UKRSIBBANK
BNP PARIBAS GROUP

Політика інформаційної безпеки АТ "УКРСИББАНК"

(зовнішня)

ЗМІСТ

Терміни та скорочення.

Доступність - забезпечення безперервного доступу до інформаційних і супутнім активам і сервісам Банку, згідно з наданими користувачам повноваженням і правами у мінімально необхідному обсязі. Повинні бути складені плани забезпечення безперервної діяльності Банку на випадок надзвичайних ситуацій.

Конфіденційність - забезпечення доступності інформації, активів тільки для офіційно авторизованих осіб і користувачів в мінімально необхідному обсязі.

Спостережливість - забезпечення можливості визначення - хто, що і коли робив з тим чи іншим інформаційним активом Банку. Забезпечення принципу неможливості відмови від вчинених дій.

Суб'єкти - все і все, що прямо або побічно впливає і/або може впливати на об'єкти.

Цілісність - захист точності/коректності та повноти активів і методів обробки інформації.

1. Введення.

Політика інформаційної безпеки (далі - Політика) - це пакет документів, який описує і регламентує систему управління інформаційною безпекою АТ "УКРСИББАНК", відповідає вимогам законодавства України, стандартах, постановах та нормативних актів НБУ з інформаційної безпеки, ґрунтується на Політиці інформаційної безпеки BNP Paribas Group та програми CyberSecurity Program 2020, а так само на рекомендаціях міжнародних стандартів ISO/IEC 2700x, NIST та PCI DSS.

Політика регламентує впровадження та ефективне управління системою забезпечення інформаційної безпеки, спрямованої на захист інформаційних активів Банку, забезпечення безперервності діяльності Банку, мінімізації ризиків інформаційної безпеки, створення позитивної репутації Банку та довірчих відносин з клієнтами.

Основним завданням інформаційної безпеки є захист інформаційних активів Банку від зовнішніх і внутрішніх, навмисних і ненавмисних загроз.

2. Мета.

Інформування клієнтів АТ "УКРСИББАНК" (далі – Банк) щодо організації інформаційної безпеки у Банку.

3. Область застосування.

Політика поширюється на всі аспекти життєдіяльності Банку та застосовується до всіх активів Банку, які можуть негативно впливати на результати діяльності Банку своєю відсутністю чи функціонуванням з помилками.

4. Політика Банку в області інформаційної безпеки.

4.1. Класифікація активів.

Як основні об'єкти області діяльності інформаційної безпеки, розглядаються наступні види активів:

- *інформаційні активи:* інформація і дані в любому вигляді, що отримуються, оброблюються, передаються, оголошуються, у т.ч. знання працівників, партнерів Банку, бази даних та файли, документація, інструкція користувача;
- *програмне забезпечення: інформаційні системи та сервіси,* прикладне програмне забезпечення, системне програмне забезпечення, сервісне програмне забезпечення і будь-яка інше програмне забезпечення, незалежно від форми отримання (придбане, власної розробки, те, що вільно розповсюджується), що використовується у Банку працівниками та системами для роботи та взаємодії з клієнтами та іншими внутрішніми і зовнішніми системами тощо;
- *фізичні активи:* працівники, апаратні засоби IT (сервери, робочі станції, пристрої типу "тонкий клієнт", планшети, смартфони, міжмережеві екрани, принтери, копіювальні апарати, телекомунікаційне обладнання, обладнання зв'язку, маршрутизатори, комутатори, АТС, факси, модеми тощо), носії даних (стрічки, диски і т.п.), меблі, приміщення, виробниче обладнання, інші технічні засоби тощо;
- *сервісні активи:* обчислювальні і комунікаційні сервіси (Інтернет, електронна пошта, канали зв'язку і т.п.), інші технічні послуги (опалення, освітлення, енергопостачання, кондиціонування повітря, системи сигналізації та моніторингу), усі послуги, пов'язані з отриманням, наданням, використанням, передачею та знищенням активів, всі юридичні і фізичні особи, організації,

установи та підприємства (а також їх працівники), послугами яких користується Банк для отримання, використання, передачі та знищення активів.

Для кожного активу визначаються можливі ризики та шляхи їх мінімізації, використовується ризико-орієнтований підхід.

4.2. Класифікація критеріїв інформаційної безпеки.

Оцінка можливих ризиків інформаційної безпеки активів ведеться за чотирма основними критеріями безпеки - Конфіденційність, Цілісність, Доступність та Спостережливість (див. Терміни та скорочення).

4.3. Задачі Політики.

Політика регламентує:

- управління доступами;
- управління правами та повноваженнями;
- управління способами авторизації;
- чітке розподілення ролей та обов'язків;
- визначення вимог інформаційної безпеки для кожного активу;
- впровадження Політики в інформаційні системи ат сервіси;
- підтримку рівня безпеки на високому рівні;
- навчання працівників інформаційної безпеки і повідомлення клієнтів Банк про ризики інформаційної безпеки;
- проведення контролю безпеки інформаційних систем;
- управління інцидентами;
- класифікацію активів та забезпечення конфіденційності інформації;
- захист від шкідливого програмного забезпечення;
- резервне копіювання і відновлення інформації;
- ліцензійну чистоту;
- вхідний/вихідний контроль засобів обчислювальної техніки;
- забезпечення фізичної безпеки;
- контроль виконання вимог Політики та інших аспектів інформаційної безпеки.

5. Ролі та відповідальність.

Відповідно до міжнародного стандарту в області інформаційної безпеки ISO/IEC 27001, BNPP CyberSecurity Program 2020, міжнародним стандартом платіжних карт PCI DSS, галузевим стандартом інформаційної безпеки ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги у Банку з ініціативи BNP Paribas Group, вищого керівництва Банку та підрозділу контролю інформаційної безпеки Банку створений і регулярно проводиться Комітет інформаційної безпеки та IT ризиків (далі – Комітет). Діяльність Комітету регулюється у відповідності до Положення про Комітет з інформаційної безпеки та IT ризиків АТ "УКРСИББАНК". Рішення Комітету є обов'язковими для виконання всіма працівниками Банку та контрагентами в рамках договірних відносин.

Вище керівництво та керівники структурних підрозділів Банку сприяють у створенні, впровадженні, постійному контролі й супроводі Політики.

Розробка, підтримка в актуальному стані або ініціювання перегляду Політик інформаційної безпеки входить в зону відповідальності підрозділу контролю інформаційної безпеки Банку.

Рішення і рекомендації підрозділу контролю інформаційної безпеки в рамках забезпечення безпеки інформаційних активів є безперечними і обов'язковими для всіх працівників Банку.

Стратегія інформаційної безпеки Банку та Стратегія розвитку інформаційних технологій Банку та всі проекти, що пов'язані з інформаційними активами не повинні суперечити даній Політиці.

Кожен співробітник Банку або співробітник контрагента (в рамках договірних зобов'язань) бере участь в підтримці високого рівня інформаційної безпеки Банку. Необхідний рівень інформаційної безпеки визначає підрозділ інформаційної безпеки Банку. В рамках своїх посадових обов'язків і повноважень, працівники Банку або контрагентів зобов'язані:

- ознайомлюватися під підпис з Політикою інформаційної безпеки Банку та вимогами інформаційної безпеки, що зазначені у посадових інструкціях або у трудових контрактах/договорах (перед прийомом на роботу);

- дотримуватися вимог Політики, законодавчих та міжнародних норм, міжнародних стандартів в області інформаційної безпеки, вимог інформаційної безпеки BNP Paribas Group та Банку, а також несуть відповідальність за їх порушення в рамках, встановлених законодавством Україна, кримінальним кодексом України, внутрішньобанківськими нормативними документами, договорів тощо .

Документи Політики доступні усім працівникам Банку на сторінці Служби інформаційної безпеки інтрасайту Банку. Працівники Банку мають сприяти у впровадженні Політики і її документів та виконувати зазначені в них вимоги.

Для мінімізації ризиків виникнення інцидентів інформаційної безпеки через необізнаність користувачів, Банк систематично, доступними методами повідомляє про ризики інформаційної безпеки працівників, контрагентів і клієнтів Банку, навчає працівників Банку і його контрагентів нормам інформаційної безпеки, проводить тестування.

На випадок різних непередбачених критичних ситуацій і надзвичайних подій, в Банку складаються, діють, систематично тестуються і оновлюються План забезпечення безперервної діяльності Банку та План аварійного відновлення.

6. Реагування на інциденти інформаційної безпеки.

Процес реагування на інциденти інформаційної безпеки, їх виявлення та документування, оповіщення відповідальних осіб проводиться відповідно до затверджених в Банк Політикою управління операційним ризиком АТ"УКРСИББАНК", Політикою управління ризиками інформаційної безпеки АТ "УКРСИББАНК" та окремих планів реагування в залежності від типу інциденту.

Про кожен інцидент інформаційної безпеки **працівники контрагентів Банк** зобов'язані негайно повідомляти:

- безпосереднього керівника;
- відповідального за взаємодію контрагента з Банком.

Про кожний інцидент інформаційної безпеки **клієнти Банк** щодо своїх активів в Банк мають право звернутися до Банк з метою його усунення або вияснення причин виникнення.

7. Перегляд Політики.

Політика переглядається по мірі необхідності або на регулярній основі не рідше одного разу на 12 місяців.

8. Аналіз ризиків.

8.1. *Ризики комплаєнс*:

- ризик застосування штрафних санкцій з боку НБУ за недотримання вимог стандартів, постанов, нормативних актів НБУ з інформаційної безпеки.
  Дії, що дозволяють нівелювати ризик: регулярна актуалізація політики у відповідності до вимог стандартів, постанов, нормативних актів НБУ з інформаційної безпеки.
- ризик непроходження сертифікації за стандартом PCI DSS.
  Дії, що дозволяють нівелювати ризик: регулярне вивчення вимог актуальної версії стандарту PCI DSS та актуалізація політики.

7.2. *Юридичні ризики:* ризик призупинення ліцензії НБУ через порушення вимог обробки та зберігання даних.
Дії, що дозволяють нівелювати ризик: регулярна актуалізація політики у відповідності до вимог стандартів, постанов, нормативних актів НБУ з інформаційної безпеки.

7.3. *Репутаційні ризики:*ризик невідповідності політики вимогам стандартів, постанов, нормативних актів НБУ з інформаційної безпеки.
Дії, що дозволяють нівелювати ризик: регулярна актуалізація політики у відповідності до вимог стандартів, постанов, нормативних актів НБУ з інформаційної безпеки.

7.4. *Операційні ризики (включаючи інформаційні ризики):* ризик відсутності або недоліку контролю.
Дії, що дозволяють нівелювати ризик: періодичний контроль актуальності вимог.

9. Історія змін.

Автор	Дата	Версія	Історія змін
СІБ	20.11.15	4	1. Період перегляду Політики у відповідності до вимог стандарту PCI DSS (розділ 7). 2. Відповідальність працівників контрагентів Банк (розділ 6). 3. Додані міжнародні стандарти, діючі процедури.
СІБ	15.11.16	5	1. Мета документу. 2. Видалені неактуальні стандарти інформаційної безпеки або їх версії (розділ 1). 3. Зазначення: діючих документів Банк, місце розташування документів з інформаційної безпеки Банк (розділ 5). 4. Додане право клієнтів Банк повідомляти Банк про інциденти з інформаційної безпеки з їх активами у Банк (розділ 6). 5. Переклад Політики на українську мову.
СІБ	20.11.17	6	Плановий перегляд.
СІБ	20.11.18	7	1. Додані вимоги щодо ознайомлення працівників Банку/контрагентів з Політикою інформаційної безпеки під особистий підпис та визначення обов'язків щодо дотримання інформаційної безпеки у посадових інструкціях/трудових договорах/контрактах працівників Банку/контрагентів (у відповідності до п. 30 розділу IV Положення НБУ № 95 від 28 вересня 2017 року ""Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України"). 2. Зазначені чинні програми та політики Банку та Групи.