УДК 004.056:336.71

ІНФОРМАЦІЙНА БЕЗПЕКА БАНКІВСЬКИХ УСТАНОВ: НОРМАТИВНО-ПРАВОВИЙ АСПЕКТ

Лещенко С. В., здобувач вищої освіти гр. МКБп-201
Науковий керівник: **Ткач Ю. М.,** д.пед.н., професор
Національний університет «Чернігівська політехніка»

Враховуючи світові тенденції інформатизації сучасного суспільства, стрімкий розвиток інформаційних технологій та інтенсивне впровадження інформаційно-телекомунікаційних систем в усі сфери життєдіяльності держави і суспільства, постає необхідність в окресленні поняття та змісту інформаційної безпеки і системи її забезпечення в банківській сфері.

Інформаційна безпека банку – це захист інформації від широкого діапазону загроз з метою забезпечення безперервності бізнесу, мінімізації бізнес ризику і максимізації рентабельності інвестицій і бізнес можливостей. Інформаційна безпека досягається впровадженням відповідного набору заходів безпеки, які охоплюють політику, процеси, процедури, організаційні структури і програмні та апаратні функції[1, с. 78].

Не можна не погодитися з тезою, що «одним із найважливіших критеріїв функціонування банківської системи є інформаційна безпека як всієї системи, так і її частин: центрального і комерційних банків» [2, с.3].

Окреслена проблема висвітлена в наукових працях вітчизняних та зарубіжних вчених. Окремим аспектам питання в своїх роботах приділяють увагу Мігус І. П. та Лаптєв С. М. які в своїй роботі говорять про необхідність розмежування понять "загроза" та "ризик" при діагностиці економічної безпеки суб'єктів господарювання[3], Зачосова Н. В. приділяє увагу концептуальним засадам формування комплексної системи забезпечення фінансово - економічної безпеки підприємств та фінансових установ України[4], Козаченко І. П., Голубєв В. О. визначають загальні принципи захисту банківської комп'ютерної інформації[5] та інші. Проте, аналіз наукових праць показав відсутність єдиного підходу щодо формування інформаційної безпеки банківських установ.

Основи забезпечення інформаційної безпеки в банківській діяльності визначаються:

- Законом України «Про банки і банківську діяльність;
- Законом України «Про Національний банк України»;
- Законом України «Про платіжні системи та переказ коштів в Україні;
- нормативно-правовими актами Національного банку України.

Метою роботи є аналіз теоретичних засад нормативно-правового забезпечення інформаційної безпеки, визначення об`єктів інформаційної безпеки, основних підходів для реалізації інформаційної безпеки та основних загроз інформаційній безпеці установ, які відносяться до банківської сфери.

Політика управління інформаційною безпекою для банків, визначаються національними стандартами України з питань інформаційної безпеки: ДСТУ ISO/IEC 27000:2015 “Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник”, ДСТУ ISO/IEC 27001:2015 “Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги”, ДСТУ ISO/IEC 27002:2015 “Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки», які прийняті наказом від 18 грудня 2015 р. № 193 (зі змінами) Державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості», вимог внутрішніх нормативних документів банку.

При вивчені даних стандартів можна класифікувати об`єкти області діяльності системи управління інформаційної безпеки наступним чином:

Таблиця 1 - Класифікація об`єктів СУІБ

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

Проаналізувавши наведені вище ДСТУ можна виділити окремі важливі підходи щодо забезпечення інформаційної безпеки у банківських установах:

- створення та затвердження переліку відомостей, що містять інформацію з обмеженим доступом;
- створення та затвердження переліку критичних бізнес-процесів за якими проводиться оцінка ризиків інформаційної безпеки та подальша їх обробка;
- встановлення правил доступу до інформаційних ресурсів та програмно-технічних комплексів;
- забезпечення контролю фізичного та логічного доступу до всіх визначених ресурсів;
- забезпечення парольного захисту програмних та сервісних ресурсів;
- забезпечення антивірусного захисту програмних та сервісних ресурсів;
- забезпечення захисту мережі;
- забезпечення віддаленого доступу до ресурсів мережі (локальної, мережі Інтернет, мереж інших організацій);

- забезпечення ідентифікації та автентифікації всіх визначених ресурсів;
- забезпечення криптографічного захисту інформації;
- проведення внутрішніх аудитіх СУІБ та аналіз СУІБ з боку керівництва Банку;
- моніторинг та вдосконалення СУІБ.

Аналізуючи загрози інформаційній системі банківських установ можна виокремити наступні:

1) випадкові загрози: помилки, а також події, що не залежать від людини(природні явища або викликані діяльністю людини);

2) навмисні загрози: можуть реалізуватися учасниками процесу обробки інформації (копіювання і крадіжка програмного забезпечення;несанкціоноване введення даних; зміна або знищення даних на магнітних носіях; крадіжка інформації; несанкціоноване використання ресурсів комп'ютерів; несанкціоноване використання банківських автоматизованих систем; несанкціонований доступ до інформації високого рівня секретності; знищення інформації);

3) перекручення інформації: зміна її змісту, порушення її цілісності, в тому числі і часткове знищення[5, с.4].

Отже було визначено нормативно-правові акти та закони України що регулюють забезпечення інформаційної безпеки в банківських установах України. Було класифіковано область діяльності системи управління інформаційною безпекою в банківських установах за такими ознаками як інформаційні ресурси, фізичні ресурси, сервісні ресурси та програмне забезпечення що дозволить спростити процедуру вибору рішень для впровадження такої системи в банківських установах. Також визначено підходи щодо забезпечення інформаційної безпеки у банківських установах які сприятимуть спрощенню процедури реалізації конфіденційності, цілісності та доступності інформації яка циркулює в межах певної банківської установи. Визначено основні загрози які можуть спіткати банки у їхній діяльності в сфері інформаційних технологій.

Список використаних джерел

1. Напора І. Ю. Інформаційна безпека банківських установ як об’єкт наукових досліджень / І. Ю. Напора // Вісник черкаського університету. Серія: Економічні науки. – 2014. – №39 (332). - С. 77-80.

2. Пичугина П.А. Проблемы обеспечения информационной безопасности в банковских информационных системах/ П.А.Пичугина. – [Електронний ресурс]. –Режим доступу: http://www.tvvlibrary.narod.ru/papers/2011/6-11.pdf.

3. Необхідність розмежування понять "загроза" та "ризик" при діагностиці економічної безпеки суб'єктів господарювання / І. П. Мігус, С. М. Лаптєв. // Ефективна економіка. - 2011. - № 12. - Режим доступу: http://nbuv.gov.ua/UJRN/efek_2011_12_5.

4. Концептуальні засади формування комплексної системи забезпечення фінансово-економічної безпеки підприємств та фінансових установ України / Н. В. Зачосова, А. В. Шостак // Економіка та держава. - 2016. - № 7. - С. 80-83. - Режим доступу: http://nbuv.gov.ua/UJRN/ecde_2016_7_17.

5. Козаченко І.П. Загальні принципи захисту банківської комп'ютерної інформації/І.П.Козаченко, В.О.Голубєв / Центр дослідження проблем комп'ютерної злочинності. – [Електронний ресурс]. –Режим доступу: http:// www.crime-research.ru/library/Koz_gol.htm.