки для зменшення ризиків інформаційної безпеки необхідно обрати цілі цих заходів безпеки відповідно до додатку А стандарту Національного банку України СОУ Н НБУ 65.1 СУІБ 1.0:2010. У разі відсутності відповідних цілій заходів безпеки у стандарті банк повинен їх визначити додатково. Додаток А до стандарту не може розглядатися як вичерпний і може доповнюватися відповідно до конкретних цілей бізнесу та особливостей організації операційної роботи банку.

Банк має розробити план оброблення ризиків із наданням інформації стосовно додаткових заходів безпеки, їх цілей та ризиків, особливо по відношенню до зменшення ризиків.

6.4. Підготовка Положення щодо застосовності

Після завершення розроблення плану оброблення ризиків банк має підготувати Положення щодо застосовності. Це Положення має включати всі заходи безпеки, включаючи додаткові, які використовуються в банку для управління інформаційною безпекою. В цьому Положенні формується перелік цілей заходів безпеки та заходи безпеки відповідно до додатку А стандарту Національного банку України СОУ Н НБУ 65.1 СУІБ 1.0:2010 з додатковими заходами безпеки, і воно повинно включати таку інформацію:

- цілі заходів безпеки і короткий опис заходів безпеки, які впроваджені на теперішній час та обґрунтування їх вибору;

- цілі заходів безпеки і короткий опис заходів безпеки, які планується впровадити з визначенням терміну впровадження та обґрунтування їх вибору;
- будь-які вилучені цілі заходів безпеки і заходи безпеки з тих, що наведено у додатку А, і обґрунтування їх вилучення, що дає можливість перевірки, що жодні заходи безпеки не були випадково пропущені.

Приклад Положення щодо застосовності наданий у додатку 4.

7. Документація

7.1. Загальний опис документації

Під час підготовки до впровадження СУІБ повинні бути створені відповідні документи, перелік яких наданий у додатку 5. За наявності таких документів у банку вони повинні бути переглянути та оновлені в разі необхідності у відповідності до вимог щодо оформлення документів, які наведені далі.

Загальний комплект документів, який повинен бути наявним на момент впровадження СУІБ і який відповідає стандарту ISO 27001. має чотирьохрівневу структуру, а саме:

- адміністративні документи;
- документи верхнього рівня;
- документи середнього рівня;
- документи нижнього рівня.

7.2. Адміністративні документи

Адміністративні документи є обов’язковою начальною точкою підготовки до впровадження СУІБ, як це описано в розділі 3, пунктах 3.1.-3.2. Ці документи включають:

- наказ про створення спеціального керівного органу з питань інформаційної безпеки (за необхідністю);
- положення про спеціальний керівний орган з питань інформаційної безпеки (за його наявністю);
- у разі відсутності спеціального керівного органу з питань інформаційної безпеки наказ про покладення обов’язків цього органу на існуючий керівний орган;
- наказ про впровадження та функціонування СУІБ;
- наказ про призначення керівника проекту впровадження та функціонування СУІБ;
- положення про службу захисту інформації (підрозділ інформаційної безпеки);

- положення про службу безпеки (охорона, пропускний та внутрішньобанківський режим тощо);
- посадові інструкції відповідальних за впровадження та функціонування СУІБ осіб;
- організаційна структура банку.

Ці документи оформляються відповідно до правил внутрішнього діловодства банку і можуть бути поєднаними згідно з особливостями роботи банку. Наприклад, якщо підрозділ захисту інформації входить до складу одного структурного підрозділу разом з фахівцями з фізичної безпеки, то потрібно тільки одне положення про підрозділ банківської безпеки. Відповідно назви підрозділів формуються згідно з внутрішніми правилами банку.

Частина описаних документів вже існує в банку, але рекомендується їх переглянути та доповнити відповідними вимогами та наданими повноваженнями щодо впровадження та функціонування СУІБ.

7.3. Документи верхнього рівня

Документи верхнього рівня є фактично основою СУІБ. Їх можна розділити на дві групи.

До першої групи відносяться два основних документа, які визначають стратегію розвитку банку та загальну політику інформаційної безпеки. Стратегія розвитку банку повинна містити основні стратегічні цілі банку, в тому числі й ті, що пов’язані з впровадженням нових бізнес-процесів/банківських продуктів із використанням новітніх технологій, які потребують захисту інформації. Наявність такого документу дозволить забезпечити планування розвитку інфраструктури банку та заходів безпеки, які повинні бути передбачені у СУІБ для зменшення операційних ризиків банку. Політика інформаційної безпеки банку повинна містити основні цілі безпеки та принципи, які мають забезпечувати безпеку банку. Обидва документа мають бути короткими (2-3 стор.), прийнятними для зрозуміння усіма працівниками банку та бути достатньо конкретними. У додатку 6 наведений приклад політики інформаційної безпеки.

До другої групи документів верхнього рівня відносяться документи, які описують основу побудови системи управління інформаційною безпекою:

- цілі СУІБ;
- сфера застосування СУІБ;
- організаційна структура банку, яка охоплюється СУІБ;
- політика управління інформаційною безпекою;
- опис методології оцінки ризиків;
- звіт щодо оцінки ризиків;
- опис методології оброблення ризиків з визначенням критеріїв прийняття залишкових ризиків;
- план оброблення ризиків;
- положення щодо застосовності.

Перші чотири документа можуть бути поєднані в один – політику управління інформаційною безпекою, але з обов'язковим уключенням перших трьох документів у вигляді окремих розділів.

Політика управління інформаційною безпекою може бути розділена на дві політики: зовнішню, яка описує політику управління інформаційною безпекою для зовнішніх зв'язків банку, та внутрішню, яка описує правила інформаційної безпеки для працівників банку.

Для зменшення обсягу політики управління інформаційною безпекою рекомендується окремі питання винести в окремі цільові політики (положення) з наданням відповідних посилань. Зокрема, за бажанням банку можуть бути створені такі окремі документи:

- перелік законодавчих, регуляторних, нормативних вимог з інформаційної безпеки для банку (пункт 3.3) (додаток 7);
- перелік відомостей, що містять інформацію з обмеженим доступом;
- перелік критичних бізнес-процесів/банківських продуктів/програмно-технічних комплексів (пункт 4.2);
- політика визначення критичних бізнес-процесів/банківських продуктів;
- політика надання доступу до інформації;
- політика контролю доступу;
- політика парольного захисту;
- політика антивірусного захисту;
- політика захисту мережі банку;
- політика віддаленого доступу до ресурсів мережі;
- політика ідентифікації та автентифікації ресурсів СУІБ;
- політика криптографічного захисту інформації;
- політика "чистого екрана та чистого стола";
- інші політикі (положення) відповідно до технології організації операційної роботи банку.

Слід зазначити, що політика управління інформаційною безпекою має бути створена передостанньою, після завершення аналізу існуючого стану інформаційної безпеки, оцінки ризиків та створення плану оброблення ризиків. Політика управління інформаційною безпекою повинна містити інформацію про існуючі заходи безпеки та плани щодо зменшення ризиків. Існування окремих цільових політик надасть можливість не описувати докладно усі заходи безпеки, а надавати посилання на відповідні політики (положення).

Останнім документом створюється Політика щодо застосовності, де повинні бути наданий перелік заходів безпеки із стандарту Національного банку України з додаванням додаткових заходів безпеки за необхідністю з коротким описом як вони реалізовані або поясненням чому вони не використовуються в банку.

Наданий перелік другої групи документів верхнього рівня є неповним і необов'язковим; він може бути скороченим або доповненим іншими документами. Під час прийняття рішення стосовно переліку цих документів

слід мати на увазі, що найбільш ефективним буде створення коротких, чітких та зрозумілих документів, ніж створення одного дуже великого документу, з яким буде дуже важко працювати як працівникам банку, які повинні його виконувати, так і авторам цього документу під час внесення необхідних змін у зв'язку зі змінами інфраструктури банку, технології оброблення інформації та заміни засобів захисту.

Для спрощення опрацювання всіх документів рекомендується ввести єдиний підхід щодо структури документів (пункт 7.6).

7.4. Документи середнього рівня

Документи середнього рівня фактично є технічними документами, які спрямовані на опис способів реалізації заходів безпеки для захисту ресурсів СУІБ від загроз. Саме на цьому рівні повинні бути описаними конкретні операції, які мають виконуватися різними користувачами, описані питання розподілу повноважень та відповідальності по кожної операції, встановлюються строки виконання кожної операції, створюються шаблони угод із зовнішніми сторонами тощо. Ці документи мають створюватися не тільки спеціалістами з інформаційної безпеки, а також спеціалістами відповідних підрозділів за напрямками, а саме: спеціалістами по інформаційним технологіям, по фізичному захисту, по роботі з персоналом, юридичного підрозділу тощо. Основними користувачами документів середнього рівня є керівники відповідних підрозділів, відповідальні особи за окремі ресурси СУІБ, адміністратори.

Наданий нижче перелік документів середнього рівня побудований згідно із Додатком А стандарту Національного банку України СОУ Н НБУ 65.1 СУІБ 1.0:2010:

А.6. Організація інформаційної безпеки:

- Зобов'язання працівників банку щодо збереження інформації з обмеженим доступом;
- Опис процедури управління санкціонуванням використання нових засобів оброблення інформації;
- Опис вимог щодо угод з третіми сторонами щодо доступу, оброблення, передавання або управління інформацією організації або засобами оброблення інформації, або щодо додавання продуктів чи послуг до засобів оброблення інформації.

А.7. Управління ресурсами СУІБ:

- Реестр ресурсів СУІБ;
- Опис процедури поводження із інформацією з обмеженим доступом.

Реєстр ресурсів СУІБ може складатися з набору декількох документів, зокрема документів, які створюються під час впровадження СУІБ (див. п. 4).

А.8 Безпека людських ресурсів:

- Процедура управления персоналом;
- Критерії прийому персоналу;

- Опис процедури перевірки кандидатів на прийом на роботу (за наявності);
- Опис процедури навчання прийнятих на роботу працівників вимогам щодо інформаційної безпеки;
- Опис процедури підготовки посадових інструкцій;
- Опис дисциплінарного процесу щодо персоналу, який здійснив порушення безпеки;
- Опис процедури звільнення персоналу з точки зору припинення відповідальності, скасування прав доступу та повернення ресурсів СУІБ;
- Програма навчання персоналу.

А.9. Фізична безпека та безпека інфраструктури:

- Опис процедури фізичної безпеки банку, схема периметру фізичної безпеки;
- Опис процедури та правил пропускного режиму;
- Опис процедури захисту від зовнішніх та інфраструктурних загроз;
- Опис процедури захисту обладнання від аварій засобів життєзабезпечення (електроживлення, заземлення, тепловідведення, тощо);
- Опис процедури обслуговування обладнання;
- Опис процедури санкціонування переміщення майна за межі банку.

А.10 Управління комунікаціями та функціонуванням:

- Опис процедур управління змінами у засобах оброблення інформації та телекомунікаційних мережах;
- Опис процедур розроблення, тестування, впровадження та експлуатації програмно-технічних комплексів/ресурсів СУІБ;
- Опис процедур моніторингу, перегляду та внесення змін у послугах третіх сторін;
- Опис процедур захисту від зловмисного та мобільного коду;
- Опис процедур резервного копіювання інформації;
- Опис процедур забезпечення безпеки мережі;
- Опис процедур поводження зі змінними носіями;
- Опис процедур забезпечення безпеки інформації і програмного забезпечення, якими обмінюються в організації та з третіми сторонами;
- Опис процедур виявлення несанкціонованої діяльності з оброблення інформації;
- Опис процедури синхронізації часу.

А.11 Контроль доступу:

- Опис процедури управління доступом користувачів (реєстрація, надання повноважень, перегляд та скасування доступу);
- Опис процедури управління паролем користувача;
- Опис процедури контролю доступу до мережі та автентифікації користувача;

- Опис процедури захисту підключень до мережі (в тому числі зовнішніх та віддалених підключень);
- Опис заходів безпеки щодо маршрутизації в мережі;
- Опис заходів контролю доступу до операційної системи;
- Опис заходів контролю доступу до програмно-технічних комплексів;
- Опис процедури дистанційної роботи.

А.12 Придбання, розроблення та підтримка інформаційних систем:

- Опис процедур внутрішньої безпеки під час обробки інформації в програмно-технічних комплексах (захист баз даних, цілісність даних під час передавання та зберігання, тощо);
- Опис процедур криптографічного захисту інформації;
- Опис процедур управління ключової інформацією;
- Опис процедури забезпечення цілісності програмного забезпечення та системних файлів;
- Опис процедури запобігання можливості витоку інформації;
- Опис вимог щодо аутсорсінгового розроблення програмного забезпечення;

А.13 Управління інцидентами інформаційної безпеки:

- Опис процедури управління інцидентами інформаційної безпеки (звітування, аналіз, вжиття коригувальних дій).

А.14 Управління безперервністю бізнесу:

- Опис дій в разі виникнення нестандартних ситуацій;
- Опис процедури тестування, підтримування та коригування планів безперервності бізнесу.

А.15 Відповідність:

- Опис процедури моніторингу законодавства та нормативних документів з питань інформаційної безпеки;
- Опис процедури внесення змін до документів;
- Опис процедури захисту організаційних записів від втрати, знищення та фальсифікації;
- Опис процедури перевірки програмно-технічних комплексів на відповідність впровадженим заходам безпеки.

Описаний перечень документів середнього рівня не може розглядатися як обов’язковий, він може доповнюватися в залежності від організації робіт в банку. Деякі документи можуть об’єднуватися, але в такому випадку слід чітко визначити відповідні розділи в загальному документі, які відповідають визначеним напрямкам питань інформаційної безпеки.

Наведені вище документи в більшості банків вже існують. Рекомендується переглянути наявні документи з точки зору повноти відображення та виконання вимог, що міститься в стандартах Національного банку України і в разі необхідності доопрацювати. Рекомендується також переглянути структуру наявних документів відповідно до вимог пункту 7.6.

7.5. Документи нижнього рівня

Документи нижнього рівня можна поділити на дві групи.

Перша група включає записи різного типу, які вимагаються стандартами. Це журнали реєстрації різних подій (наприклад, реєстрації несправностей обладнання), журнали аудиту різних систем (операційної, прикладних програм, надання доступу до ресурсів мережі Інтернет тощо). Частина цих записів ведеться автоматично і потрібно забезпечити їх збереження та захист від знищення та несанкціонованої модифікації.

Друга група документів нижнього рівня містить інструкції (пам'ятки) по виконанню тих чи інших операцій щодо інформаційної безпеки і призначена для кінцевих користувачів. При правильному підході до їх створення ці документи є ефективним інструментом зменшення ризиків, пов'язаних з людським фактором.

7.6. Рекомендації щодо оформлення документів

Під час перегляду існуючих документів та підготовки нових та доопрацьованих документів рекомендується всі необхідні документи формувати за єдиними правилами. Це надасть можливість більш чіткого та короткого викладення цих документів та більшого розуміння їх користувачами.

Рекомендована структура документів відповідно до міжнародних стандартів наведена у додатку 8.

На титульному листі необхідно надати назву банку та назву документу, а також дату його затвердження.

У розділі "Вступ" надати короткий опис документу – 1-2 речення.

У розділі "Терміни та скорочення" надати визначення термінів та скорочень, які використовуються в цьому документі.

У розділі "Ціль документа" коротко описати цілі цього документа та очікувані результати застосування цього документа з точки зору інформаційної безпеки.

У розділі "Сфера застосування" описати сферу застосування та надати перелік організаційних структур банку, які охоплюються цим документом.

У розділі "Предмет документу та опис дій" описати принципи, які застосовуються для досягнення цілій документу, розподіл обов'язків та терміни виконання за необхідністю.

У розділі "Ролі та відповідальності" описуються ролі та відповідальності персоналу банку під час виконання дій, пов'язаних з принципами та сферою застосування цього документа.

У розділі "Перегляд документа" описуються принципи перегляду та оновлення документа, а також ситуації, які потребують обов'язкового перегляду цього документу.

У розділі "Перелік взаємопов'язаних документів" надається перелік документів, на які зустрічаються посилання в цьому документі, та інструкції і

пам’ятки, які докладно описуються дії, що повинні виконуватися для досягнення цілій цього документу.

У розділі “Історія змін” надається таблиця внесення змін (додаток 8), яка заповнюється після внесення змін до документу. Внесення змін може бути зроблено, наприклад, у разі змін в організаційної структурі банку, перерозподілу ролей та відповідальностей тощо. У разі суттєвих змін у технології або принципах, які застосовуються для досягнення цілій документу, рекомендується підготувати нову версію документу.

Серед загальних рекомендацій щодо формування документів можна виділити такі:

- усі документи формувати у єдиному стилі;
- документи повинні бути простими для розуміння та максимально короткими;
- для спрощення розуміння рекомендується використовувати блок-схеми, рисунки, таблиці;
- за можливістю рекомендується поєднати загальні правила для користувачів в одному документі;
- рекомендується відображати вимоги з інформаційної безпеки в посадових інструкціях;
- в залежності від технології документообігу банку слід вибирати найбільш оптимальний варіант поширення документів в електронному або паперовому вигляді. При використанні електронних документів слід забезпечити їх цілісність протягом усього періоду використання;
- рекомендується постійно переглядати перелік документації з метою його оптимізації та зменшення обсягу конкретних документів;
- рекомендується створювати журнали для записів тільки там, де цього потребують стандарти та існуючі правила бізнесу. За можливістю рекомендується автоматизувати процедуру ведення журналів.

8. Впровадження та функціонування СУІБ

Впровадження та функціонування СУІБ потребує не тільки діяльності, пов’язаної із впровадженням заходів безпеки, а також специфічної діяльності для підтримки функціонування СУІБ в подальшому.

За результатами діяльності, яка описана у попередніх розділах, створюється політика управління інформаційною безпекою, де визначаються основні види діяльності щодо впровадження та функціонування СУІБ з посиланнями на всі документи нижчого рівня (окремі політики, процедури, методики, інструкції). У цій політиці управління інформаційною безпекою повинні бути також визначені процедури та строки виконання специфічних для функціонування СУІБ видів діяльності, а саме:

- моніторинг функціонування СУІБ;

- вимірювання ефективності СУІБ;
- внутрішній аудит СУІБ;
- навчання та тренінг персоналу;
- управління інцидентами інформаційної безпеки;
- перегляд СУІБ керівництвом банку;
- корегуючі та запобіжні дії.

Діяльність щодо супроводження керівництвом впровадження та функціонування СУІБ повинна розпочинатися і бути регламентованою на початкових стадіях впровадження СУІБ.

Процедура моніторингу повинна бути описана та погоджена керівництвом банку і має бути спрямована на досягнення таких цілей:

- терміново виявляти помилки;
- терміново ідентифікувати вдалі та невдалі спроби порушень безпеки і інциденти безпеки;
- надати можливість керівництву банку встановити, чи є діяльність щодо безпеки очікувано продуктивною;
- сприяти своєчасному виявленню подій безпеки і, таким чином, запобігати інцидентам безпеки, використовуючи відповідні показники;
- встановити, чи були ефективними дії, вжиті для усунення порушення безпеки;
- оцінювати ефективність СУІБ відповідно до розробленої методики вимірювань ефективності;
- у заплановані терміни переглядати оцінки ризиків, а також залишкові ризики та визначені прийнятні рівні ризиків, враховуючи зміни в структурі банку, бізнес-процесах, технології операційної роботи, ідентифікованих загрозах, змінах в законодавстві та регуляторних актах тощо.

Банк повинен мати процедуру реєстрації та оброблення **інцидентів інформаційної безпеки**, де докладно описані дії користувачів і керівництва щодо інформування, оброблення та усунення інцидентів інформаційної безпеки в банку.

Банк повинен в заплановані терміни проводити **внутрішні аудити СУІБ** для встановлення чи цілі заходів безпеки, заходи безпеки, процеси та процедури СУІБ відповідають вимогам з інформаційної безпеки, стандартам Національного банку України, законодавству та нормативно-правовим актам Національного банку України, є ефективно впровадженими та підтримуваними.

Програма аудиту повинна плануватися з урахуванням статусу і важливості бізнес-процесів, а також результатів попередніх аудитів. Повинні бути визначені критерії, сфера застосування, частота і методи аудиту. Відбір аудиторів і проведення аудитів повинні забезпечувати об’єктивність і неупередженість процесу аудиту. Аудитори не повинні проводити аудит своєї власної роботи. У разі відсутності власного підрозділу з аудиту інформаційної безпеки для проведення аудиту повинні долучатися зовнішні аудитори.

Спеціалісти з питань інформаційної безпеки можуть виконувати лише аудит персоналу на перевірку виконання усіх вимог та процедур інформаційної безпеки.

Відповідальності та вимоги до планування і проведення аудитів, а також звітування про результати повинні бути визначені в задокументованій процедурі.

Керівництво банку повинне здійснювати **перегляд СУІБ** у заплановані терміни (не менш одного разу на рік). Цей перегляд повинен містити оцінку можливостей вдосконалення і потреби внесення змін у СУІБ, уключаючи зміни в політиці інформаційної безпеки і цілях інформаційної безпеки. Процедура перегляду СУІБ з боку керівництва повинна бути чітко задокументована і містити перелік вхідних даних для перегляду з боку керівництва, зокрема: результати аудитів СУІБ; методи, продукти або процедури, які можуть використовуватися для вдосконалення продуктивності та ефективності СУІБ; звіти про інциденти інформаційної безпеки за попередній період; вразливості або загрози, які не були адекватно враховані в попередній оцінці ризиків; результати вимірів ефективності СУІБ; будь-які зміни, що можуть мати вплив на СУІБ; рекомендації щодо вдосконалення. В результаті перегляду СУІБ з боку керівництва банку мають бути прийняти рішення щодо вдосконалення ефективності СУІБ, оновлення оцінки ризиків та плану оброблення ризиків, модифікації та, за необхідності, процедур і заходів безпеки.

Керівництво банку має забезпечувати поінформованість персоналу з питань інформаційної безпеки за допомогою відповідних **програм навчання та тренінгів** персоналу, що повинно допомогти персоналу зрозуміти значення та важливість діяльності із забезпечення інформаційної безпеки. У великих банках рекомендується організовувати окремі тренінги з питань інформаційної безпеки, які відносяться до певних або набору бізнес-процесів/банківських продуктів/ програмно-технічних комплексів.

Функціонування СУІБ повинно постійно супроводжуватися підвищенням ефективності СУІБ шляхом використання політики інформаційної безпеки, цілей інформаційної безпеки, результатів аудитів, аналізу подій, що підлягають моніторингу, коригувальних і запобіжних дій та перегляду з боку керівництва.

Банк має здійснювати дії для усунення причин невідповідностей вимогам СУІБ, щоб запобігати їх повторенню. Задокументована **процедура коригувальних дій** повинна визначати вимоги до ідентифікації та встановлення причин невідповідностей; оцінювання потреби у діях для усунення невідповідностей; встановлення та впровадження потрібних коригувальних дій.

Банк повинен визначити дії для усунення причини потенційних невідповідностей вимогам СУІБ для запобігання їх появі. Здійснені запобіжні дії повинні відповідати величині впливу потенційних проблем. Задокументована **процедура запобіжних дій** повинна визначити вимоги до ідентифікації потенційних невідповідностей та їх причин; оцінювання потреби

в діях для запобігання виникненню невідповідностей; визначення та впровадження необхідних запобіжних дій. Пріоритети запобіжних дій повинні бути встановлені на основі результатів оцінки ризику.

Директор Департаменту інформатизації А.С.Савченко

Додаток 1

Приклади типових загроз

Загрози можуть бути навмисними (Н), випадковими (В), природними (П) і можуть бути результатом втрати будь-яких сервісів. У таблиці наведений перелік типових загроз із наданням джерела загроз. Цей перелік не може вважатися вичерпним і може бути доповненим або скороченим.

Загроза	*Джерело*	*Тип*
Фізичне пошкодження/втрата будівлі/обладнання/інформації	Пожежа	В, Н, П
	Пошкодження водою/повінь	В, Н, П
	Техногенна аварія	В, Н
	Крадіжка	В, Н, П
	Тероризм	В, Н
	Масові заворушення, політична нестабільність	В, Н
	Кліматичні та метеорологічні явища	П
	Сейсмічні загрози	П
	Електромагнітна радіація	В, Н
	Неконтрольований ремонт	В, Н
Часткове/повне пошкодження /втрата обладнання/даних	Неефективність системи клімат-контролю або водопостачання	В, Н
	Збої електроживлення	В, Н, П
	Недбалість персоналу	В, Н
	Відмова телекомунікаційного обладнання	В, Н
	Порушення експлуатації обладнання/програмного забезпечення	В, Н
	Неавторизоване використання обладнання/програмного забезпечення	В, Н
	Збої обладнання/програмного забезпечення	В, Н
	Неправильне використання обладнання/програмного забезпечення	В, Н
	Віддалений шпіонаж	Н
	Перехоплення побічних електромагнітних сигналів	Н
	Підслуховування	Н
	Відновлення середовища, що повторно використовується або викинуто	Н

Компрометація інформації	Розкриття/продаж інформації працівниками банку	В, Н
	Підробка обладнання/програмного забезпечення	Н
	Шахрайське копіювання даних	Н
	Нелегальне оброблення даних	Н
	Помилка/недбалість персоналу під час оброблення даних	В, Н
	Зловживання працівником правами доступу до інформації	Н
	Підробка прав доступу до інформації	Н
	Отримання несанкціонованого доступу до інформації зовнішніми зловмисниками	Н
	Неправильна робота системи захисту інформації	В, Н
	Навмисне невикористання системи захисту інформації	Н
	Компрометація паролів доступу	В, Н
	Компрометація ключів криптографічного захисту інформації	В, Н
Викривлення/підробка інформації/даних	Помилки програмного забезпечення	В, Н
	Неправильна робота системи захисту інформації	В, Н
	Компрометація/передача особистих ключів електронного цифрового підпису	В, Н

Особливу увагу слід звернути на людські джерела загроз, які можуть мати різну мотивацію від політичних причин до простого самоствердження. Найбільш вірогідними та найбільш серйозними можна вважати загрози від власних працівників банку, в тому числі ті загрози, які можуть виникати від недостатньої обізнаності персоналу в питаннях інформаційної безпеки. Приклади таких загроз наведені нижче у таблиці.

Джерело загрози	*Загроза*
Хакери, кракери	• Хакерські дії • Соціальна інженерія • Втручання до системи, злом • Неавторизований доступ до системи
Комп’ютерні злочинці	• Комп’ютерні злочини

	• Шахрайські дії • Продаж інформації • Спуфінг • Втручання до системи • Руйнування інформаційної системи
Тероризм	• Бомба/тероризм • Інформаційна війна • Атаки на систему (наприклад, розподілена відмова в обслуговуванні) • Підробка системи • Фінансування терористичних організацій
Дії конкурентів	• Політична перевага • Економічні дії • Крадіжка інформації • Вручання в особисте життя • Соціальна інженерія • Проникнення до системи • Неавторизований доступ до системи
Персонал	• Напад на персонал • «Чорна пошта» • Перегляд інформації з обмеженим доступом • Комп’ютерні зловживання • Шахрайство і крадіжка • Продаж інформації • Фальсифікація та підробка даних • Перехоплення • Зловмисні коди (віруси, логічні бомби, троянські коні, тощо) • Продаж персональної інформації • Дефекти системи • Втручання до системи • Системний саботаж • Неавторизований доступ до системи

Додаток 2

Приклади вразливостей, які можуть бути використані для реалізації відповідних загроз

У таблиці наведений перелік типових загроз з наданням вразливостей, які можуть бути використані для реалізації відповідних загроз. Цей перелік не може вважатися вичерпним і може бути доповненим або скороченим.

Приклади загроз	*Приклади вразливостей*
Фізичне пошкодження/втрата будівлі/обладнання/інформації від пожежі	• Відсутність пожежної сигналізації • Відсутність системи пожежогасіння • Дозвіл на паління в приміщенні • Наявність легкозаймистих матеріалів • Неякісна електропроводка • Відсутність захисту від блискавки • Неконтрольований ремонт • Наявність зловмисного підпалювача • Халатність персоналу • Необізнаність персоналу • Злочинні дії
Фізичне пошкодження/втрата будівлі/обладнання/інформації від пошкодження водою/повінню	• Невдале розташування будівлі • Невдале розміщення обладнання у підвальному приміщенні /на перших поверхах будівлі • Приміщення банку в аварійному стані • Неякісна каналізаційна система
Фізичне пошкодження/втрата будівлі/обладнання/інформації від техногенної аварії	• Наявність будівництва поряд • Старе приміщення банку (в аварійному стані) • Неякісна каналізаційна система • Відсутність контролю системи електроживлення • Відсутність резервних джерел електроживлення • Відсутність резервних каналів зв’язку • Відсутність резервного обладнання • Відсутність віддаленого резервного пункту
Фізичне пошкодження/втрата обладнання/інформації від крадіжки	• Неефективна система охорони • Недостатній контроль за переміщенням майна за межі банку

	• Недбалість персоналу • Неправильний підбор персоналу • Необізнаність персоналу • Відсутність резервного обладнання/ програмного забезпечення
Фізичне пошкодження/втрата будівлі/обладнання/інформації від тероризму	• Відсутність інструкції стосовно дій у надзвичайних ситуаціях • Неефективна система охорони • Неправильний підбор персоналу • Відсутність резервного обладнання/ програмного забезпечення
Фізичне пошкодження/втрата будівлі/обладнання/інформації від масових заворушень, політичної нестабільності	• Відсутність інструкції стосовно дій у надзвичайних ситуаціях • Неефективна система охорони • Неправильний підбор персоналу • Відсутність резервного обладнання/ програмного забезпечення • Відсутність віддаленого резервного пункту
Фізичне пошкодження/втрата будівлі/обладнання/інформації від кліматичних та метеорологічних явищ	• Старе приміщення банку (в аварійному стані) • Неякісна каналізаційна система • Відсутність контролю системи електроживлення • Відсутність резервних джерел електроживлення • Відсутність резервних каналів зв’язку • Відсутність резервного обладнання • Відсутність віддаленого резервного пункту
Фізичне пошкодження/втрата будівлі/обладнання/інформації від сейсмічних загроз	• Старе приміщення банку (в аварійному стані) • Неякісна каналізаційна система • Відсутність контролю системи електроживлення • Відсутність резервних джерел електроживлення • Відсутність резервних каналів зв’язку • Відсутність резервного обладнання • Відсутність віддаленого резервного пункту
Фізичне пошкодження/втрата обладнання/інформації від	• Відсутність екранування серверного приміщення

електромагнітної радіації	• Чутливість обладнання до електромагнітної радіації • Неефективна охорона
Фізичне пошкодження/втрата обладнання/інформації від неконтрольованого ремонту	• Відсутність належного контролю за працівниками третіх сторін • Відсутність вимог з інформаційної безпеки в угодах з третіми сторонами • Відсутність резервних джерел електроживлення • Відсутність резервних каналів зв'язку • Відсутність резервного обладнання
Часткове/повне пошкодження /втрата обладнання/даних від неефективності системи кліматконтролю або водопостачання	• Неправильний розрахунок потужності обладнання для відведення тепла • Відсутність або недостатність вимог з інформаційної безпеки в угодах з третіми сторонами • Неефективне обслуговування обладнання працівниками третіх сторін або персоналом банку • Відсутність належного контролю та моніторингу обладнання
Часткове/повне пошкодження /втрата обладнання/даних від збоїв електроживлення	• Неправильний розрахунок необхідної потужності електроживлення • Відсутність контролю та моніторингу системи електроживлення • Відсутність резервних джерел електроживлення • Відсутність резервного обладнання • Відсутність або недостатність вимог з інформаційної безпеки в угодах з третіми сторонами • Неефективне обслуговування обладнання працівниками третіх сторін або персоналом банку
Часткове/повне пошкодження /втрата обладнання/даних від недбалості персоналу	• Недосвідченість персоналу • Відсутність системи моніторингу роботи IT інфраструктури • Недосконала IT система • Неефективна охорона • Відсутність контролю за переміщенням майна банку • Відсутність або недостатність тестування обладнання/програмного

	забезпечення • Можливість використання обладнання/програмного забезпечення не за призначенням • Неефективне розмежування прав доступу до програмного забезпечення/даних • Недостатня захищеність вузла доступу до загальних мереж (наприклад, інтернет) від зовнішніх зловмисників • Недостатньо ефективна система розподілу прав доступу до інформації • Відсутність “logout” під залишення працівником робочої станції • Передача/втрата контролю за носіями криптографічних ключів • Передача/компрометація паролів доступу • Передача або повторне використання середовища збереження даних без відповідного знищення інформації • Невиконання процедур резервного копіювання інформації • Незахищене зберігання даних/ документів • Неконтрольоване копіювання інформації
Часткове/повне пошкодження /втрата даних від відмови телекомунікаційного обладнання	• Відсутність резервних каналів зв’язку • Відсутність резервного телекомунікаційного обладнання • Недбалість персоналу • Необізнаність персоналу • Відсутність або недостатність вимог безпеки в угодах з провайдерами зв’язку • Зловмисні дії персоналу провайдерів зв’язку • Погане з’єднання та розміщення кабелів • Наявність єдиної точки відмови
Часткове/повне пошкодження /втрата даних від порушення експлуатації обладнання/ програмного забезпечення	• Необізнаність персоналу • Відсутність системи моніторингу роботи IT інфраструктури • Недосконала IT система • Ускладнений інтерфейс користувача • Відсутність документації

	• Недосконале або нове програмне забезпечення • Відсутність або недостатність тестування обладнання/програмного забезпечення • Відсутність перевірки цілісності програмного забезпечення під час його запуску • Можливість використання обладнання/програмного забезпечення не за призначенням • Неефективне розмежування прав доступу до програмного забезпечення/даних • Наявність єдиної точки відмови
Часткове/повне пошкодження /втрата даних від неавторизованого використання обладнання/програмного забезпечення	• Відсутність контролю за використанням обладнання/програмного забезпечення • Відсутність контролю за внесенням змін до складу обладнання/програмного забезпечення • Наявність незахищеного з'єднання з публічними мережами • Відсутність політик використання обладнання/програмного забезпечення • Неефективне розмежування прав доступу до програмного забезпечення/обладнання • Неефективна політика управління мережею
Часткове/повне пошкодження /втрата даних від збою обладнання/програмного забезпечення	• Відсутність плану забезпечення безперервної роботи • Необізнаність персоналу • Відсутність системи моніторингу роботи IT інфраструктури • Недосконале або нове програмне забезпечення • Відсутність контролю цілісності програмного забезпечення під час його запуску • Відсутність або недостатність тестування обладнання/програмного забезпечення • Можливість використання

	обладнання/програмного забезпечення не за призначенням • Неефективне розмежування прав доступу до програмного забезпечення/даних • Наявність єдиної точки відмови • Відсутність або недосконаліть системи резервного копіювання інформації • Відсутність резервного обладнання • Неадекватне реагування для підтримки сервісів • Відсутність або недосконаліть угоди про рівень обслуговування третіми сторонами
Часткове/повне пошкодження /втрата даних від неправильного використання обладнання/ програмного забезпечення	• Необізнаність персоналу • Відсутність системи моніторингу роботи IT інфраструктури • Недосконала IT система • Ускладнений інтерфейс користувача • Відсутність документації • Недосконале або нове програмне забезпечення • Відсутність або недостатність тестування обладнання/програмного забезпечення • Можливість використання обладнання/програмного забезпечення не за призначенням • Неефективне розмежування прав доступу до програмного забезпечення/даних • Відсутність або недосконаліть системи резервного копіювання інформації • Відсутність резервного обладнання • Неадекватне реагування для підтримки сервісів
Компрометація інформації за допомогою віддаленого шпіонажу	• Небезпечна архітектура мережі • Відсутність або неефективність ідентифікації та аутентифікації користувача • Передавання паролів у відкритому вигляді • Незахищене з’єднання з публічними

	мережами • Недостатній контроль за функціонуванням та управлінням мережею • Недостатня обізнаність персоналу у питаннях інформаційної безпеки
Компрометація інформації за допомогою перехоплення побічних електромагнітних сигналів	• Відсутність екранування серверної кімнати • Неефективна охорона та пропускний режим для відвідувачів
Компрометація інформації за допомогою підслуховування	• Наявність незахищених комунікаційних ліній • Відсутність процедури безпечного проведення нарад • Наявність незахищеного конфіденційного трафіку • Необізнаність персоналу
Компрометація інформації за допомогою відновлення середовища, що повторно використовується або викинуто	• Відсутність процедури знищення інформації • Необізнаність персоналу • Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки
Компрометація інформації за допомогою розкриття/продажу інформації працівниками банку	• Неправильний підбір персоналу • Необізнаність персоналу у питаннях інформаційної безпеки • Відсутність класифікації інформації • Відсутність затвердженої процедури поводження з інформацією з обмеженим доступом • Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки • Незахищене з’єднання з публічними мережами • Відсутність контролю за роботою електронної пошти • Відсутність або неефективність ідентифікації та аутентифікації користувача • Недостатній контроль за функціонуванням та управлінням мережею

	• Неефективне розмежування прав доступу до програмного забезпечення/даних
Компрометація інформації за допомогою підробки обладнання/програмного забезпечення	• Відсутність або неефективність процедури контролю вводу нового програмного забезпечення/обладнання • Неправильний підбір персоналу • Відсутність або неефективність ідентифікації та аутентифікації користувача • Недостатній контроль за функціонуванням та управлінням мережею • Неефективне розмежування прав доступу до програмного забезпечення/даних • Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки
Компрометація інформації за допомогою шахрайського копіювання даних	• Неправильний підбір персоналу • Відсутність або неефективність ідентифікації та аутентифікації користувача • Недостатній контроль за функціонуванням та управлінням мережею • Неефективне розмежування прав доступу до програмного забезпечення/даних • Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки • Відсутність ефективної процедури моніторингу дій користувачів • Відсутність записів про роботу користувачів в журналах аудиту
Компрометація інформації за допомогою нелегального оброблення даних	• Неправильний підбір персоналу • Відсутність або неефективність ідентифікації та аутентифікації користувача • Доступність сервісів, в яких немає необхідності • Недостатній контроль за

	функціонуванням та управлінням мережею • Неефективне розмежування прав доступу до програмного забезпечення/даних • Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки • Відсутність ефективної процедури моніторингу дій користувачів • Відсутність записів про роботу користувачів в журналах аудиту
Компрометація інформації за рахунок помилки/недбалості персоналу під час оброблення даних	• Необізнаність персоналу • Відсутність або неефективність навчання персоналу • Ускладнений інтерфейс користувача • Доступність сервісів, в яких немає необхідності • Відсутність документації • Неефективне розмежування прав доступу до програмного забезпечення/даних • Відсутність ефективної процедури моніторингу дій користувачів • Відсутність записів про роботу користувачів в журналах аудиту Підробка програмного забезпечення
Компрометація інформації за рахунок зловживання працівником правами доступу до інформації	• Неправильний підбір персоналу • Відсутність або неефективність ідентифікації та аутентифікації користувача • Доступність сервісів, в яких немає необхідності • Відсутність формальної процедури реєстрації та відміни реєстрації прав доступу користувача • Відсутність формальної процедури перегляду прав доступу користувачів • Неефективне розмежування прав доступу до програмного забезпечення/даних • Відсутність або неефективність процедур контролю прав доступу

	• Відсутність регулярних аудитів • Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки • Відсутність ефективної процедури моніторингу дій користувачів • Відсутність записів про роботу користувачів в журналах аудиту
Компрометація інформації за рахунок підробки прав доступу до інформації	• Неправильний підбір персоналу • Відсутність або неефективність ідентифікації та аутентифікації користувача • Доступність сервісів, в яких немає необхідності • Наявність незахищених таблиць паролів • Недосконале управління паролями доступу • Неправильні параметри інсталяції програмного забезпечення • Недосконале програмне забезпечення • Відсутність формальної процедури реєстрації та відміни реєстрації прав доступу користувача • Відсутність формальної процедури перегляду прав доступу користувачів • Неефективне розмежування прав доступу до програмного забезпечення/даних • Відсутність або неефективність процедур контролю прав доступу • Відсутність регулярних аудитів • Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки • Відсутність ефективної процедури моніторингу дій користувачів • Відсутність записів про роботу користувачів в журналах аудиту
Компрометація інформації за рахунок отримання несанкціонованого доступу до інформації зовнішніми зловмисниками	• Небезпечна архітектура мережі • Відсутність або неефективність ідентифікації та аутентифікації користувача • Передавання паролів у відкритому

	вигляді • Незахищене з'єднання з публічними мережами • Відсутність або недостатність вимог з інформаційної безпеки з клієнтами та/або третіми сторонами • Недостатній контроль за функціонуванням та управлінням мережею/програмним забезпеченням • Відсутність ефективної процедури моніторингу дій користувачів • Відсутність записів про роботу користувачів в журналах аудиту • Недостатня обізнаність персоналу у питаннях інформаційної безпеки
Компрометація інформації за рахунок неправильної роботи системи захисту інформації	• Помилки під час проектування та розроблення системи захисту інформації • Відсутність документації • Необізнаність персоналу • Відсутність або неефективність навчання персоналу • Ускладнений інтерфейс користувача • Відсутність контролю цілісності системи захисту інформації під час її запуску/ініціалізації • Відсутність записів про роботу системи захисту в журналах аудиту
Компрометація інформації за рахунок навмисного невикористання системи захисту інформації	• Помилки під час проектування та розроблення системи захисту інформації • Відсутність записів про роботу системи захисту в журналах аудиту • Неправильний підбір персоналу • Відсутність регулярних аудитів • Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки
Компрометація інформації за рахунок компрометації паролів доступу	• Необізнаність персоналу • Порушення персоналом правил зберігання паролів • Доступність сервісів, в яких немає необхідності • Наявність незахищених таблиць паролів • Недосконале управління паролями

	доступу • Відсутність формальної процедури перегляду прав доступу користувачів • Неефективне розмежування прав доступу до програмного забезпечення/даних • Відсутність або неефективність процедур контролю прав доступу • Відсутність регулярних аудитів • Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки • Відсутність ефективної процедури моніторингу дій користувачів • Відсутність записів про роботу користувачів в журналах аудиту
Компрометація інформації за рахунок компрометації ключів криптографічного захисту інформації	• Помилки під час проектування та розроблення системи захисту інформації • Помилки під час генерації ключів, в тому числі генерація ключів без паролю • Неефективна процедура розповсюдження ключів • Відсутність документів стосовно поводження з криптографічними ключами для користувачів • Відсутність записів про роботу системи захисту в журналах аудиту • Відсутність регулярних аудитів • Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки
Викривлення/підробка інформації/даних за рахунок помилок програмного забезпечення	• Помилки під час проектування та розроблення програмного забезпечення в питаннях використання системи криптографічного захисту інформації • Невикористання електронного цифрового підпису для захисту цілісності електронних банківських документів • Відсутність перевірки електронного цифрового підпису під час роботи з електронними документами, які зберігаються в базах даних/сховищах

	даних/електронних архівах • Відсутність записів про роботу системи захисту в журналах аудиту • Відсутність документації • Ускладнений інтерфейс користувача
Неправильна робота системи захисту інформації	• Помилки під час проектування та розроблення системи захисту інформації • Невикористання електронного цифрового підпису для захисту цілісності електронних банківських документів • Відсутність документації • Необізнаність персоналу • Відсутність або неефективність навчання персоналу • Ускладнений інтерфейс користувача • Відсутність записів про роботу системи захисту в журналах аудиту
Компрометація/передача особистих ключів електронного цифрового підпису	• Помилки під час проектування та розроблення системи захисту інформації • Помилки під час генерації ключів, в тому числі генерація ключів без паролю • Неефективна процедура розповсюдження ключів • Відсутність документів стосовно поводження з ключами електронного цифрового підпису для користувачів • Відсутність записів про роботу системи захисту в журналах аудиту • Відсутність регулярних аудитів • Відсутність належного визначення відповідальності за інформаційну безпеку • Відсутність визначеного дисциплінарного процесу у випадку інциденту інформаційної безпеки

Додаток 3

Звіт оцінки ризиків
для бізнес-процесу/банківському продукту

_____

(назва)

1	2	3	4	5	6	7
Загальний ризик бізнес-процесу/банківського продукту						

Назви стовбців:
1 – Загроза//вразливість;
2 – Оцінка ймовірності реалізації загрози з використанням вказаної вразливості;
3 – Оцінка впливу реалізації загрози на цілісність;
4 – Оцінка впливу реалізації загрози на конфіденційність;
5 – Оцінка впливу реалізації загрози на доступність;
6 – Оцінка впливу реалізації загрози на спостережність;
7 – Рівень ризику за окремою парою загроза/вразливість.

Рівень ризику за окремою парою загроза/вразливість, яка може використовуватися для реалізації цієї загрози, визначається перемноженням *загального рівня оцінки величини наслідків* на оцінку ймовірності реалізації загрози. *Загальний рівень оцінки величини наслідків реалізації кожної пари загроза/вразливість* на сервіси безпеки визначається як **максимальна величина** з окремих оцінок впливу на цілісність, конфіденційність, доступність, спостережність.

Загальний рівень ризику для бізнес-процесу/банківського продукту дорівнює **максимальної величині** з усіх ризиків за кожною парою загроза/вразливість.

За наявності використання декількох програмно-технічних комплексів в одному бізнес-процесі/банківському продукті та різниці у системах захисту інформації слід у кожної парі загроза/вразливість вказати докладно місце виникнення загрози/вразливості. Особливу увагу слід звертати на захищеність інтерфейсів для обміну інформацією між програмно-технічними комплексами.

Якщо будь-яка вразливість для певної загрози усунена відповідними заходами безпеки, ця пара загроза/вразливість не включається до звіту оцінки ризиків, але відповідне посилання на документи з описом цих заходів безпеки повинне бути включено до Положення щодо застосовності (додаток 4)

Додаток 4

Приклад Положення щодо застосовності

1	2	3	4

Назва стовбців у таблиці:

1. Номер параграфу в додатку А до стандарту Національного банку України СОУ Н НБУ 65.1 СУІБ 1.0:2010. У разі використання додаткових заходів безпеки, які не вказані у додатку А стандарту, рекомендується надати їм свою нумерацію.
   Приклад заповнення: А.5.1.1; А.12.3
2. Позначка щодо застосовності.
   Приклади заповнення: Так; Ні; Частково
3. Посилання на відповідні документи
   Цей стовпчик заповнюється в разі значення позначки щодо застосовності: *Так* або *Частково*. Надаються назви документів (політик, правил, інструкцій тощо), які регламентують використання відповідних заходів безпеки.
   Приклад заповнення: Політика антивірусного захисту
4. Коментар
   Цей стовпчик повинен бути заповнений в обов'язковому порядку в разі значення позначки щодо застосовності: *Ні* або *Частково.* В цьому стовпчику надаються причини невикористання або часткового використання заходів безпеки або плани щодо їх використання в майбутньому з визначенням дати впровадження.

Додаток 5

Перелік документів, які повинні бути створені
під час підготовки до впровадження СУІБ в банках України

№ пункту	Зміст пункту Методичних рекомендацій	Документ
3.	**Підготовка до впровадження СУІБ**	
3.1.	Зобов'язання керівництва щодо управління інформаційною безпекою	Наказ про створення спеціального керівного органу з питань інформаційної безпеки (за необхідністю)
3.2.	Призначення відповідальних за впровадження та функціонування СУІБ	Наказ про призначення керівника проекту впровадження та функціонування СУІБ
3.3.	Визначення вимог з інформаційної безпеки для банку	Перелік законодавчих, регуляторних, нормативних вимог з інформаційної безпеки для банку
4.	**Опис існуючої інфраструктури та заходів безпеки**	
4.1.	Класифікація інформації	1. Зобов'язання працівників банку щодо збереження інформації з обмеженим доступом; 2. Перелік відомостей, що містять інформацію з обмеженим доступом; 3. Положення щодо спеціального діловодства для документів, які містять інформацію з обмеженим доступом.
4.2.	Опис критичних бізнес-процесів та програмно-технічних комплексів, які забезпечують їх функціонування	1. Перелік критичних бізнес-процесів/ банківських продуктів/ програмно-технічних комплексів; 2. Короткій опис кожного бізнес-процесу/ банківського продукту/ програмно-технічного комплексу; 3. Блок-схема зв'язків між бізнес-процесами/ банківськими продуктами/ програмно-технічними комплексами
4.3.	Опис організаційної структури банку, яка охоплюється СУІБ	Перелік організаційних структур банку, які охоплюється СУІБ
4.4.	Опис структури мережі банку	1. Положення про мережу банку; 2. Положення (політики) по різним питанням управління мережею;
4.5.	Опис фізичного середовища	1. Опис географічного та територіального розташування приміщень банку; 2. Опис принципів пропускного режиму;

		3. Наказ із визначення приміщень з обмеженим доступом та опис відповідного захисту цих приміщень із забезпеченням контролю доступу до таких приміщень; 4. Опис принципів побудови систем відео спостереження; 5. Опис системи електроживлення та заземлення; 6. Опис охоронної та пожежної сигналізації; 7. Опис умов зберігання магнітних, оптомагнітних, паперових та інших носіїв інформації, в тому числі електронних архівів.
4.6.	Опис принципів забезпечення безперервності роботи банку	План забезпечення безперервної діяльності та дій в разі виникнення надзвичайних ситуацій
5.	**Аналіз ризиків**	
5.3.	Ідентифікація загроз та вразливостей	Перелік загроз та вразливостей
6.	**Оцінка ризиків**	
6.1.	Методологія оцінювання ризиків	1. Опис методології оцінки ризиків; 2. Звіт щодо оцінки ризиків за кожним критичним бізнес-процесом./банківським продуктом
6.2.	Оброблення ризиків	1. Опис методології оброблення ризиків; 2. Документи стосовно прийняття залишкових ризиків.
6.3.	Визначення цілій додаткових заходів безпеки та плану впровадження заходів безпеки	План оброблення ризиків
6.4.	Підготовка Положення щодо застосовності	Положення щодо застосовності
7.	**Документація**	
		Документи відповідно до опису в цьому розділу
8.	**Впровадження та функціонування СУІБ**	
		1. Політика управління інформаційною безпекою; 2. Опис процедури моніторингу СУІБ; 3. Опис методики вимірювань

		ефективності СУІБ; 4. Опис процедури реєстрації та оброблення інцидентів інформаційної безпеки; 5. Опис процедури внутрішнього аудиту; 6. Програма внутрішнього аудиту; 7. Опис процедури перегляду СУІБ з боку керівництва; 8. Програма та плани навчання та тренінгів персоналу; 9. Опис процедури коригувальних дій; 10. Опис процедури запобіжних дій;

Додаток 6

Приклад Політики інформаційної безпеки

Назва банку

Затверджено
рішенням Правління банку
“___” _____ 201_ р.

Політика інформаційної безпеки

Вступ

Політика інформаційної безпеки описує та регламентує функціонування системи управління інформаційною безпекою (далі – СУІБ) відповідно до стандартів Національного банку України СОУ Н НБУ 65.1 СУІБ 1.0:2010 та СОУ Н НБУ 65.1 СУІБ 2.0:2010, відповідає вимогам законодавства України та нормативно-правовим актам Національного банку України, а також вимогам міжнародних та внутрідержавних платіжних систем та систем переказу коштів.

Ціль політики

Ціллю Політики є впровадження та ефективне функціонування системи управління інформаційною безпекою, яка буде забезпечувати захист інформації та ресурсів банку від зовнішніх і 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.

Сфера застосування

Політика розповсюджується на банк у цілому і повинна використовуватися для всіх критичних бізнес-процесів/банківських продуктів банку.

Предмет політики

Основними принципами Політики інформаційної безпеки є підтримання належного захисту інформації із забезпеченням цілісності, конфіденційності,

доступності та спостережності. Це в першу чергу стосується інформації з обмеженим доступом, яка відноситься до “банківської таємниці”, “комерційної таємниці” та іншої конфіденційної інформації.

Банк підтримує ризик-орієнтовний підхід, який забезпечує розуміння, моніторинг та зменшення ризиків операційної діяльності. Деталі ризик-орієнтовного підходу описані в політики управління інформаційною безпекою.

Весь персонал банку обізнаний та виконує вимоги інформаційної безпеки в роботі. Під час розроблення, впровадження та функціонування програмно-технічних комплексів враховуються вимоги інформаційної безпеки.

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

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

Ролі та відповідальності

Керівництво банку чітко розуміє, що інформаційна безпека банку є основою життєдіяльності банку. У банку створений та постійно працює керівний орган з питань інформаційної безпеки, рішення якого є обов’язковими для виконання усім персоналом банку.

Документи Політики інформаційної безпеки розробляються підрозділом інформаційної безпеки та іншими підрозділами за відповідними напрямками діяльності. Постійний контроль впровадження, виконання, вдосконалення та підтримки Політики в актуальному стані покладений на підрозділ інформаційної безпеки.

Керівництво банку сприяє створенню, впровадженню, контролю та підтримці Політики інформаційної безпеки.

Стратегія розвитку інформаційних технологій банку, всі проекти, які пов’язані з інформаційними технологіями, узгоджуються з Політикою інформаційної безпеки.

Кожен працівник банку забезпечує підтримку відповідного рівня інформаційної безпеки банку. В межах своїх службових обов’язків та повноважень працівники повинні виконувати та відповідати за виконання вимог Політики, законодавчих, регуляторних і внутрішньобанківських норм і несуть відповідальність за їх порушення згідно із законодавством України та внутрішньобанківськими нормативними документами.

Документи Політики доступні працівникам банку у межах їх повноважень і призначені надавати допомогу у виконанні вимог інформаційної безпеки.

Для зменшення ризиків виникнення інцидентів інформаційної безпеки керівництво банку створює працівникам умови для систематичного навчання нормам та заходам інформаційної безпеки.

У банку складаються, діють, тестуються та оновляються плани забезпечення безперебійного функціонування на випадок непередбачених критичних ситуацій.

Перегляд документа

Виконується робота щодо підтримки Політики інформаційної безпеки в актуальному стані. Політика переглядається за необхідністю, але не менш ніж одного разу на рік. Причинами внесення змін до Політики є зміни в інформаційної інфраструктурі та/або впровадженні нових інформаційних технологій, а також змінах в законодавчих, регуляторних та інших нормах.

Історія змін

Дата	Автор	Зміст змін

Керівник підрозділу
інформаційної безпеки (підпис)

Додаток 7

Перелік Законів України та нормативно-правових актів
Національного банку України, які містять вимоги інформаційної безпеки

Закони України

- Про інформацію
- Про захист інформації в інформаційно-телекомунікаційних системах
- Про електронні документи та електронний документообіг
- Про електронний цифровий підпис
- Про захист персональних даних
- Про Національний банк України
- Про банки і банківську діяльність
- Кодекс України про адміністративні правопорушення
- Кримінальний кодекс України
- Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму

Нормативно-правові акти Національного банку України

- Інструкція про безготівкові розрахунки в Україні в національної валюті, затверджена постановою Правління Національного банку України від 21.01.2004 № 22 (зі змінами), зареєстрована в Міністерстві юстиції України 05.05.2005 за № 469/10749.
- Інструкція про міжбанківський переказ коштів в Україні в національній валюті, затверджена постановою Правління Національного банку України від 16.08.2006 № 320, зареєстрована в Міністерстві юстиції України 06.09.2006 за № 1035/12909.
- Положення про організацію операційної діяльності в банках України, затверджене постановою Правління Національного банку України від 18.06.2003 № 254, зареєстроване в Міністерстві юстиції України 08.07.2003 за № 559/7880 (зі змінами).
- Положення про забезпечення безперервного функціонування інформаційних систем Національного банку та банків України, затверджене постановою Правління Національного банку України від 17.06.2004 № 265.
- Перелік документів, що утворюються в діяльності Національного банку та банків України із зазначенням строків зберігання, затверджений постановою Правління Національного банку України від 08.12.2004 № 601
- Положення про порядок формування, зберігання та знищення електронних архівів у Національному банку України і банках України, затверджене постановою Правління Національного банку України від

12.09.2006 № 357, зареєстроване в Міністерстві юстиції України 03.10.2006 за № 1089/12963.

- Правила зберігання, захисту, використання та розкриття банківської таємниці, затверджені постановою Правління Національного банку України від 14.07.2006 № 267, зареєстровані в Міністерстві юстиції України 03.08. 2006 за № 935/12809
- Положення про здійснення банками фінансового моніторингу, затверджене постановою Правління Національного банку України від 14.05.2003 №189, зареєстроване в Міністерстві юстиції України 19.11.2004 за № 1062/8383 (зі змінами).
- Положення про діяльність в Україні внутрішньодержавних і міжнародних платіжних систем, затверджене постановою Правління Національного банку України від 25.09.2007 № 348, зареєстроване в Міністерстві юстиції України 15.10. 2007 за № 1173/14440 (зі змінами)
- Правила організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України, затверджені постановою Правління Національного банку України від 02.04.2007, № 112, зареєстровані в Міністерстві юстиції України 24.04.07 за № 419/13686.
- Правила технічного захисту приміщень банків, у яких обробляються електронні банківські документи, затверджені постановою Правління Національного банку України від 04.07.2007 № 243, зареєстровані в Міністерстві юстиції України 17.08.2007 за № 955/14222 .
- Постанова Правління Національного банку України "Про затвердження нормативно-правових актів з питань функціонування електронного цифрового підпису в банківській системі України" від 04.06.2010 № 284, зареєстрована в Міністерстві юстиції України 04.11.2010 за № 1034/18329
- Правила реєстрації, засвідчення чинності відкритого ключа та акредитації центрів сертифікації ключів банків України в Засвідчувальному центрі Національного банку України, зареєстровані в Міністерстві юстиції України 04.11.2010 за № 1035/18330
- Правила оформлення Регламенту роботи центрів сертифікації ключів банків України, зареєстровані в Міністерстві юстиції України 04.11.2010 за № 1036/18331

Додаток 8

Типова структура документів

Титульний лист

Вступ

Терміни та скорочення

Ціль документа

Сфера застосування

Предмет документу та опис дій

Ролі та відповідальності

Перегляд документа

Перелік взаємопов’язаних документів

Історія змін

Дата	Автор	Зміст змін