9. Про внесення змін до деяких законодавчих актів України щодо запобігання негативному впливу на стабільність банківської системи [Електронний ресурс] : Закон України від 04.07.2014 р. № 1586-VII. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/1586-18?nreg=1586-18&find=1&text=500+%EC%EB%ED.%E3%F0%ED&x=0&y=0.

10. Про банки і банківську діяльність [Електронний ресурс] : Закон України від 07.12.2000 р. № 2121-III. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2121-14.

11. Прес-реаліз НБУ від 12.09.2016 [Електронний ресурс] : дані Національного банку України – Режим доступу : https://bank.gov.ua/control/uk/publish/article?art_id=36329514&cat_id=55838.

12. Zielinska K. Financial Stability in the Eurozone / K. Zielinska // Comparative Economic Research, Volume 19, Number 1, 2016. – 177 p. , c. 14.

ВПРОВАДЖЕННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВСЬКИХ УСТАНОВ

IMPLEMENTATION OF INFORMATION SECURITY POLICY IN BANKING INSTITUTIONS

УДК 336.7

Кібальник Л.О.
д.е.н., доцент,
завідувач кафедри
моделювання економіки і бізнесу
Черкаський національний університет
імені Богдана Хмельницького
Напора І.Ю.
аспірант кафедри менеджменту
та економічної безпеки
Черкаський національний університет
імені Богдана Хмельницького

У статті досліджено підходи до трактування поняття «політика інформаційної безпеки». Визначено мету та основні завдання політики інформаційної безпеки банківських установ. Наведено основні об'єкти політики інформаційної безпеки банків. Розглянуто напрями щодо забезпечення інформаційної безпеки банків. Визначено ієрархічний підхід до впровадження політики інформаційної безпеки банківських установ.

Ключові слова: *банківська установа, безпека, загроза, інформаційна безпека, політика.*

В статье исследованы подходы к трактовке понятия «политика информационной безопасности». Определены цели и основные задачи политики информационной безопасности банковских учреждений. Приведены основные объекты политики информационной безопасности банков. Рассмотрены направления по обеспечению информационной безопасности банков. Определен иерархический подход к внедрению политики информационной безопасности банковских учреждений.

Ключевые слова: *банковское учреждение, безопасность, угроза, информационная безопасность, политика.*

In the article the approaches to the interpretation of the concept of "information security policy" are investigated. Goals and major tasks of the bank's information security policy are defined. The basic objects of the bank's information security policy are listed. Areas of information security procuring in banks are considered. The hierarchical approach to implementing information security policy in banks is defined.

Key words: *banking institution, security, threat, informational security, policy.*

Постановка проблеми. Актуальність питання впровадження політики інформаційної безпеки банківських установ пов'язано з швидким розвитком засобів і форм автоматизації процесів обробки інформації та високою залежністю банківської установи від інформаційних ресурсів та мереж. Відсутність у банківській установі правил і контролю щодо інформаційної безпеки викликає проблеми з ефективністю її функціонування. Важливим є побудова ефективної політики інформаційної безпеки, адже через недостатню увагу до інформаційної безпеки відбувається витік інформації, що в свою чергу призводить до значних фінансових збитків та втрати довіри клієнтів. Банк повинен забезпечити власну безпеку, а також безпеку своїх клієнтів. Політика інформаційної безпеки визначає стратегію і тактику побудови системи захисту інформації.

Аналіз останніх досліджень і публікацій. Питання щодо політики інформаційної безпеки банківських установ висвітлені у наукових працях вітчизняних та зарубіжних вчених. Окремим аспектам даного питання в своїх роботах приділяють увагу Анікін І. В., Бодюл Є. М., Бондаренко М. Ф., Домарєв В. В., Зубок М. І., Кавун С. В., Петренко С. А., Страхарчук А. Я. та інші. Проте аналіз наукових праць показав недостатність вивчення даного питання.

Формулювання цілей статті. Мета статті полягає у дослідженні питання щодо впровадження політики інформаційної безпеки банківських установ. Основними завданнями, які повинні допомогти досягти поставленої мети, є: дослідження підходів до трактування терміну «політика інформаційної безпеки», визначення мети та основних завдань політики інформаційної безпеки банківських установ, наведення основних об'єктів політики інформаційної безпеки банків, розгляд напрямів щодо забезпечення інформаційної безпеки банків, визначення ієрархічного підходу до впровадження політики інформаційної безпеки банківських установ.

Виклад основного матеріалу. У зв'язку з надшвидким розвитком інформаційних технології, в тому числі у банківській системі, постає питання щодо інформаційної безпеки.

Питання впровадження ефективної політики інформаційної безпеки банківської установи є надзвичайно актуальним.

Актуальність впровадження політики інформаційної безпеки банківської установи пояснюється необхідністю створенням механізму управління і планування інформаційної безпеки.

Політика інформаційної безпеки банківської установи визначає стратегію і тактику побудови системи захисту інформації.

Впровадження ефективної політики інформаційної безпеки дозволить підвищити рівень довіри до банківської установи, мінімізувати ризики та витрати, підвищити рівень забезпечення інформаційної безпеки.

Домарєв В. В. зазначає, що під політикою інформаційної безпеки слід розуміти набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз [1, с. 102].

Так на думку Бондаренка М. Ф. поняття «політика інформаційної безпеки банку» являє собою сукупність правових і морально-етичних норм, правил, адміністративних, організаційних заходів і технічних, програмних і криптографічних засобів, направлених на захист інформаційної інфраструктури банку від випадкового і навмисного втручання в процес її функціонування [2].

Анікін І. В. трактує політику інформаційної безпеки, як набір норм, правил і практичних рекомендацій, що регламентують процес обробки інформації, виконання яких забезпечує захист від заданої множини загроз [3, с. 21].

Страхарчук А. Я. розглядає політику інформаційної безпеки, як набір законів, правил і практичних рекомендацій, на базі яких здійснюється керування, захист і розподіл критичної інформації в системі [4].

Бодюл Є. М. під поняттям «політика інформаційної безпеки банківської установи» розуміє науково обґрунтовану систему поглядів на визначення основних напрямів, умов і порядку практичного вирішення задач інформаційного захисту банківської установи від протиправних дій [4, с. 53].

Пропонуємо під поняттям «політика інформаційної безпеки банківської установи» розуміти сукупність правил, обмежень і рекомендацій, прийнятих керівництвом банку, які спрямовані на захист інформації від внутрішніх та зовнішніх загроз.

Метою політики інформаційної безпеки має бути надійний захист інформаційних ресурсів банку від зовнішніх та внутрішніх загроз завдяки впровадженню та ефективному управлінню системою інформаційної безпеки.

Основним завданням політики інформаційної безпеки є захист інформаційних активів від загроз, а саме:

– виявлення та мінімізація потенційних загроз інформаційній безпеці;

– захист інформаційних активів організації;

– забезпечення безпеки та конфіденційності інформації про клієнтів;

– забезпечення стабільної та ефективної діяльності банківської установи.

Основним принципом інформаційної безпеки, якого доцільно дотримуватися банку, є підтримання таких властивостей інформації, як: конфіденційність – захист від несанкціонованого ознайомлення; цілісність – захист від несанкціонованого спотворення, руйнування або знищення; доступність – захист від несанкціонованого блокування [6, с. 7].

Серед основних об'єктів політики інформаційної безпеки банківських установ виокремимо наступні:

– фінансові ресурси – національна й іноземна валюта, банківські операції та угоди банку, коштовності, фінансові документи;

– персонал банку – керівництво і вищий менеджмент банку, особи, які мають доступ до конфіденційної інформації, банківської та комерційної таємниці, інші працівники банку;

– матеріальні засоби – апаратні засоби інформаційних технологій, носії даних, будівлі, приміщення, меблі, транспорт тощо;

– сервісні ресурси та підтримуюча інфраструктура – обслуговуючі засоби обчислювальної техніки, енергопостачання, забезпечення необхідних умов експлуатації і тощо;

– програмне забезпечення – прикладне, системне чи сервісне програмне забезпечення тощо, яке використовується співробітниками банківської установи для роботи з системами і клієнтами;

– інформаційні ресурси – будь-яка інформація банку, що обробляється та зберігається в банківській установі (бази даних, файли, документи) [7, с. 20].

Джерелами загроз інформаційній безпеці банку можуть бути як зовнішні, так і внутрішні. До внутрішніх загроз безпеці банківської установи можна віднести втрату інформації, некомпетентність персоналу, розголошення інформації, знищення інформації, викривлення інформації, викрадення конференційної інформації, витік інформації; до зовнішніх – модифікацію змісту, порушення конфіденційності, порушення логічної цілісності, порушення прав власності на інформацію, порушення фізичної цілісності тощо [8, с. 122].

Фахівці виокремлюють наступні напрями щодо забезпечення інформаційної безпеки в контексті впровадження політики інформаційної безпеки банківської установи:

– перелік законодавчих, регуляторних, нормативних вимог;

– затвердження переліку відомостей, що містять інформацію з обмеженим доступом;

– встановлення правил доступу до інформаційних ресурсів та програмно-технічних комплексів;

– визначення критичних бізнес-процесів/банківських продуктів/ програмно-технічних комплексів;

– забезпечення надання доступу (у тому числі віддаленого) до інформації, її контролю та захисту;

– проведення політики ідентифікації та автентифікації ресурсів;

– політика криптографічного захисту інформації;

– політика «чистого екрана» та «чистого столу»;

– проведення внутрішнього аудиту та вдосконалення системи управління інформаційної безпеки.

Виділяють основні етапи розробки політики інформаційної безпеки:

– визначення та оцінка інформаційних активів;

Рис. 1. Ієрархічний підхід до впровадження інформаційної політики банківської установи

– визначення загроз безпеці;
– оцінка інформаційних ризиків;
– визначення відповідальності;
– створення комплексного документа;
– реалізація;
– управління програмою безпеки [9, с. 70-71].

Основою для формування політики інформаційної безпеки банківської установи можна визначити:
– характеристику об'єкта застосування;
– аналіз поточного стану захисту інформаційної інфраструктури банку;
– облік можливих негативних факторів впливу та ймовірність їх реалізації;
– створення методології ухвалення управлінських рішень щодо забезпечення інформаційної безпеки [2].

Кожній банківській установі доцільно розробити власну політику інформаційної безпеки та ефективно впроваджувати комплекс заходів із захисту конфіденційних даних та інформаційних процесів.

Головною метою політики інформаційної безпеки є інформування працівників, менеджерів і клієнтів банківської установи про їх обов'язки щодо захисту інформації.

Розглянемо ієрархічний підхід до впровадження інформаційної політики банківської установи (рис. 1).

Політика інформаційної безпеки банківських установ повинна розробляється відповідно до вимог чинних законодавства, нормативно-правових актів, міжнародних стандартів та внутрішніх нормативних документів.

Дотримання політики інформаційної безпеки є обов'язковим для всіх співробітників. Документи щодо системи управління інформаційною безпекою доступні працівникам банку лише у межах їх обов'язків і повноважень. Кожний працівник банківської установи несе відповідальність за порушення правил згідно чинного законодавства та внутрішніх нормативних документів.

Політика інформаційної безпеки банківської установи повинна періодично переглядається та удосконалюватися через впровадження нових інформаційних технологій та зміни у законодавчих і внутрішніх нормативних документах.

Неможливо побудувати ідеальну політику інформаційної безпеки банківської установи, оскільки банк це відкрита установа з тисячами клієнтів.

Керівництво банку повинно розуміти, що інформаційна безпека є основою для нормального функціонування банку, та всебічно сприяти виконанню політики інформаційної безпеки.

Для забезпечення інформаційної безпеки банківської установи необхідно застосовувати комплекс заходів, яких повинен дотримуватися кожен працівник банку, виходячи з покладених на нього обов'язків та визначеними правилами згідно політики інформаційної безпеки банку.

Висновки. За результатами проведеного аналізу ми можемо зробити наступні висновки: досліджено сучасний підхід до трактування поняття «політика інформаційної безпеки», що дало змогу запропонувати авторське визначення; визначено мету та основні завдання політики інформаційної безпеки банківських установ; наведено основні об'єкти політики інформаційної безпеки банків; розглянуто напрями щодо забезпечення інформаційної безпеки банків; визначено ієрархічний підхід до впровадження політики інформаційної безпеки банківських установ.

Дослідження питання щодо впровадження політики інформаційної безпеки банківських установ дає основу для побудови ефективної системи інформаційної безпеки банківських установ.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Домарєв В. В. Обґрунтування основних функцій системи управління інформаційною безпекою / В. В. Домарєв, Д. В. Домарєв, С. Б Гордієнко. // Вісник Державного університету інформаційно-комунікаційних технологій. – 2012. – Т. 10, № 2. – С. 102-104.

2. Бондаренко М. Ф. Визначення та обґрунтування суті політики інформаційної безпеки / М. Ф. Бондаренко, О. В. Потій, Ю. І. Горбенко та ін.// Радиотехника. – 2003. – № 134. – С. 9-25.

3. Аникин И. В. Методы и средства защиты компьютерной информации / И. В. Аникин, В. И. Глова, А. Н. Нигматуллина // Учебное пособие. Казань: Изд-во Казан. гос. техн. ун-та, 2008. – 212 с.

4. Страхарчук А. Я. Інформаційні системи і технології в банках: Навч. посіб. / А. Я. Страхарчук, В. П. Страхарчук – К.: УБС НБУ: Знання, 2010. – 515 с. – Режим доступу: http://libfree.com/102585050-bankivska_spravainformatsiyni_sistemi_i_tehnologiyi_v_bankah__straharchuk_aya.html.

5. Бодюл Є. М. Інформаційна безпека банку / Є. М. Бодюл // Протидія злочинам, які вчиняються з використанням комп'ютерних мереж [Текст]: тези доповідей Міжнародної науково-практичної конференції (м. Севастополь, 1–2 жовтня 2010 року) / Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України». – Суми : ДВНЗ «УАБС НБУ», 2010. – С. 53-55.

6. Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. –Харків: Вид. ХНЕУ, 2008. –352 с.

7. Зубок М. І. Безпека банківської діяльності: Навч. Посібник / М. І. Зубок. – К.: КНЕУ, 2002. – 190 с.

8. Черевко О. В. Джерела виникнення загроз інформаційній безпеці банківських установ / О. В. Черевко, В. М. Андрієнко, І. Ю. Напора // Вісник Черкаського університету. Серія: Економічні науки. – 2016. – № 3. – С. 120-127.

9. Петренко С. А. Политики информационной безопасности / С. А. Петренко, В. А. Курбатов. – М.: Компания АйТи. 2006. – 400 с.