МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ
ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

«До захисту допущено»
Завідувач кафедри УІКБ
_____ С.В.Легомінова
(підпис)
“___”_____20__ р.

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

на тему: **«УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ БАНКІВ»**

Студент групи УБДМ-61 Тисячний Роман Олегович _____
(підпис)

Науковий керівник: к.е.н., доцент Мордас Ірина Василівна _____
(підпис)

Нормоконтроль: к.держ.упр. Мужанова Тетяна Михайлівна _____
(підпис)

Київ – 2020

Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою

«Затверджую»
Завідувач кафедри УІКБ
_____ С.В.Легомінова
(підпис)
“___”_____20__ р.

ЗАВДАННЯ
на магістерську атестаційну роботу
студенту Тисячному Роману Олеговичу

1. Тема роботи: «УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ БАНКІВ» затверджена наказом ректора від «___» _____ 20__ р. № __.

2. Термін здачі студентом оформленої роботи: «___» _____ 20__ р.

3. Об’єкт дослідження: інформаційна безпека банків.

4. Предмет дослідження: управління інформаційною безпекою банків.

5. Мета дослідження: розробка рекомендацій щодо удосконалення управління інформаційною безпекою банків.

6. Перелік питань, які мають бути розроблені:

1. Основи управління інформаційною безпекою банків.
2. Особливості управління інформаційною безпекою в банківських установах України.
3. Рекомендації щодо захищеності доступу до інформаційної діяльності банків та проведення аудиту для удосконалення управління інформаційною безпекою в банках.

7. Дата видачі завдання: «___» _____ 20__ р.

Науковий керівник: Мордас І. В.

Завдання прийнято до виконання: Тисячний Р. О.

Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою

КАЛЕНДАРНИЙ ПЛАН
виконання магістерської атестаційної роботи
студентом Тисячним Романом Олеговичем

Дата видачі завдання: «__» _____ 20__ р.

№ з/п	Етапи виконання магістерської атестаційної роботи	Термін виконання етапів	Примітка
1.	Визначення об'єкту, предмету, мети та завдань дослідження.	10.10.2019	
2.	Збір та аналіз літератури.	18.10.2019	
3.	Написання 1-го розділу роботи.	31.10.2019	
4.	Написання 2-го розділу роботи.	14.11.2019	
5.	Написання 3-го розділу роботи.	28.11.2019	
6.	Формулювання висновків за результатами проведеного дослідження.	05.12.2019	
7.	Оформлення роботи.	12.12.2019	
8.	Оформлення презентації.	19.12.2019	
9.	Отримання рецензії на роботу.	26.12.2019	
10.	Захист в ДЕК.	__.01.2020	

Студент групи УБДМ-61 Тисячний Роман Олегович _____
(підпис)

Науковий керівник: к.е.н., доцент Мордас Ірина Василівна _____
(підпис)

Нормоконтроль: к.держ.упр. Мужанова тетяна Михайлівна _____
(підпис)

РЕФЕРАТ

Робота містить вступ, три розділи з підрозділами, висновки, список використаних джерел та додатки. Загальний обсяг роботи – 86 сторінок.

Об’єкт дослідження – інформаційна безпека банків.

Предмет дослідження – управління інформаційною безпекою банків.

Мета дослідження – розробка рекомендацій щодо удосконалення управління інформаційною безпекою банків.

У магістерській атестаційній роботі розглянуто основи управління інформаційною безпекою банків; досліджено особливості управління інформаційною безпекою в банківських установах України; визначено рекомендації щодо захищеності доступу до інформаційної діяльності банків та проведення аудиту для удосконалення управління інформаційною безпекою в банках.

БАНК, ІНФОРМАЦІЙНА БЕЗПЕКА БАНКІВ, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ БАНКІВ, ПОЛІТИКА ІФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АРМ	Автоматизовані робочі місця
АС	Автоматизована система
ДСТУ	Державний стандарт України
ЕОМ	Електронна обчислювальна машина
ЕЦП	Електронний цифровий підпис
ІБ	Інформаційна безпека
ІД	Інформаційна діяльність
ІзОД	Інформація з обмеженим доступом
ІС	Інформаційна система
ІТ	Інформаційні технології
КСЗІ	Комплексна система захисту інформації
ПЗ	Програмне забезпечення
СЗІ	Система захисту інформації
СІБ	Система інформаційної безпеки
СУІБ	Система управління інформаційною безпекою
ISO	International Organization for Standardization

ВСТУП

Актуальність теми. Актуальність проблем інформаційної безпеки в даний час стає одним з найважливіших аспектів загальної економічної безпеки діяльності сучасного банку, характеризуючи стан захищеності його бізнес-середовища. Захист інформації являє собою особливу діяльність щодо запобігання витоку інформації, несанкціонованих змін її потоків та інших дій, які негативно впливають на стабільну роботу банків та пов'язаних з ними економічних агентів (клієнтів, постачальників обладнання, інвесторів та ін.). У зв'язку з цим ефективне управління інформаційною безпекою та своєчасна, оперативна і коректна оцінка ризиків зниження або повної втрати інформаційної безпеки сьогодні є актуальною проблемою в діяльності будь-якого банку.

В даний час для захисту інформації потрібна не просто розробка приватних механізмів захисту, а й реалізація системного підходу, що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів і т. д.). Головною метою будь-якої системи забезпечення інформаційної безпеки є створення умов функціонування підприємства, запобігання загроз його безпеці, захист законних інтересів банку від протиправних посягань, недопущення розкрадання фінансових засобів, розголошення, втрати, витоку, спотворення і знищення службової інформації, забезпечення в рамках діяльності всіх підрозділів банку.

Доцільність проведення даного дослідження обумовлюється тим, що фінансова сфера в світі, зокрема в Україні постійно розвивається та потребує постійного доопрацювання та удосконалення безпеки, так як нові ризики та атаки трапляються щодня. Все більше вчених приділяють цьому увагу, проводять дослідження. Кожного року оновлюються навчальні програми в навчальних закладах, через те що IT сфера рухається без упину вперед.

Мета і завдання дослідження. Мета роботи полягає у розробці пропозицій щодо удосконалення управління інформаційною безпекою банків.

Для досягнення цієї мети в роботі необхідно виконати наступні *завдання:*

1. Розглянути основи управління інформаційною безпекою банків.

2. Дослідити особливості управління інформаційною безпекою в банківських установах України.

3. Визначити рекомендації щодо захищеності доступу до інформаційної діяльності банків та проведення аудиту для удосконалення управління інформаційною безпекою в банках.

Об'єкт дослідження – інформаційна безпека банків.

Предмет дослідження – управління інформаційною безпекою банків.

Методи дослідження. У роботі були використані методи системного аналізу, наукової абстракції, порівняння та ін.

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу здійснити обґрунтований вибір методів і засобів захисту інформації, інфраструктури та персоналу банків у відповідності до цілей, можливостей та ресурсів.

Розділ 1
ОСНОВИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ БАНКІВ

1.1. Інформаційна безпека підприємств та організацій – поняття та визначення

Насичений та стрімкий розвиток інформаційних технологій призвів до інформаційної революції, внаслідок чого основною цінністю для суспільства стають інформаційні ресурси. В наслідок розвитку стало необхідним забезпечення інформаційної безпеки поступово, що виходить на перші плани у проблематиці національної безпеки.

Інформаційна безпека досягається впровадженням ефективної системи управління інформаційною безпекою, яка охоплює політику, процеси, процедури, організаційні структури і програмні та апаратні функції захисту інформації. Ці ключові аспекти служать основою корпоративної програми безпеки. Метою безпеки та програми безпеки є захист компанії та її активів, зокрема банківської установи.

З одного боку, використання інформаційних технологій дає ряд очевидних переваг: підвищення ефективності процесів управління, обробки і передачі даних. У наш час вже неможливо уявити велику організацію без застосування новітніх інформаційних технологій, починаючи від автоматизації окремих робочих місць і закінчуючи побудовою корпоративних розподілених інформаційних систем.

З іншого боку, розвиток мереж, їх ускладнення, взаємна інтеграція, відкритість призводять до появи якісно нових загроз, збільшенню числа зловмисників, які мають потенційну можливість впливати на систему.

На сьогодні інформація стала одним із найбільш важливих ресурсів. Постійно зростаюча необхідність в інформації, підвищенні рівня розвитку та ефективності використання засобів її обробки та передачі призвела до появи

нового поняття, такого як інформаційні ресурси.

Інформаційна безпека – це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення (у цьому значенні частіше використовують термін «захист інформації») [15].

Забезпечення безпечної діяльності необхідне для будь-яких підприємств і установ, починаючи від державних організацій і закінчуючи малими підприємствами з десятками працівників. Різниця полягатиме лише в тому, які засоби і методи й у якому обсязі будуть потрібні для забезпечення їх безпеки.

Основні принципи інформаційної безпеки [15]:

1. Цілісність даних - така властивість, відповідно до якого інформація зберігає своє утримання і структуру в процесі її передачі та зберігання. Створювати, знищувати або змінювати дані користувача, який має право доступу;

2. Конфіденційність - властивість, яке вказує на необхідність обмеження доступу до конкретної інформації для позначеного кола осіб. Таким чином, конфіденційність дає гарантію того, що в процесі передачі даних, вони можуть бути відомі тільки авторизованим користувачам;

3. Доступність інформації - це властивість, яка характеризує здатність забезпечувати своєчасний і безперешкодний доступ повноправних користувачів до необхідної інформації;

4. Достовірність - даний принцип виражається в суворій приналежності інформації суб'єкту, який є її джерелом або від якого вона прийнята.

Об’єктами інформаційної безпеки підприємства є [31]:

1. обладнання автоматизованої системи (фізичні ресурси);

2. інформаційні ресурси (бази даних, файли тощо);

3. програмне забезпечення (системне, прикладне, інші допоміжні

програми);

4. сервіс та підтримуюча інфраструктура (обслуговуючі засоби обчислювальної техніки, енергопостачання, забезпечення необхідних умов експлуатації і т. ін.).

При цьому інформаційна безпека підприємства досягається організацією збору інформації про внутрішнє і зовнішнє середовище підприємства, проведенням інформаційно-аналітичного дослідження клієнтів, партнерів та конкурентів, інформаційного аудиту та інформаційного моніторингу, аналітичної обробки інформації; організацією системи інформаційного забезпечення рішень керівництва підприємства; визначенням категорій інформації та виробленням відповідних заходів щодо її захисту; дотриманням відповідних режимів діяльності; виконанням усіма працівниками норм і правил роботи з інформацією; своєчасним виявленням спроб і можливих каналів втрати інформації.

Проведений аналіз та практичний досвід показують, що в якості базової змістовної моделі забезпечення безпеки інформації необхідно використовувати модель, що визначається міжнародним стандартом ISO/IEC 15408 «Єдині критерії оцінки безпеки систем інформаційних технологій» та ISO/IEC 15446 «Керівництво з розробки профілю захисту та проекту безпеки» [51].

Для характеристики основних властивостей інформації як об'єкта захисту часто використовується модель CIA (confidentiality, integrity, availability) де оцінюється:

1. Конфіденційність інформації (information confidentiality) — властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом;

2. Цілісність інформації (information integrity) — властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом;

3. Доступність (availability) — властивість ресурсу системи (послуги,

інформації), яка полягає в тому, що користувач або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого невеликого проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний.

Питання інформаційної безпеки стають першочерговими в тих випадках, коли вихід з ладу або виникнення помилки в конкретній комп'ютерній системі можуть призвести до тяжких наслідків.

Перш ніж приступити до розгляду сучасного стану проблеми інформаційної безпеки, доцільно розглянути проблеми безпеки взагалі. Спочатку необхідно визначити, що підлягає захисту і якими основними принципами слід керуватися при організації захисту.

За сформованою історичною та міжнародною практикою безпеки об’єктами захисту з урахуванням їх пріоритетів є:

1. особа;

2. інформація;

3. матеріальні цінності.

Якщо пріоритет збереження безпеки особи є природним, то пріоритет інформації над матеріальними цінностями вимагає більш докладного розгляду. Це стосується не тільки інформації, що становить державну чи комерційну таємницю, а й відкритої інформації.

Ринкові відносини з їх невід’ємною частиною - конкуренцією обов’язково вимагають протидії зовнішнім і внутрішнім впливам. Об’єкти захисту більшою чи меншою мірою, залежно від цілей зловмисника і від конкретних умов, можуть зазнавати різних нападів чи загроз, опинитися в ситуації, в якій вони з об’єктивних причин наражаються на небезпеку.

Поняття «безпечна діяльність» будь-якого підприємства чи організації включає:

1. фізичну безпеку, під якою розуміється забезпечення захисту від загрози життю людей;

2. економічну безпеку;

3. інформаційну безпеку (ІБ);

4. матеріальну безпеку, тобто збереження матеріальних цінностей від усякого роду загроз – починаючи від їх крадіжок і закінчуючи загрозами пожежі та інших стихійних лих.

На сьогоднішній день термінологія щодо ІБ в основному розроблена, хоча цей процес триває досі. Найбільш поширені і необхідні терміни зафіксовані в Українському стандарті з технічного захисту інформації [11], безпека інформації (information security) – стан інформації, у якому забезпечується збереження визначених політикою безпеки властивостей інформації.

Автоматизована система (АС) – це організаційно-технічна система, що об’єднує обчислювальну систему, фізичне середовище, персонал і оброблювану інформацію.

Захист інформації в АС – це діяльність, яка спрямована на забезпечення безпеки оброблюваної в АС інформації та АС у цілому і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків унаслідок реалізації загроз.

Комплексна система захисту інформації (КСЗІ) - сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

Також слід розглянути загрози в інформаційній безпеці. Під загрозою інтересів суб'єктів інформаційних відносин розуміють потенційно можливу подію, процес або явище, яке з допомогою впливу на інформацію або інші компоненти інформаційної системи може прямо або опосередковано призвести до нанесення шкоди інтересам даних суб'єктів.

Носіями загроз безпеки інформації є джерела загроз. В якості джерел загроз можуть виступати як суб'єкти (особистість), так і об'єктивні прояви,

наприклад, конкуренти, злочинці, корупціонери, адміністративно-управлінські органи. Джерела загроз переслідують при цьому наступні цілі: ознайомлення з охоронюваними відомостями, їх модифікація в корисливих цілях і знищення для нанесення прямого матеріального збитку [14].

Загроза – це сукупність умов і факторів, що створюють потенційну або реально існуючу небезпеку порушення конфіденційності, доступності та (або) цілісності інформації (див. рис. 1.1) [9].

Рис. 1.1 Загрози безпеці інформації

Основними ризиками, загрозами та небезпеками інформаційній безпеці підприємства є [31]:

1. втрата (порушення) конфіденційності інформації та ресурсів, тобто розкриття змісту інформаційного ресурсу несанкціонованим користувачем (зловмисником);

2. втрата (порушення) цілісності інформації та ресурсів внаслідок впливів як природного, так і штучного характеру;

3. втрата або неякісна доступність до інформації та ресурсів підприємства, можливість доступу до інформації зловмисників;

4. неякісна спостережливість власників та/або користувачів за інформацією та ресурсами.

Необхідно виділити два найбільш важливих типи загроз [26]:

1. намір завдати шкоди, який з'являється у вигляді оголошеного мотиву діяльності суб'єкта;

2. можливість нанесення шкоди - існування достатніх для цього умов і факторів.

Жодна, навіть процвітаюча фірма не зможе продовжити існування, якщо її інформація, що становить комерційну таємницю, стане відомою. Таким чином, економічна та інформаційна безпека виявляються тісно взаємозалежними.

Зменшення загрози для економічної діяльності будь-якої організації передбачає одержання інформації про конкурентів. Тому, цілком природно, зменшення даної загрози для одних організацій спричиняє збільшення загрози економічній діяльності інших організацій. Це стало можливим через наявність промислового, і зокрема економічного, шпигунства.

Одним із важливих нормативних документів підприємства з інформаційної безпеки повинне бути «Положення про комерційну таємницю і конфіденційну інформацію». У ньому вказують склад відомостей, що становлять комерційну таємницю та конфіденційну інформацію підприємства, порядок їх захисту, хто відповідає за організацію заходів захисту, відповідальність за розголошення таких відомостей.

У наказі може вказуватись склад комісії, яка розглядатиме і визначатиме цінність комерційної інформації, подаватиме пропозиції керівнику щодо надання відповідній інформації статусу комерційної таємниці чи конфіденційної інформації. Наказом також можуть передбачатися заходи щодо роботи персоналу стосовно збереження ним у таємниці службової інформації.

Визначення порядку захисту інформації, організації роботи з нею

здійснюється відповідно до положення про організацію роботи з інформацією, що становить комерційну таємницю та є конфіденційною. Положення передбачає: права співробітників підприємства та інших осіб щодо отримання інформації з обмеженим доступом, обов'язки посадових осіб і службовців щодо роботи з грифованими документами, виробами та засобами, правила ведення конфіденційних переговорів за допомогою засобів зв'язку; правила оформлення доступу до інформації з обмеженим доступом, порядок розроблення, зберігання, пересилання та руху грифованих документів; загальні обов'язки працівників підприємства щодо зберігання його таємниць; порядок доступу на засідання і наради, де обговорюються питання, в яких присутня інформація з обмеженим доступом; інші питання, що регулюють правила доступу до інформації з обмеженим доступом.

Окремим наказом може оголошуватись список осіб, яким у повному обсязі може доводитись інформація, що становить банківську і комерційну таємницю та є конфіденційною. Нормативна база банку з питань інформаційної безпеки є основою для правового захисту як таємниць підприємства, так і всієї його діяльності.

Таким чином, завдання безпеки будь-яких видів доводиться вирішувати щоразу при розгляді різноманітних аспектів людської діяльності. Але, як бачимо, всі види безпеки тісно пов’язані з ІБ, і, більше того, їх неможливо забезпечити без забезпечення ІБ. Отже, забезпечення високого рівня ІБ підприємства є вкрай складним і відповідальним завданням.

1.2. Методи і засоби управління інформаційною безпекою банків

Система управління інформаційною безпекою (Information Security Management System) є частиною загальної системи управління, що базується на аналізі ризиків і призначеної для проектування, реалізації, контролю, супроводу та вдосконалення заходів в області інформаційної безпеки. Систему складають

організаційні структури, політика, дії з планування, обов'язки, процедури, процеси і ресурси [33].

Дивлячись на те, що банківські установи та системи будь-якої сучасної держави перебувають у тісному взаємозв’язку із банківськими системами інших держав і міжнародними банківськими організаціями, проблема забезпечення надійності, безпечності, стабільності банківської діяльності виходить далеко поза межи суто внутрішньодержавного регулювання.

У структурі інформаційної безпеки банківської установи виділяють такі основні складові [13]:

– безпека інформаційних ресурсів;

– безпека інформаційної інфраструктури;

– безпека «інформаційного поля».

Створення систем інформаційної безпеки (СІБ) в банківській установі ґрунтується на наступних принципах: системний підхід до побудови системи захисту, що означає оптимальне поєднання взаємопов'язаних організаційних програмних, апаратних, фізичних та інших властивостей, підтверджених практикою створення вітчизняних і зарубіжних систем захисту і застосовуються на всіх етапах технологічного циклу обробки інформації.

Принцип безперервного розвитку системи. Цей принцип, який є одним з основоположних для комп'ютерних інформаційних систем, ще більш актуальний для СІБ. Способи реалізації загроз інформації в ІТ безперервно удосконалюються, а тому забезпечення безпеки ІС не може бути одноразовим актом. Це безперервний процес, що полягає в обґрунтуванні і реалізації найбільш раціональних методів, способів і шляхів вдосконалення СІБ, безперервному контролі, виявленні її вузьких і слабких місць, потенційних каналів витоку інформації та нових способів несанкціонованого доступу.

Поділ і мінімізація повноважень по доступу до оброблюваної інформації та процедурам обробки, тобто надання як користувачам, так і самим працівникам ІС, мінімуму суворо визначених повноважень, достатніх для

виконання ними своїх службових обов'язків. Повнота контролю та реєстрації спроб несанкціонованого доступу, тобто необхідність точного встановлення ідентичності кожного користувача і протоколювання його дій для проведення можливого розслідування, а також неможливість здійснення будь-якої операції обробки інформації в ІТ без її попередньої реєстрації.

Технологічні, виробничі і комерційні дані, які використовують підприємства, мають високу вартість, а їх втрата або витік може привести до серйозних фінансових втрат. Компаній, що мають стратегічне значення для економіки країни, ціна питання особливо велика. Тому однією з цілей для підприємств галузі є створення надійної системи захисту інформації (СЗІ).

Інформаційна безпека будується на наступних принципах [2]:

1. Побудова системи інформаційної безпеки, також як і інформаційної безпеки організації або підприємства, вимагає до себе системного підходу, який передбачає оптимальну пропорцію між організаційних, програмних, правових і фізичних властивостей інформаційної безпеки, підтвердженої практикою створення засобів захисту інформації за методами захисту інформації, які можна застосувати на будь-якому етапі циклу обробки інформації системи;

2. Безперервність розвитку системи управління інформаційною безпекою. Для будь-якої концепції інформаційної безпеки, тим більше, якщо використовуються методи захисту інформації в локальних мережах і комп'ютерних системах, принцип безперервного розвитку є основоположним, адже інформаційна безпека постійно піддається все новим і новим з кожним разом ще більш витонченим атакам, тому забезпечення інформаційної безпеки організації не може бути разовим актом, і створена один раз технологія захисту інформації, буде постійно вдосконалюватися слідом за зростанням рівня зломщиків;

3. Принцип забезпечення надійності системи захисту інформації та інформаційна безпека - це неможливість зниження рівня надійності системи під час збоїв, відмов, помилок і зломів;

4. Обов'язково необхідно забезпечити контроль і управління інформаційною безпекою, для відстеження і регулювання механізмів захисту;

5. Забезпечення засобів боротьби з шкідливим ПЗ. Наприклад, всілякі програми для захисту інформації і система захисту інформації від вірусів;

6. Економічна доцільність використання системи захисту інформації та державної таємниці. Доцільність побудови системи захисту економічної інформації полягає в перевищенні суми збитку при зломі системи захисту інформації на підприємстві над вартістю розробки засоби захисту комп'ютерної інформації, захисту інформації та комплексного захисту інформації.

Система заходів щодо захисту інформації в широкому сенсі слова повинна будуватися виходячи з тих початкових умов і факторів, які, в свою чергу, визначаються станом спрямованості розвідок противника або діями конкурента на ринку товарів і послуг, спрямованими на оволодіння інформацією, що підлягає захисту.

Методи захисту даних на персональних комп'ютерах надзвичайно різноманітні як по кінцевій меті, так і по технічному втіленню; їх можна розділити на механічні, апаратні і програмні.

До механічних засобів захисту ставляться різноманітні кришки і чохли з замками (що замикають, наприклад, дисковод гнучких дисків або мережний вимикач), клейкі пластини для приклеювання термінала до комп'ютера, а комп'ютера до столу, помешкання що замикаються із сигналізацією і багато інших.

Апаратні засоби реалізуються у вигляді спеціальних електронних модулів, що підключаються до системного каналу комп'ютера або портів вводу-виводу, і здійснюють обмін кодовими послідовностями програмами, що захищається.

Найбільш різноманітні програмні засоби. Сюди відносяться програми шифрування даних по заданому користувачем ключу, адміністратори дисків, що дозволяють обмежити доступ користувачів до окремих логічних дисків, методи встановлення програмного продукту з дистрибутивних дискет, що дозволяють

виконати установку не більше вказаного числа запуску програм, що захищаються за допомогою некопійованих ключових дискет, спеціальні захисні програмні оболонки, куди поміщаються програми що захищаються [2].

Згідно «ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення» можливі такі варіанти захисту інформації в банківській установі [9]:

1. досягнення необхідного рівня захисту ІзОД за мінімальних затрат і допустимого рівня обмежень видів ІД;

2. досягнення необхідного рівня захисту ІзОД за допустимих затрат і заданого рівня обмежень видів ІД;

3. досягнення максимального рівня захисту ІзОД за необхідних затрат і мінімального рівня обмежень видів ІД.

Захист інформації, яка не є державною таємницею, забезпечується, як правило, застосуванням першого чи другого варіанту. Захист інформації, яка становить державну таємницю, забезпечується, як правило, застосуванням третього варіанту.

Криптографічні методи захисту інформації – це спеціальні методи шифрування, кодування або іншого перетворення інформації, у результаті якого її утримання стає недоступним без пред'явлення ключа криптограми й оберненого перетворення. Криптографічний метод захисту, безумовно, самий надійний метод захисту, тому що охороняється безпосередньо сама інформація, а не доступ до неї (наприклад, зашифрований файл не можна прочитати навіть у випадку крадіжки носія) [6].

Криптографія – це наука, яка вивчає і описує модель інформаційної безпеки даних. Криптографія відкриває вирішення багатьох проблем інформаційної безпеки мережі: аутентифікація, конфіденційність, цілісність і контроль взаємодіючих учасників [5].

Термін «Шифрування» означає перетворення даних в форму, не неможливу для прочитання для людини і програмних комплексів без ключа

шифрування-розшифрування. Криптографічні методи захисту інформації дають високий результат захисту інформації в банківських установах, тому вони є частиною комплексу системи інформаційної безпеки [5].

Даний метод захисту реалізується у виді програм або пакетів програм, що розширюють можливості стандартної операційної системи. Захист на рівні операційної системи, частіше усього, повинен доповнюватися засобами захисту на рівні систем керування базами даних, що дозволяють реалізовувати складні процедури керування доступом.

На сьогодні не існує звичайної класифікації криптографічних методів захисту інформації. Проте, коли піддається перетворенню (шифровці) кожний символ переданого повідомлення («симетричний» метод закриття інформації), можна умовно виділити чотири основні групи [19]:

1. підстановка – символи тексту що шифрується заміняються символами того ж або іншого алфавіту відповідно до заздалегідь визначеного правила;

2. перестановка – символи тексту що шифрується переставляються по деякому правилу в межах заданого блока переданого тексту

3. аналітичне перетворення – текст що шифрується перетвориться по деякому аналітичному правилу;

4. комбіноване перетворення – вихідний текст шифрується двома або великим числом засобів шифрування.

Також існує метод форматування накопичувача. Відомо, що на початку кожного накопичувача розташовані таблиці розділів, таблиці розміщення файлів, каталоги – тому знищення інформації починається саме з них і навіть після декількох секунд роботи даного пристрою на накопичувачі залишену інформацію, дуже важко відновити. Якщо ж пристрій відпрацює декілька хвилин, то вся інформація буде знищена.

Подібний метод знищення інформації може здаватися «варварським», проте якщо правильно організувати роботу (резервне копіювання щодня, ведення повного протоколу роботи за день і т. п.), то стерту інформацію можна

відновити із мінімальними втратами (диск не страждає).

Серед основних напрямків захисту інформації поряд з організаційної виділяють правовий та інженерно-технічний захист інформації.

На сьогоднішній день існує великий арсенал інженерно-технічних методів забезпечення інформаційної безпеки [19]:

- Засоби ідентифікації, автентифікації і авторизації користувачів. Ідентифікація та авторизація – це ключові елементи інформаційної безпеки. Функція авторизації відповідає за те, до яких ресурсів конкретний користувач має доступ. Функція адміністрування полягає в наділенні користувача певними ідентифікаційними особливостями в рамках даної мережі і визначенні обсягу допустимих для нього дій.

- Засоби шифрування інформації, що зберігається на комп'ютерах і переданої мережами дозволяють мінімізувати втрати в разі несанкціонованого доступу до даних, що зберігаються на жорсткому диску або іншому носії, а також перехоплення інформації при її пересилання по електронній пошті або передачі по мережевим протоколам. Завдання даного засобу захисту – забезпечення конфіденційності. Основні вимоги, що пред'являються до систем шифрування – високий рівень криптостійкості і легальність використання на території багатьох держав.

- Міжмережеві екрани представляють собою систему або комбінацію систем, що утворить між двома або більше мережами захисний бар'єр, що оберігає від несанкціонованого потрапляння в мережу або виходу з неї пакетів даних.

- Віртуальні приватні мережі. Їх використання дозволяє вирішити проблеми конфіденційності і цілісності даних при їх передачі по відкритим комунікаційним каналам.

- Засоби контентної фільтрації – ефективний засіб захисту від втрати конфіденційної інформації – фільтрація вмісту вхідної та вихідної електронної пошти.

- Інструменти перевірки цілісності вмісту дисків дозволяють виявляти будь-які дії з файлами (зміна, видалення або ж просто відкриття) і ідентифікувати активність вірусів, несанкціонований доступ або крадіжку даних авторизованими користувачами.

- Засоби антивірусного захисту. Сучасні антивірусні технології дозволяють виявити практично всі вже відомі вірусні програми через порівняння коду підозрілого файлу із зразками, що зберігаються в антивірусній базі.

- Системи виявлення вразливостей мереж і аналізатори мережевих атак.

Кожне з перерахованих пунктів може бути використано як самостійно, так і в інтеграції з іншими. Це робить можливим створення систем інформаційного захисту для мереж будь-якої складності і конфігурації, що не зале-жать від використовуваних платформ.

Протоколювання і аудит є невід'ємною частиною забезпечення інформаційної безпеки банківської установи. Ці поняття мають на увазі збір, накопичення і аналіз подій, що відбуваються в інформаційній системі в реальному часі.

Реалізація протоколювання і аудиту вирішує наступні завдання [29]:

1. забезпечення підзвітності користувачів і адміністраторів;

2. забезпечення можливості реконструкції послідовності подій;

3. виявлення спроб порушень інформаційної безпеки;

4. надання інформації для виявлення і аналізу проблем.

При протоколюванні події рекомендується записувати, по крайній мірі, наступну інформацію [29]:

1. дата і час події;

2. унікальний ідентифікатор користувача – ініціатора дії;

3. тип події;

4. результат дії (успіх або невдача);

5. джерело запиту (наприклад, ім'я терміналу);

6. імена порушених об'єктів (наприклад, що відкриваються або файлів, що видаляються);

7. опис змін, внесених до баз даних захисту (наприклад, нова мітка безпеки об'єкта).

У свою чергу зловмисники так само застосовують ряд методів і засобів для порушення систем захисту банківської установи. Ситуація протистояння розробників і зловмисників постійно змінюється за рахунок комбінування вже відомих методів захисту та нападу, а так само за рахунок створення і використання нових методів.

Завдання забезпечення управління інформаційною безпекою банківської установи має на увазі реалізацію багатопланових і комплексних заходів щодо запобігання і відстеження несанкціонованого доступу неавторизованих осіб, а також дій, що попереджають неправомірне використання, пошкодження, спотворення, копіювання, блокування інформації.

1.3. Проблеми управління інформаційною безпекою банків

Проблема інформаційної безпеки підприємств та організацій є надзвичайно актуальною на сучасному етапі розвитку інформаційних технологій, інформаційних систем і мереж. Це пояснюється зростаючими технічними і програмними можливостями доступу до інформації, що не завжди є правомірним. Актуальність проблеми інформаційної безпеки підприємств і організацій визначається рядом взаємозв’язаних факторів, більшість з яких є наслідком процесу інформатизації сучасного суспільства.

Серед таких факторів, з одного боку – формування правових засад інформатизації, поширення застосування сучасних інформаційних технологій у підприємницькій діяльності, а з іншого – висока уразливість інформаційних систем, стрімкий прогрес розвитку так званої «інформаційної зброї». Особливості соціально-економічної ситуації, відсутність реальних обмежень

щодо доступу до засобів інформаційного нападу призводять до численних фактів їх застосування конкурентами, кримінальними елементами, іншими суб’єктами проти комерційних структур.

Найпоширеніші джерела операційного ризику, що впливають на безпеку інформаційних даних в банківських установах стосуються [7]:

1. Персонал (людський фактор), зокрема ненавмисні та/або некомпетентні дії, пов'язані з відсутністю навичок та знання; неправильне навчання; нестача усвідомлення стандартів виконання; задіяні методи інструменти та процедури; недбалість; технічні помилки; неправильний контроль тощо;

Умисні дії, пов'язані з несанкціонованими транзакціями; крадіжка; підробка даних у системі бухгалтерського обліку; підробка фінансових платіжних документів; хакерство; порушення правил та процедур банку; відмивання грошей; інсайдерська торгівля та інші навмисні дії з метою особистого збагачення;

Погане планування та управління персоналом - дефіцит персоналу і його заміна, недостатньо підготовлені або кваліфіковані кадри; хворі листи; плин кадрів тощо;

Вплив на інтереси клієнтів через порушення інформаційної безпеки банку; розголошення особистого та/або конфіденційного характеру інформації; кривда інтересів клієнтів і т. д .;

2. Внутрішні процеси - порушення встановлених правил, інструкцій, процесів, політики та процедури контролю; погана оцінка ризиків та вимірювання ризику внаслідок помилок або пропущень;

3. Проблеми в ІТ-системах, що призводять до часткового або повного переривання банківських операцій. Це може бути розділено на:

- Загальні систематичні ризики, пов'язані з обмеженим доступом до системи та мережі; неналежні дії для резервного копіювання даних та відновлення захисту від вірусів та шкідливих програм; політика щодо обмеження несанкціонованого доступу до системи тощо;

- Ризики, пов'язані з використовуваним програмним забезпеченням, яке може бути пов'язане з провалами системи; помилки в обчисленні та/або звітності операцій та інші помилки програмування в результаті застарілих та/або недостатніх технологій; несанкціонований доступ до даних клієнтів та рахунків; проблеми резервного копіювання даних тощо;

- Ризики, пов'язані з апаратним забезпеченням, які стосуються переважно використання застарілих або неякісних комп'ютерних систем; відсутність критично важливих резервних копій серверів та апаратних елементів, відсутність резервної копії та системи відновлення; відсутність аварійних енергосистем та інше;

4. Зовнішні фактори, пов'язані з:

- Форс-мажором - катастрофи, пожежі, вандалізм, терористичні напади, тощо;

- Умисні сторонні дії - пограбування, шахрайство від імені банку, хакерські атаки, незаконний доступ до рахунків клієнтів, інші навмисні дії;

- Ризики, пов'язані з постачальниками послуг - провайдерами телефонних послуг, енергопостачання, телекомунікації, послуги аутсорсинга тощо.

Основні проблемні напади на безпеку даних банківських систем через крадіжку, маніпулювання або знищення даних - це спроба збагатитись швидко або для покриття чи вчинення іншого злочину. Вони пов'язані головним чином з [38]:

1. Шахрайством, що пов'язане з ідентифікацією, у випадку переходу на рахунки третіх сторін або відкриття рахунків та придбання фінансових цінних паперів через фальшиву ідентичність. Хоча метою злодіїв насамперед є перший вид злочину - пряма крадіжка готівки, другий тип злочину, як правило, є частиною складної кримінальної схеми для здійснення комерційних, фінансових, страхових або податкових шахрайств;

2. Отримання конфіденційної інформації для участі в різних шпигунських діях, в більшості випадків збирати інформацію про бізнес або про партнера, а

також отримати доступ до внутрішньої інформації, яка може бути використана для майбутнього збагачення;

3. Використання існуючої банківської інфраструктури для фінансування податкових злочинів. Окрім фінансового, комерційного та податкового шахрайства які включають банківські рахунки реальних та / або вигаданих осіб і компанії, організована злочинність також використовує банківську систему, щоб приховати справжнє походження статків, отриманих неправомірно, і полегшити їх проникнення та інтеграцію в законну економіку, процес, відомий як «відмивання грошей».

4. Кіберзлочини в більшості випадків призначені для крадіжки коштів онлайн, злочинці вони можуть бути прихильниками приховання доказів іншого злочину шляхом знищення всіх доступних або резервних даних в банку. Кібер-тероризм та інформаційна війна, незважаючи на наявність різних джерел та завдань, створюють серйозну загрозу для банку оскільки вони спрямовані на те, щоб повністю знищити дані та IT інфраструктуру, перервати звичайні бізнес-процеси, а також викликати проблеми банкам, фінансовій системі та економіці в загалом.

Основний вид збитків, завданих банками через порушення безпеки даних, стосується [48]:

1. Прямих фінансових втрат, пов'язаних з крадіжкою коштів, що утримуються та управляються комерційним банком;

2. Непрямі фінансові втрати внаслідок регуляторних штрафів, судових витрат, витрат на відшкодування, втрати довіри клієнтів та лояльності;

3. Відображення витрат, пов'язаних із втратою довіри громадськості та споживачів через публічне розголошення порушень безпеки даних та витоку конфіденційної інформації про банківські операції, клієнти, відмивання грошей, участь у кримінальних схемах тощо.

4. Витрати на можливі нещасні випадки із захистом даних у банку, який, крім двох вищезазначених пунктів, також стосується погіршення

конкурентоспроможності банку; зміна внутрішніх та організаційних пріоритетів; зменшення робочого навантаження, що впливає на операційний прибуток тощо;

5. Витрати на оборону ІТ, які включають витрати на проектування ІТ-інфраструктури та комунікаційної інфраструктури для запобігання атак та забезпечення відмово стійкості банківських ІТ-систем, а також витрати, пов'язані з розгортанням організаційних заходів з підвищення безпеки даних та підвищення рівня підготовки та обізнаності персоналу і клієнтів з точки зору нових ризиків ІТ та їх запобігання.

Процеси глобалізації та оцифрування повільно, але незворотно, змінюють всі аспекти сучасного суспільства. Незважаючи на надання нових можливостей, ці процеси також створюють нові ризики та виклики, отже, зростає значення безпеки даних та даних у новому цифровому середовищі. Єдиним доступним рішенням для комерційних банків є адаптація та розвиток в нових умовах, що вимагає оцифрування та автоматизації існуючих процесів; експлуатація нових каналів розподілу для надання банківських продуктів та послуг; а також створення нових продуктів та послуг. Отже, управління інформаційною безпекою даних стало новим ключовим аспектом управління банківськими ризиками та загальним управлінням банківськими установами.

При аналізі проблематики, пов'язаної з інформаційною безпекою, необхідно враховувати специфіку даного аспекту безпеки, що полягає у тому, що інформаційна безпека є складовою частиною інформаційних технологій області, що розвивається надзвичайно високими темпами.

Тут важливі не стільки окремі рішення (закони, навчальні курси, програмно-технічні засоби), що перебувають на сучасному рівні, скільки механізми генерації нових рішень, що дозволяють жити в темпі технічного прогресу.

На жаль, сучасна технологія програмування не дозволяє створювати безпомилкові програми, що не сприяє швидкому розвитку засобів забезпечення

ІБ. Варто виходити з того, що необхідно конструювати надійні системи(інформаційної безпеки) із залученням ненадійних компонентів (програм). У принципі, це можливо, але вимагає дотримання певних архітектурних принципів і контролю стану захищеності протягом усього життєвого циклу ІС.

У таких умовах системи інформаційної безпеки повинні вміти протистояти різноманітним атакам, як зовнішнім, так і внутрішнім, атакам автоматизованим і скоординованим. Іноді напад триває долі секунди; часом промацування уразливих місць ведеться повільно й розтягується на години, так що підозріла активність практично непомітна. Метою зловмисників може бути порушення всіх складових ІБ - доступності, цілісності або конфіденційності.

Застосування міжнародних стандартів у вирішенні проблем управління інформаційною безпекою банку

Особливим напрямом інформаційної безпеки банку є забезпечення захисту банківських інформаційно-обчислювальних мереж, систем електронних платежів, комп'ютерних баз даних від несанкціонованого проникнення, а також від технічних перебоїв і неполадок [10].

На даний час в сфері інформаційної безпеки банків існує ряд проблем, а саме: ставлення керівників банків до інформаційних технологій неоднозначне: одні підтримують упровадження сучасних інформаційних технологій, розуміючи, що це дасть конкурентні переваги банку, сприятиме популярності серед клієнтів; інших стримує та обставина, що сучасні інформаційні технології потребують значних фінансових ресурсів, особливо під час впровадження [32].

Керівництво банку часто вважає, що витрати на систему захисту інформації занадто великі, та не приносять прибутку, тому без них можна обійтись. Однак, якщо банк не приділятиме достатньої уваги інформаційній безпеці в майбутньому він може зазнати значних ризиків: фінансові втрати, погіршення репутації, часті хакерські атаки, помилки та недостатня обізнаність персоналу, відсутність належної системи захисту, неправильна робота

програмно-технічних комплексів, використання небезпечних інформаційних технологій, неправильне використання послуг третіх сторін та ін. Всі ці ризики призводять до втрати конфіденційності, цілісності й доступності інформації, тобто - до порушення інформаційної безпеки.

Щоб зменшити (усунути) ці ризики банк повинен розробити і впровадити систему захисту інформації та політику інформаційної безпеки. Для покращення реалізації цих заходів варто звернути увагу на міжнародні стандарти з управління інформаційною безпекою (див. Додаток А), які дозволяють: оптимізувати вартість побудови та підтримання системи інформаційної безпеки; постійно відслідковувати та оцінювати ризики з урахуванням цілій бізнесу; ефективно виявляти найбільш критичні ризики та знижувати 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.

Однак, наведені вище переваги не будуть досягнуті шляхом лише “формального” підходу до розроблення, впровадження та функціонування системи управління інформаційною безпекою, необхідно, щоб керівництво і працівники банку були теж зацікавлені в підвищенні рівня інформаційної безпеки.

Висновки до першого розділу

Отже, інформаційна безпека банківської установи - це стан, при якому забезпечується необхідний рівень інформованості керівництва та персоналу банківської установи, а також зовнішнього середовища, ефективний захист усіх видів інформації від зовнішніх і внутрішніх ризиків, загроз та небезпек.

Завдання забезпечення управління інформаційною безпекою банківської установи має на увазі реалізацію багатопланових і комплексних заходів щодо запобігання і відстеження несанкціонованого доступу неавторизованих осіб, а також дій, що попереджають неправомірне використання, пошкодження, спотворення, копіювання, блокування інформації.

Методи і засоби захисту даних в банківських установах надзвичайно різноманітні як по кінцевій меті, так і по технічному втіленню; їх можна розділити на механічні, апаратні і програмні. Окремо слід виділити метод форматування накопичувача, криптографічний метод. До засобів слід віднести - засоби авторизації користувачів, міжмережеві екрани, віртуальні приватні мережі, засоби контентної фільтрації, засоби антивірусного захисту.

Узагальнюючи аналіз джерел можна виділити основні пункти до основних проблем управління інформаційною безпекою (див. Додаток Б). Найчастішою проблемою є людський фактор. Працівники банківської установи можуть випадково чи навмисно видати конфіденційну інформацію.

Наступним є те що, банківських установ як приватних так і державних в Україні достатньо багато, що спричиняє високу конкурентність, саме через це загрозою банківської установи може бути банківська установа конкурентів. Також застосування міжнародних стандартів у вирішенні проблем управління інформаційною безпекою сприятиме стабільній роботі банківських установ.

Розділ 2
УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В БАНКІВСЬКИХ УСТАНОВАХ УКРАЇНИ

2.1. Необхідність запровадження управління інформаційною безпекою в банківських установах

На сьогоднішній день нагальною постає проблема збільшення інформаційної безпеки банківських установ, яка значною мірою залежить від ступеня захищеності інформаційної сфери. Рівень інформаційної безпеки впливає на розвиток та впровадження науково-технічних інновацій у процеси виробництва, збереження стабільності функціонування можливості економічного зростання.

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.

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 [25]:

1. оптимізувати вартість побудови та підтримання системи інформаційної безпеки;

2. постійно відслідковувати та оцінювати ризики з урахуванням цілей бізнесу;

3. ефективно виявляти найбільш критичні ризики та знижати ймовірність їх реалізації;

4. розробити ефективну політику інформаційної безпеки та забезпечити її якісне виконання;

5. ефективно розробляти, впроваджувати та тестувати плани відновлення бізнесу;

6. забезпечити розуміння питань інформаційної безпеки керівництвом та всіма працівниками банку;

7. забезпечити підвищення репутації та ринкової привабливості банків;

8. знизити ризики рейдерських та інших шкідливих для банку атак.

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.

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

Джерелами вимог з інформаційної безпеки є [25]:

- 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.

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).

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

Наша держава має висококваліфікований кадровий потенціал в інформаційній сфері, постійно зростаючий та поновлюваний парк комп’ютерної техніки, сучасні системи та засоби телекомунікацій, зв’язку, високу ступінь інформатизації банківської сфери. Однак, стан розбудови інформаційного суспільства в Україні порівняно із світовими тенденціями є недостатнім і не відповідає потенціалу та можливостям України.

Проблеми національної безпеки українські фахівці інтенсивно розробляють з 90-х років минулого століття. Національна безпека, як важлива функція кожної держави, що покликана гарантувати сприятливі умови для життя і продуктивної діяльності громадянам, державних інститутів, захищати життєво важливі інтереси людини, суспільства й держави від зовнішніх і внутрішніх загроз.

Національна безпека, як зазначено у ст.1 Закону України „Про основи національної безпеки України", виступає як „захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам" [12].

Захищеність людини і громадянина, суспільства і держави забезпечується відповідною діяльністю, яка зменшує або відвертає ймовірні загрози і підвищує захисні, мобілізаційні функції у період небезпеки чи загроз.

В основі цієї діяльності лежить обстоювання і реалізація національного інтересу певної країни – глобального, всеохоплюючого інтегрального інтересу, втілення якого уможливлює здійснення життєво важливих приватних, групових і суспільних інтересів переважної більшості громадян.

Правову основу національної безпеки становлять Конституція України, закони, інші нормативно-правові акти, а також визнані Україною міжнародні договори і угоди.

Стратегія національної безпеки України – визначає принципи, пріоритетні цілі, завдання та механізми забезпечення життєво важливих інтересів особи, суспільства і держави від зовнішніх і внутрішніх загроз.

Необхідність запровадження управління інформаційною безпекою в банку 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.

2.2. Управління інформаційною безпекою банківських установ в законодавстві України

Банківський сектор є важливим елементом цілісної фінансової системи будь-якої країни. Комерційні банки покликані акумулювати грошові активи, здійснювати кредитування різних галузей економіки. З моменту свого виникнення, банки несамовито викликали і викликають інтерес, котрі пов'язаний не тільки зі зберіганням або отриманням грошових активів, але і з секретною інформацією у фінансовій діяльності різних суб'єктів економіки, що мають угоди з банками [24].

Інформаційна безпека України як один з видів національної безпеки, важлива функція держави, означає [21]:

1. законодавче формування державної інформаційної політики;
2. створення відповідно до законів України можливостей досягнення інформаційної достатності для ухвалення рішень органами державної влади, громадянами та об’єднаннями громадян, іншими суб’єктами права в Україні;
3. гарантування свободи інформаційної діяльності та права доступу до інформації у національному інформаційному просторі України;
4. всебічний розвиток інформаційної структури;
5. підтримка розвитку національних інформаційних ресурсів України з урахуванням досягнень науки і техніки та особливостей духовно-культурного життя народу України;
6. створення і впровадження безпечних інформаційних технологій;
7. захист права власності всіх учасників інформаційної діяльності в національному просторі України;
8. збереження права власності держави на стратегічні об’єкти інформаційної інфраструктури України;

9. охорону державної таємниці, а також інформації з обмеженим доступом, що є об’єктом права власності або об’єктом лише володіння, користування чи розпорядження державою;

10. створення загальної системи охорони інформації, зокрема охорони державної таємниці, а також іншої інформації з обмеженим доступом;

11. захист національного інформаційно простору України від розповсюдження спотвореної або забороненої для поширення законодавством України інформаційної продукції;

12. встановлення законодавством режиму доступу іноземних держав або їх представників до національних інформаційних ресурсів України та порядок використання цих ресурсів на основі договорів з іноземними державами;

13. законодавче визначення порядку поширення інформаційної продукції зарубіжного виробництва на території України.

Державна політика інформаційної безпеки визначається пріоритетністю національних інтересів, системою небезпек і загроз і здійснюється шляхом реалізації відповідних доктрин, стратегій, концепцій і програм в інформаційній сфері відповідно до чинного законодавства.

Забезпечення інформаційної безпеки певної інформаційної системи вимагає комплексного підходу. Виділяють наступні заходи забезпечення інформаційної безпеки [17]:

1. законодавчі заходи забезпечення інформаційної безпеки;

2. адміністративні заходи (накази і інші дії керівництва організацій, пов’язаних з інформаційними системами, що захищаються);

3. процедурні заходи (заходи безпеки, орієнтовані на людей);

4. програмно-технічні заходи.

Закони і нормативні акти орієнтовані на всіх суб’єктів інформаційних відносин незалежно від їх організаційної приналежності (це можуть бути як юридична, так і фізична особи) в межах країни (міжнародні конвенції мають навіть ширшу область дії), адміністративні заходи - на всіх суб’єктів в межах

організації, процедурні - на окремих людей (або невеликі категорії суб'єктів), програмно-технічні - на устаткування і програмне забезпечення.

Відповідно до статей 7, 15, 56 Закону України "Про Національний банк України", з метою удосконалення вимог до захисту інформації в інформаційних системах банків з урахуванням актуальних кіберзагроз, установлення вимог щодо організації заходів із забезпечення інформаційної безпеки та кіберзахисту банків, Правління Національного банку України постановляє [28]:

Це Положення розроблено відповідно до Законів України "Про Національний банк України", "Про банки і банківську діяльність", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про основи національної безпеки України", указів Президента України від 13 лютого 2017 року № 32/2017 "Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації" та від 15 березня 2016 року № 96/2016 "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України", національних стандартів України з питань інформаційної безпеки ДСТУ ISO/IEC 27000:2015 "Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник" (далі - ДСТУ ISO/IEC 27000:2015), ДСТУ ISO/IEC 27001:2015 "Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги" (далі - ДСТУ ISO/IEC 27001:2015), ДСТУ ISO/IEC 27002:2015 "Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки" (далі - ДСТУ ISO/IEC 27002:2015), які прийняті наказом Державного підприємства "Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості" від 18 грудня 2015 року № 193, та з урахуванням міжнародних стандартів з питань інформаційної безпеки, загальноприйнятих у міжнародній практиці принципів забезпечення інформаційної безпеки і кіберзахисту з метою підвищення рівня інформаційної безпеки в банківській системі України.

Це Положення встановлює [28]:

1. обов'язкові мінімальні вимоги щодо організації заходів із забезпечення інформаційної безпеки та кіберзахисту;

2. принципи управління інформаційною безпекою;

3. вимоги до інформаційних систем банку, що взаємодіють з інформаційними системами Національного банку України (далі - Національний банк), з урахуванням напрямів розвитку криптографічного захисту інформації в інформаційних системах Національного банку.

Це Положення не встановлює вимог щодо[28]:

1. фізичної безпеки приміщень банків, технічного захисту інформації для приміщень банків, використання криптографічних засобів захисту інформації Національного банку в інформаційних системах Національного банку, вимоги до яких визначені відповідними нормативно-правовими актами Національного банку;

2. використання хмарних технологій/сервісів (Cloud technologies) у сфері автоматизації, технічної й технологічної підтримки діяльності банків, вимоги до яких визначаються окремим документом.

Принципи забезпечення інформаційної безпеки:

1. підхід до забезпечення інформаційної безпеки має бути системним (комплексним);

2. процес удосконалення та розвитку інформаційної безпеки має бути безперервним і здійснюватися шляхом обґрунтування та реалізації раціональних засобів, методів, заходів із застосуванням найкращого міжнародного досвіду;

3. заходи захисту від реальних та потенційних загроз інформаційній безпеці банку мають бути своєчасні й адекватні;

4. забезпечення належного рівня інформаційної безпеки банку неможливе без підтримки та контролю з боку керівників банку;

5. сталий розвиток систем інформаційної безпеки можливий лише в разі забезпечення достатності ресурсів, у тому числі фінансових.

Принципи криптографічного захисту інформаційних систем Національного банку [28]:

1. криптографічний захист інформації в інформаційних системах Національного банку на ділянці зв'язку між учасником інформаційних систем Національного банку та Національним банком забезпечується застосуванням багаторівневого (ешелонованого) підходу, за яким окремо за допомогою незалежних систем криптографічного захисту інформації захищається сеансовий рівень базової еталонної моделі взаємодії відкритих систем (Open systems interconnection basic reference model, OSI/ISO) та прикладний рівень моделі взаємодії відкритих систем інформаційних систем Національного банку;

2. для захисту сеансового рівня моделі взаємодії відкритих систем інформаційних систем Національного банку використовується криптографічний протокол захисту на транспортному рівні (Transport layer security, TLS), забезпечуються контроль цілісності та конфіденційність інформації. Для прикладного рівня моделі взаємодії відкритих систем інформаційних систем Національного банку використовуються такі механізми захисту: ідентифікація/автентифікація підписувача, контроль цілісності та конфіденційність на всіх етапах оброблення інформації;

3. залежно від категорії інформації щодо критерію конфіденційності, для забезпечення ідентифікації та автентифікації, використовується односпрямований (криптографічний ключ лише на стороні сервера, сувора криптографічна автентифікація сервера) або двоспрямований достовірний канал захисту на транспортному рівні (криптографічний ключ на стороні клієнта і на стороні сервера, сувора криптографічна автентифікація обох сторін з'єднання);

4. інформаційні системи Національного банку підтримують роботу криптографічного протоколу захисту на транспортному рівні останньої версії, але не нижче версії 1.2;

5. інформаційні системи Національного банку використовують криптографічні набори захисту на транспортному рівні лише з шифруванням та застосовують симетричні криптографічні алгоритми з довжиною ключа не менше ніж 128 біт;

Департамент безпеки Національного банку надає криптобібліотеки для криптографічних засобів захисту інформації, рекомендації щодо їх використання та програмне забезпечення генерації ключів.

Банк зобов'язаний упровадити систему управління інформаційною безпекою згідно з ДСТУ ISO/IEC 27001:2015 для визначеної сфери застосування з урахуванням обов'язкових вимог щодо впровадження СУІБ.

Передумовами впровадження СУІБ у банку є:

1. упровадження процесного підходу до діяльності банку;

2. упровадження ризик-орієнтованого підходу до забезпечення інформаційної безпеки банку.

Банк зобов'язаний запровадити процес управління ризиками інформаційної безпеки в рамках системи управління ризиками банку. Банк має право самостійно визначати підходи (методики) оцінювання та оброблення ризиків інформаційної безпеки.

Банк зобов'язаний запровадити, використовуючи ризик-орієнтований підхід, заходи безпеки, визначені додатком А до ДСТУ ISO/IEC 27001:2015, згідно з ДСТУ ISO/IEC 27002:2015 та з урахуванням обов'язкових вимог щодо організації заходів безпеки інформації, викладених у розділах IV і V цього Положення.

Банк зобов'язаний визначити мінімальною сферою застосування СУІБ усі критичні бізнес-процеси банку. Банк має право розширити сферу

застосування СУІБ банку відповідно до особливостей його діяльності, характеру та обсягу банківських, фінансових послуг та інших видів діяльності.

Національний банк має право здійснювати перевірку стану впровадження СУІБ банку та повноту виконання заходів безпеки інформації, що встановлені цим Положенням.

Банк зобов'язаний сформувати колективний керівний орган з питань впровадження та функціонування СУІБ (далі - керівний орган СУІБ) або наділити цими повноваженнями існуючий колективний керівний орган банку та розробити положення про керівний орган СУІБ банку з чітким визначенням його завдань, функцій та відповідальності.

Банк зобов'язаний включити до складу керівного органу СУІБ голову правління банку та/або його заступника, що відповідає за інформаційну безпеку банку, керівників підрозділів банку - власників критичних бізнес-процесів банку та керівника підрозділу банку з управління ризиками. Банк має право ввести до складу керівного органу СУІБ інших працівників банку відповідно до потреб, що обумовлені особливостями діяльності банку.

Банк зобов'язаний покласти на керівний орган СУІБ обов'язок виконання таких завдань [28]:

1. погодження та перегляд політики інформаційної безпеки, положення щодо застосовності та стратегії розвитку інформаційної безпеки банку;

2. узгодження впровадження нових проектів, напрямів, стратегічних завдань з питань інформаційної безпеки банку та заходів інформаційної безпеки;

3. розгляд, затвердження та контроль за виконанням проектів щодо розроблення, упровадження, функціонування, моніторингу, перегляду, підтримання та вдосконалення СУІБ банку;

4. визначення необхідних оптимальних ресурсів для впровадження заходів інформаційної безпеки;

5. організація практичних заходів щодо підвищення обізнаності/навчання персоналу банку з питань інформаційної безпеки;

6. забезпечення своєчасного моніторингу стану впровадження та ефективності функціонування СУІБ банку з подальшою оцінкою можливостей вдосконалення та потреби проведення коригувальних дій.

Банк зобов'язаний розробити та впровадити політику інформаційної безпеки, яка має містити:

1. цілі інформаційної безпеки;

2. сферу застосування політики інформаційної безпеки;

3. принципи, правила та вимоги інформаційної безпеки в банку;

4. визначення функцій (ролей) і відповідальності за забезпечення інформаційної безпеки.

Банк зобов'язаний забезпечити підтримку політики інформаційної безпеки в актуальному стані та її перегляд не рідше ніж один раз на рік. Якщо за результатами перегляду зміни до політики інформаційної безпеки не вносяться, то повторне її затвердження не потрібно.

Банк зобов'язаний затвердити політику інформаційної безпеки і довести її зміст до відома всього персоналу банку та, за необхідності, представникам третіх сторін.

Банк зобов'язаний розробити та затвердити стратегію розвитку інформаційної безпеки. Банк має право затвердити стратегію розвитку інформаційної безпеки банку в документі, яким затверджено загальну стратегію розвитку банку, у вигляді окремого розділу. Зміст стратегії має узгоджуватися з політикою інформаційної безпеки банку, основними стратегічними цілями банку, що пов'язані із впровадженням нових бізнес-процесів/банківських продуктів з використанням технологій, які потребують захисту інформації, а також враховувати планування розвитку інфраструктури банку та заходів інформаційної безпеки для мінімізації ризиків інформаційної безпеки.

Банк зобов'язаний розробити та затвердити план забезпечення безперервності діяльності банку, у якому враховано безперервність функціонування заходів інформаційної безпеки в рамках процесу управління безперервністю діяльності банку.

Банк має право розробляти документи СУІБ у формі окремих документів або об'єднаних за типом (тематикою) в загальні документи, із зазначенням у них розділів, що відповідають визначеним напрямам (питанням) інформаційної безпеки.

Учасники інформаційних систем Національного банку зобов'язані налаштувати системи криптографічного захисту інформації в інформаційних системах Національного банку згідно з вимогами, які визначені у відповідній експлуатаційній документації кожної інформаційної системи Національного банку.

Банк зобов'язаний забезпечити захист інформаційних систем банку від несанкціонованого доступу та дій, направлених на відмову в обслуговуванні відповідно до вимог цього положення [28].

Отже, структура системи забезпечення інформаційної безпеки України (зокрема і структура системи суб'єктів, які його здійснюють) є похідною від тих пріоритетів та завдань, які ставить перед собою держава в інформаційній сфері. Тому саме державна інформаційна політика є визначальною для формування системи забезпечення інформаційної безпеки, а остання є похідною від неї.

2.3. Документація, що використовується в процесі впровадження системи управління інформаційною безпекою банківських установ

З урахуванням геополітичної і внутрішньої обстановки в Україні діяльність усіх державних органів має бути зосереджена на прогнозуванні, своєчасному виявленні, попередженні і нейтралізації зовнішніх і внутрішніх загроз національній безпеці, захисті суверенітету і територіальної цілісності

України, безпеки її прикордонного простору, піднесенні економіки країни, забезпеченні особистої безпеки, конституційних прав і свобод людини громадянина, викоріненні злочинності, вдосконаленні системи державної влади, зміцненні законності і правопорядку та збереженні соціально-політичної стабільності суспільства, зміцненні позицій України у світі, підтриманні на належному рівні її оборонного потенціалу і обороноздатності, радикальному поліпшенні екологічної ситуації.

Суверенітет, як повнота влади держави, самостійність держави, її незалежність від інших держав у внутрішній і зовнішній політиці, є одним із принципів міжнародного права, що закріплений в Статуті ООН, ряді міжнародних договорів і декларацій [39].

Суверенітет держави виступає визначальною і невід'ємною якістю держави, що відображає її верховенство на своїй території та незалежність (самостійність) у міжнародних відносинах.

Нерідко поняття суверенітету кореспондують не державі, а узагальнено державній владі. У міжнародному праві термін «суверенітет» уживається у зв'язку з правосуб'єктністю держави, в національному – пов'язується насамперед з процесом і результатами владарювання, здійснюваного державними органами і посадовими особами.

В чинній Конституції України суб'єктом здійснення права на самовизначення названі як українська нація, так і Український народ - громадяни України всіх національностей [16].

Інформаційний суверенітет, на думку дослідників, виступає володінням і розпорядженням національними інформаційними ресурсами, які включають усю належну державі інформаційну інфраструктуру, інформацію – незалежно від змісту, форми, часу і місця її створення, і забезпечується виключним правом держави на формування і здійснення національної інформаційної політики, власності на інформаційні ресурси, сформовані за державний кошт, створенням

національних систем інформації, встановленням режиму доступу інших держав до інформаційних ресурсів України.

Розвиток інформаційних технологій є не лише важливою державною функцією, а й обов'язковою умовою забезпечення ефективного використання нагромаджених суспільством інформаційних ресурсів для створення розвиненого і захищеного інформаційного середовища.

Інформаційне суспільство як своєрідний суспільний організм, що формується нині в багатьох розвинених країнах і в основі якого лежить раціональне використання інформатики та інформації в усіх основних сферах життя. Це суспільство постіндустріального типу з характерно вираженою роллю в його функціонуванні інформації, інформаційних структур і технологій як управлінських механізмів.

Співвідношення понять «національна безпека» та «інформаційна безпека», як і самі підходи до визначення категорії «інформаційна безпека» потребують подальшого дослідження.

Документація, що використовується в процесі впровадження системи управління інформаційною безпекою підприємства [25].

Адміністративні документи та документи верхнього рівня. Під час підготовки до впровадження СУІБ повинні бути створені відповідні документи. За наявності таких документів у банку вони повинні бути переглянуті 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:

1. адміністративні документи;
2. документи верхнього рівня;
3. документи середнього рівня;
4. документи нижнього рівня.

Адміністративні документи є обов'язковою начальною точкою підготовки до впровадження СУІБ, ці документи включають:

1. наказ про створення спеціального керівного органу з питань інформаційної безпеки (за необхідністю);

2. положення про спеціальний керівний орган з питань інформаційної безпеки (за його наявністю);

3. у разі відсутності спеціального керівного органу з питань інформаційної безпеки наказ про покладення обов'язків цього органу на існуючий керівний орган;

4. наказ про впровадження та функціонування СУІБ;

5. наказ про призначення керівника проекту впровадження та функціонування СУІБ;

6. положення про службу захисту інформації (підрозділ інформаційної безпеки);

7. положення про службу безпеки (охорона, пропускний та внутрішньо-банківський режим тощо);

8. посадові інструкції відповідальних за впровадження та функціонування СУІБ осіб;

9. 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.

Документи верхнього рівня є фактично основою СУІБ. Їх можна розділити на дві групи [25]:

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 або 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:

1. цілі СУІБ;
2. сфера застосування СУІБ;
3. організаційна структура банку, яка охоплюється СУІБ;
4. політика управління інформаційною безпекою;
5. опис методології оцінки ризиків;
6. звіт щодо оцінки ризиків;
7. опис методології оброблення ризиків з визначенням критеріїв прийняття залишкових ризиків;
8. план оброблення ризиків;
9. 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.

Слід зазначити, що для побудови ефективного управління інформаційною безпекою в банківських установах України 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.

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.

Організація інформаційної безпеки [25]:

1. зобов'язання працівників банку щодо збереження інформації з обмеженим доступом;

2. опис процедури управління санкціонуванням використання нових засобів оброблення інформації;

3. 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.

Управління ресурсами СУІБ [25]:

1. реєстр ресурсів СУІБ;

2. опис процедури поводження із інформацією з обмеженим доступом.

3. реєстр ресурсів СУІБ може складатися з набору декількох документів, зокрема документів, які створюються під час впровадження СУІБ.

Безпека людських ресурсів:

1. процедура управління персоналом;

2. критерії прийому персоналу;

3. опис процедури перевірки кандидатів на прийом на роботу (за наявності);

4. опис процедури навчання прийнятих на роботу працівників вимогам щодо інформаційної безпеки;

5. опис процедури підготовки посадових інструкцій;

6. опис дисциплінарного процесу щодо персоналу, який здійснив порушення безпеки;

7. опис процедури звільнення персоналу з точки зору припинення відповідальності, скасування прав доступу та повернення ресурсів СУІБ;

8. програма навчання персоналу.

Фізична безпека та безпека інфраструктури [25]:

- 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.

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.

Контроль доступу [25]:

- 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.

Придбання, розроблення та підтримка інформаційних систем [25]:

- 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;

Управління інцидентами інформаційної безпеки [25]:

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

Управління безперервністю бізнесу [25]:

- Опис дій в разі виникнення нестандартних ситуацій;

- Опис процедури тестування, підтримування та коригування планів безперервності бізнесу.

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 перелік 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.

Документи нижнього рівня можна поділити на дві групи [25]:

1. 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.

2. 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.

Висновки до другого розділу

Підсумовуючи необхідність запровадження управління інформаційною безпекою в банку вартує зазначити, що інформаційна безпека як стан захищеності інформаційного простору, який забезпечує його формування і розвиток в інтересах громадян, організацій і держави в цілому, захист від неправомірного зовнішнього і внутрішнього втручання; стан інформаційної інфраструктури, процесів, за яких інформація використовується суворо за призначенням і не впливає негативно на інформаційну чи інші системи як самої держави, так і інших країн при її використанні.

Для запровадження безпеки та ефективного управління інформаційною безпекою в українських банківських установах слід використовувати документацію яка поділяється на адміністративні документи, що являються документами верхнього рівня, документи середнього рівня фактично є технічними документами та документи нижнього рівня які вимагаються стандартами або інструкціями.

Закон України досить повно розкриває всі положення, але зі стрімким розвитком ІТ сфери, що напряму стосується банківських установ, підлягає

постійному удосконаленню норм та правил. Інформаційна безпека України як важлива складова національної безпеки передбачає системну превентивну діяльність органів державної влади по наданню гарантій інформаційної безпеки особі, соціальним групам та суспільству в цілому і спрямована на досягнення достатнього для розвитку державності та соціального прогресу рівня духовного та інтелектуального потенціалу країни.

Розділ 3.
РЕКОМЕНДАЦІЇ ЩОДО УДОСКОНАЛЕННЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В БАНКАХ

3.1. Удосконалення захищеності доступу до інформаційної діяльності банків

З метою надійного захисту інформації в банківських системах, каналах передачі даних безпечна робота забезпечується на таких рівнях:

Організаційний рівень - створення відповідних умов для захисту приміщень, комп'ютерів, облік конфіденційної, таємної інформації, контроль за розповсюдженням, копіюванням та діями персоналу;

Технічний рівень - апаратно-програмний захист, розподіл доступу до баз даних, мереж: передачі, введення паролів, криптозахист, накладання електронних цифрових підписів (ЕЦП).

У фінансових установах існує два підходи до захисту інформації над якими слід працювати та удосконалювати:

Автономний - направлений на захист конкретної ділянки або частини інформаційної системи, яка, як правило, є найбільш вразливою або може бути джерелом зловживань;

Комплексний - захищає інформаційну систему в цілому, всі її складові частини, приміщення, персонал тощо.

До основних засобів захисту інформації можна віднести наступні:

1. фізичні засоби;
2. апаратні засоби;
3. програмні засоби;
4. апаратно-програмні засоби;
5. криптографічні та організаційні методи.

Фізичні засоби захисту - це засоби, необхідні для зовнішнього захисту засобів обчислювальної техніки, території та об'єктів. Вони реалізуються на базі ЕОМ, які спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і несанкціонованого доступу до компонентів інформаційних систем, що захищаються.

Апаратні засоби захисту - це різні електронні, електронно-механічні та інші пристрої, які вмонтовуються в серійні блоки електронних систем обробки і передачі даних для внутрішнього захисту засобів обчислювальної техніки: терміналів, пристроїв введення та виведення даних, процесорів, ліній зв'язку тощо.

Програмні засоби захисту, які вмонтовані до складу програмного забезпечення системи, необхідні для виконання логічних та інтелектуальних функцій захисту.

Апаратно-програмні засоби захисту - це засоби, які основані на синтезі програмних та апаратних засобів.

Організаційні заходи захисту інформації складають сукупність заходів щодо підбору, перевірки та навчання персоналу, який бере участь у всіх стадіях інформаційного процесу [20].

Останнім часом корпоративні мережі майже всі підключаються до мережі Інтернет або навіть використовують її як свою основу. З огляду на те, яку загрозу може принести незаконне вторгнення в корпоративну мережу, необхідно використовувати відповідні методи захисту.

Для захисту корпоративних інформаційних мереж використовуються брандмауери. Брандмауер - це система чи комбінація систем, що дозволяють розділити мережу на дві чи більше частин і реалізувати набір правил, що визначають умови проходження пакетів з однієї частини в іншу. Як правило, ця межа проводиться між локальною мережею підприємства та Інтернетом, хоча її можна провести і у середині мережі.

Брандмауер пропускає через себе весь трафік і для кожного пакета приймає рішення - пропускати його чи відкинути. Для того щоб брандмауер міг приймати ці рішення, для нього визначається набір правил.

Брандмауер може бути реалізований як апаратними засобами (тобто як окремий фізичний пристрій), так і у вигляді спеціальної програми, запущеної на комп'ютері.

Брандмауер звичайно складається з декількох різних компонентів, включаючи фільтри або екрани, що блокують передачу частини трафіку.

Усі брандмауери можна розділити на два типи:

Пакетні фільтри, що здійснюють фільтрацію IP-пакетів засобами фільтруючих маршрутизаторів;

Сервери прикладного рівня, що блокують доступ до певних сервісів мережі.

Таким чином, брандмауер можна визначити як набір компонентів чи систему, що розташовується між двома мережами і має такі властивості [19]:

1. весь трафік із внутрішньої мережі у зовнішню та із зовнішньої мережі у внутрішню повинен пройти через цю систему;

2. тільки трафік, визначений локальною стратегією захисту, може пройти через цю систему;

3. система надійно захищена від проникнення.

Застосування криптографічного захисту, тобто кодування тексту з допомогою складних математичних алгоритмів, завойовує все більшу популярність. Звичайно, жоден з шифрувальних алгоритмів не дає цілковитої гарантії захисту від зловмисників, але деякі методи шифрування настільки складні, що ознайомитися зі змістом зашифрованих повідомлень практично неможливо.

Основними криптографічними методами захисту інформації є:

Шифрування з допомогою датчика псевдовипадкових чисел, яке полягає в тому, що генерується гамма шифру за допомогою датчика псевдовипадкових чисел і накладається на відкриті дані з урахуванням зворотності процесу;

Шифрування за допомогою криптографічних стандартів шифрування даних (з симетричною схемою шифрування), в основі якого використовуються перевірені і випробувані алгоритми шифрування даних з великою криптостійкістю;

Шифрування за допомогою пари ключів (з асиметричною системою шифрування), у яких один ключ є відкритим і використовується для шифрування інформації, другий ключ - закритим і використовується для розшифрування інформації.

Криптографічні методи захисту інформації широко використовуються в автоматизованих банківських системах і реалізуються у вигляді апаратних, програмних чи програмно-апаратних методів захисту. Використовуючи шифрування повідомлень в поєднанні з правильною установкою комунікаційних засобів, належними процедурами ідентифікації користувача, можна добитися високого рівня захисту інформації.

Криптографія є одним з найкращих засобів забезпечення конфіденційності і контролю цілісності інформації. Вона займає центральне місце серед програмно-технічних регуляторів інформаційної безпеки, є основою її реалізації [34].

Також як варіант захисту мережі можна використовувати систему надання права на доступ, автентифікації і реєстрації підключень.

Процес ідентифікації користувача називається автентифікацією. Стандартний метод автентифікації - використання імені користувача і пароля як попередня призначена пара ідентифікаторів, які користувач повинен ввести у відповідь на запит системи для діставання доступу до мережевих засобів. При цій, найбільш простій, формі автентифікації ідентифікатор користувача і пароль передаються по мережі відкритим текстом (тобто не в зашифрованому вигляді).

Сам процес автентифікації – порівняння переданої пари ідентифікаторів із записами таблиці, що знаходиться на сервері, – виконується відповідно до протоколу автентифікації по паролю (Password Authentication Protocol, PAP). Записи, що зберігаються, зашифровані, на відміну від передаваної пари ідентифікаторів, і це є слабкою стороною даного методу автентифікації.

Більш вдосконалена система запит-відповідь функціонує відповідно до протоколу автентифікації за запитом при встановленні зв'язку (Challenge Handshake Authentication Protocol, CHAP). Згідно цьому протоколу, агент автентифікації (ПЗ, що знаходиться на сервері) передає користувачеві ключ, за допомогою якого той шифрує своє ім'я і пароль і пересилає цю інформацію назад на сервер. Авторизація – процеснадання користувачеві права доступу до засобів системи, під час якого ім'я користувача і призначений йому пароль записуються в спеціальну таблицю системи.

Широко поширена система, що забезпечує високий рівень захисту при автентифікації, система запит-відповідь, в якій використовуються смарт-карти.

Регіструючи спроби доступу до мережі, можна легко визначити, чи не намагався неавторизований користувач проникнути у систему, а також дізнатися, чи не забув свій пароль хто-небудь з співробітників.

Блокування доступу. В багатьох організаціях як ідентифікатори користувачів вказувалися їх ініціали і прізвища. Зловмисникові, щоб спробувати проникнути в систему, досить було дізнатися такі. Розробники ПЗ створили програму блокування доступу до системи. Дуже часто ПЗ, що виконує блокування доступу, дозволяє задати ще один поріг: цим порогом визначається час, протягом якого система буде заблокована.

Розпізнавання – це гарантування, що інформація (пакет) надійшла від законного джерела законному одержувачу.

Справді, однією з найпоширеніших практик зловмисників у мережах є перехоплення пакетів та підміна їх своїми або скерування їх іншому адресату. Тому всі сучасні мережеві протоколи, зазвичай, оснащені засобами

розпізнавання. Одним з механізмів розпізнавання пакетів є розміщення у відправника та одержувача однакових генераторів псевдовипадкових чисел. Кожен пакет позначають псевдовипадковим числом, яке порівнюється з таким же числом одержувача.

Аналогічне завдання виконує електронний підпис - послідовність байтів, які формують спеціальними алгоритмами та автентичність яких можна перевірити.

Для розпізнавання використовують окремі сервери, які видають електронні сертифікати. Сервери сертифікації застосовують у всіх достатньо потужних операційних системах [20].

Одним з найвідоміших рішень є система централізованого розпізнавання Kerberos (вона реалізована програмним шляхом та сумісна з усіма типами систем. Працює система у клієнт-серверній парадигмі. Вона складається з програм-клієнтів, розміщених на робочих станціях користувачів, та серверних програм. Є три типи серверних програм: сервер розпізнавання, сервер надання дозволів та сервер адміністрування. У процесі розпізнавання клієнта беруть участь перші два з цих серверів. Кожен сервер має свою сферу дії, визначену змістом його бази даних користувачів).

Для вимірювання точності розпізнавання використовують два показники: відсоток хибного розпізнавання (False Acceptance Rate (FAR)) та відсоток хибного не розпізнавання (False Rejection Rate (FRR)) [36].

Отже, до основних рекомендацій щодо удосконалення захищеності доступу до інформаційної діяльності банківської установи, з урахуванням проблем захисту інформації в корпоративних мережах відносяться:

1. Регулярне оновлення програмного забезпечення серверного обладнання, пристроїв захисту та автоматизованих робочих місць користувачів. В рамках зазначеного, особливу увагу приділити критичним оновленням та оновленням безпеки операційних систем, оновленням веб-браузерів, програм для роботи з текстом та медіа контентом. Для реалізації оновлення операційної

системи та програмного забезпечення виробництва компанії Microsoft, як приклад, встановити сервер WSUS та налаштувати АРМ та серверне обладнання на автоматичне оновлення.

2. Активація використання стандартних міжмережевих екранів (брандмауерів) та/або встановлення додаткового програмного забезпечення, яке реалізує зазначені функції.

3. Перегляд парольної політики з метою виявлення нестійких паролів, паролів, встановлених за замовчуванням або не встановлених взагалі. Розробити єдині вимоги щодо складності паролю, частоти та порядку його зміни, а також забезпечити контроль за їх виконанням. Уникнути випадків зберігання логінів та паролів у відкритому вигляді на робочих столах моніторів та інших місцях файлової системи операційної системи, а також на паперових носіях інформації біля моніторів, клавіатур та інших загальнодоступних місць. На програмному рівні заборонити зберігання логінів та паролів у веб-браузерах, утилітах для роботи з базами даних, або іншому клієнтського програмному забезпеченні (Total Commander, FTP-, SSH- клієнтах тощо).

4. При організації корпоративного електронного поштового обміну на поштовому сервері налаштувати використання захищених протоколів, таких як POP3S (IMAP4S), SMTPS, уникнувши тим самим передавання автентифікаційної інформації (логінів та паролів) у відкритому вигляді.

5. За допомогою антивірусного програмного забезпечення, проводити сканування АРМ на предмет наявності шкідливого програмного забезпечення. Регулярно здійснювати оновлення антивірусного програмного забезпечення (державним органам керуватися наказом Адміністрації Держспецзв'язку від 26.03.2007 № 45 та вжити заходів щодо організації отримання оновлень з веб-сайту Центру антивірусного захисту інформації Держспецзв'язку).

6. Забезпечення ведення моніторингу працездатності активного мережевого, серверного обладнання, засобів захисту та каналів зв'язку. Як приклад, використовувати відповідне програмне забезпечення (Cacti, Nagios,

Munin, MRTG, Zabbix) та можливості протоколу SNMP, попередньо змінивши встановленні за замовчуванням значення «community string».

7. Розробка регламенту резервного копіювання критичних інформаційних ресурсів та конфігурацій апаратного забезпечення, а також передбачення порядку відновлення працездатності елементів ІТС на випадок збоїв.

8. З метою забезпечення можливості з’ясування об’єктивних обставин та причин на випадок порушення штатного режиму функціонування елементів ІТС або витоку інформації внаслідок несанкціонованих дій, забезпечити здійснення реєстрації та журналювання системних подій і подій безпеки (програмні або апаратні збої, доступ до баз даних, адміністративний доступ до обладнання та інше) та здійснювати їх регулярний аналіз.

3.2. Проведення аудиту для удосконалення управління інформаційною безпекою в банках

Система управління інформаційною безпекою в банківській установі передбачає проведення періодичних аудитів: як внутрішніх, силами самої організації, так і зовнішніх, що сертифікують органами (зрозуміло, при наявності сертифікації). Проведення аудиту доцільно і перед впровадженням СУІБ - для оцінки поточного стану безпеки і визначення основних напрямків її вдосконалення.

Аудит інформаційної безпеки – це системний процес одержання об'єктивних якісних і кількісних оцінок поточного стану безпеки інформаційної системи або інформаційно-телекомунікаційної системи, комплексна оцінка рівня інформаційної безпеки Замовника з урахуванням трьох основних факторів: персоналу, процесів та технологій [1].

До завдань аудиту входить оцінка відповідності документації ІБ критеріям аудиту, чинному законодавству і укладеними договорами, перевірка

дотримання персоналом банківської установи вимог регламентів з ІБ, а також виявлення шляхів поліпшення інформаційної безпеки.

Сфера аудиту включає:

1. підрозділи організації;
2. їх види діяльності;
3. бізнес процеси організації;
4. інформаційні активи;
5. ризики;
6. період проведення аудиту.

Для всіх організацій область перевірки визначається областю діяльності ІБ, заявленої самою організацією.

Основні напрямки аудиту інформаційної безпеки деталізуються на наступні: атестацію; контроль захищеності інформації; спеціальні дослідження технічних засобів і проектування об'єктів в захищеному виконанні [46].

1. Атестація об'єктів інформатизації за вимогами безпеки інформації:

- атестація автоматизованих систем, засобів зв'язку, обробки і передачі інформації;

- атестація приміщень, призначених для ведення конфіденційних переговорів;

- атестація технічних засобів, встановлених у виділених приміщеннях.

2. Контроль захищеності інформації обмеженого доступу:

- виявлення технічних каналів витоку інформації та шляхів несанкціонованого доступу до неї;

-контроль ефективності застосовуваних засобів захисту інформації.

3. Спеціальні дослідження технічних засобів на наявність побічних електромагнітних випромінювань і наведень (ПЕМВН):

- персональні ЕОМ, засоби зв'язку та обробки інформації;

- локальні обчислювальні системи;

- оформлення результатів досліджень у відповідності з вимогами

Держтехкомісій.

4. Проектування об'єктів в захищеному виконанні:

- розробка концепції інформаційної безпеки;

- проектування автоматизованих систем, засобів зв'язку, обробки і передачі інформації в захищеному виконанні;

- проектування приміщень, призначених для ведення конфіденційних переговорів [14].

Ще раз підкреслимо, що об'єктом аудиту в прийнятому нами розумінні не програмні або технічні засоби, а сам банк, його система управління ІБ. Аудит передбачає не тільки вивчення необхідної документації, а й перевірку наявності записів, регламентованих стандартами, а також проведення роз’яснювальної роботи з банківськими керівниками і спеціалістами для оцінки рівня їх знань в області інформаційної безпеки і визначення відповідності виконуваних дій по ІБ.

При необхідності аудит може бути розширено - включати аналіз IT інфраструктури, тобто конкретних програмно-технічних засобів для забезпечення ІБ. Аудит СУІБ - це не раптова інспекторська акція. Його програму потрібно завжди розробляти заздалегідь і погоджувати з керівництвом банку. Начальників підрозділів слід своєчасно оповіщати про майбутню перевірку. І сприйняття аудиту як такого персоналом організації повинно бути максимально адекватним: це не захід, за підсумками якого за виявлені порушення летять голови з плечей, а комплексні дії, спрямовані на пошук слабких місць в ІБ з метою їх усунення.

Зрозуміти і донести цю думку до співробітників - пряме завдання керівництва банку. В іншому випадку підрозділи будуть приховувати необхідну інформацію і всіляко перешкоджати проведенню аудиторської перевірки. В ході комплексної перевірки складається список невідповідностей банківської СУІБ вимогам стандартів і внутрішніх документів з інформаційної безпеки. На його основі формується перелік рекомендацій щодо виправлення виявлених

недоліків та підвищення результативності СУІБ, а також з розвитку технічної інфраструктури, спрямованої на підвищення рівня ІБ банку. Аудит має і ряд неявних переваг: оцінку проведеного в організації аналізу ризиків інформаційних ресурсів і заходів щодо їх зниження; об'єктивність інформації для аналізу керівництвом; підвищення компетентності співробітників в питаннях ІБ; обгрунтування інвестицій на вдосконалення системи захисту та забезпечення їх окупності; не упереджені висновки про ступінь відповідності банківським бізнес завданням внутрішніх механізмів захисту і їх здатності забезпечити безперервність бізнесу; підтвердження для клієнтів якості надаваних банком послуг.

3.3. Рекомендації щодо інформаційної безпеки для персоналу та клієнтів банків

Керівники банківських установ відіграють вирішальну роль у процесі управління безпекою даних у рамках всього процесу управління операційними ризиками. Отже, рада директорів несе відповідальність за розробку та покращення операційної бази для управління інформаційною безпекою; і визначити максимальну ефективність роботи банківської установи по відношенню до інформаційної безпеки; і забезпечити належні шляхи відходу та правильне подолання ризиків, який банк бере на себе.

Операційну структуру можна розглядати як сукупність стратегій, прийнятих банками у сфері безпеки даних; методи, які банки використовують для визначення, оцінки та мінімізації ризиків, а також їх організаційну структуру, повноваження та обов'язки щодо управління ІБ.

Роль вищого керівництва банку у цьому процесі пов'язана з встановленням передумов для ефективного впровадження та реалізації політики, стратегій та процедур, які рада встановила та затвердила для управління ІБ, а також оцінку та моніторинг загального процесу та здійснення

коригуючих дій у разі виявлених недоліків та недоліків або змін у внутрішньому та / або зовнішньому середовищі. Деякі заходи, прийняті для підвищення безпеки даних, також пов'язані з вербуванням та навчанням посадових осіб банку; модернізація обладнання та програмних продуктів, які використовують банки; а також впровадження ефективної політики внутрішнього контролю.

Оперативне управління ризиком, пов'язаним із безпекою даних, зазвичай відповідає спеціалізованим підрозділам інформаційної безпеки, які можуть звітувати безпосередньо відділам інформаційних технологій або комітетам з управління ризиками. Безпосередній нагляд за діяльністю банківських службовців їх керівниками з точки зору дотримання встановлених правил та процедур внутрішнього контролю, безумовно, є важливою умовою зменшення ризику шахрайства чи бездіяльності внутрішніх банків [47].

Організаційний захист інформації є організаційним початком в загальній системі захисту конфіденційної інформації банківської установи. Від повноти і якості вирішення керівництвом банківської установи і посадовими особами організаційних завдань залежить ефективність функціонування системи захисту інформації в цілому. Роль і місце організаційної захисту інформації в загальній системі заходів, спрямованих на захист конфіденційної інформації підприємства, визначаються винятковою важливістю прийняття керівництвом своєчасних і вірних управлінських рішень з урахуванням наявних в його розпорядженні сил, засобів, методів і способів захисту інформації і на основі чинного нормативно-методичного апарату.

Організаційний захист інформації розроблений за допомогою вибору конкретних сил і засобів (які включають в себе правові, інженерно-технічні та інженерно-геологічні) реалізувати на практиці сплановані керівництвом банку заходи щодо захисту інформації. Ці заходи вживаються в залежності від конкретної обстановки в банківській установі, пов'язаної з наявністю можливих загроз, що впливають на захищається інформацію і ведуть до її витоку.

Роль керівництва підприємства у вирішенні завдань із захисту інформації важко переоцінити. Основними напрямками діяльності, здійснюваної керівником підприємства в цій галузі, є: планування заходів щодо за-хисту інформації та персональний контроль за їх виконанням, прийняття рішень про безпосередньому доступі до конфіденційної інформації своїх спів-робітників і представників інших організацій, розподіл обов'язків і завдань між посадовими особами та структурними підрозділами , аналітична робота і т. д.

Мета прийнятих керівництвом підприємства і посадовими особами організаційних заходів – виняток витоку інформації і, таким чином, зменшення або повне виключення можливості нанесення підприємству збитку, до якого цей витік може привести.

Для унеможливлення віддаленого захвату управління вашим комп'ютером, з якого здійснюється обмін електронними платіжками, ми рекомендуємо дотримуватися додаткових заходів забезпечення безпеки [47]:

1. Комп'ютер, з якого здійснюється підготовка і відправка електронних документів в банк, необхідно виділити в окрему довірену зону, виключивши його із загальної локальної мережі організації.

2. Для виділеної довіреної зони встановити повну заборону на доступ до ресурсів мережі інтернет, за винятком налаштувань, необхідних для коректної роботи транспортної підсистеми системи.

3. Здійснюйте постійний контроль платіжних документів, що відправляються, при роботі з системою, а також стан свого розрахункового рахунку.

4. Намагайтеся не працювати з не довірених комп'ютерів (інтернет-кафе, кіоски і так далі).

Також для додаткової безпеки Клієнти банку мають використовувати токен. Електронні ключі eToken PRO (Java) – персональний засіб аутентифікації та захищеного зберігання даних, що призначені для користувача. Апаратно

підтримує роботу з цифровими сертифікатами та електронним цифровим підписом (ЕЦП) [50].

Зовні USB-ключ eToken PRO (Java) виглядає як показано на рисунку 3.1, а на рисунку 3.2 – смарт-карта.

Рис. 3.1 USB-ключ eToken PRO (Java)

Рис. 3.2 Смарт-карта eToken PRO (Java)

Характеристики eToken PASS здебільшого схожі на характеристики попереднього токену. Це автономний генератор одноразових паролів, що не вимагає підключення до комп'ютера і встановлення додаткового програмного забезпечення. Може використовуватися в будь-яких операційних системах, а також при доступі до захищених ресурсів з мобільних пристроїв і терміналів, які не мають USB-роз'єму або пристрою читання смарт-карт [49]. На рисунку 3.4 зовнішній вигляд брелоку eToken PASS.

Рис. 3.4 Брелок eToken PASS

Додаткові методи захисту ЕЦП ключа клієнта:

1. Зберігати ключ ЕЦП на USB – токені. З нього неможливо ні вилучити ключ, ні скопіювати. USB – токен зберігати в сейфі, підключати до комп’ютера лише для роботи з системою. Після роботи виймати токен з комп’ютеру та повертати до сейфу.

2. Використовувати СМС аутентифікацію для ключів на Зовнішніх носіях. Після вводу паролю на ключ буде приходити СМС з одноразовим паролем.

3. Використовувати СМС – аутентификацію для підтвердження платежів з сумою більше порогової (встановлюється адміністратором банку за заявою клієнта).

4. Якщо на комп’ютері для доступу в мережу Інтернет використовується фіксована IP адреса, зафіксувати її в банку (вносить в картку клієнта адміністратор банку, за заявою клієнта).

При виборі пароля доступу до секретного ключа ЕЦП рекомендуємо виконувати наступні правила:

1. Вибирайте свій пароль самостійно і нікому його не повідомляйте.

2. Постарайтеся запам'ятати свій пароль. Якщо Ви все-таки записали пароль на папері, зберігаєте його в місці, недоступному для сторонніх осіб.

3. Пароль повинен містити не менше 6 різних символів. Чим складніше буде пароль, тим важче його буде підібрати.

4. Обов'язково змініте пароль в тому випадку, якщо він став відомий сторонній особі.

5. Не використовуйте як пароль:

- послідовності символів складаються з одних цифр (у тому числі дати, номери телефонів і тому подібне);

- послідовності букв, що повторюються, або цифр;

- підряд клавіатури, що йдуть в розкладці, або в алфавіті символи;

- імена і прізвища.

Необхідно забезпечити заходи по захисту комп'ютера, з якого здійснюється робота в системі:

1. Забезпечте безпеку приміщення і обмежте доступ співробітників і сторонніх осіб до ключів ЕЦП і комп'ютерам з Системою. Доступ повинні мати лише довірені особи.

2. Використовуйте ліцензійне програмне забезпечення з перевірених і надійних джерел. Регулярно виконуйте оновлення операційної системи і прикладного програмного забезпечення, особливо в частині безпеки.

3. На комп'ютері має бути встановлене антивірусне програмне забезпечення з регулярно оновлюваними базами. Періодично здійснюйте повну перевірку комп'ютера на предмет наявності вірусів.

4. На комп'ютері не повинні запускатися програми, отримані з неперевірених джерел (особливу небезпеку можуть представляти програми, отримані по електронній пошті або через Інтернет).

5. Вкрай бажано встановити на комп'ютер персональний міжмережевий екран.

Система «Internet клієнт-банк» призначена для підготовки, передачі по каналах зв'язку і зберігання фінансових документів, представлених в електронному вигляді (далі – «Електронний документ»).

Безпека обміну електронними документами забезпечується за допомогою шифрування таких документів, використання електронного цифрового підпису, який є аналогом власноручного підпису, а також наявністю захищеного каналу передачі інформації.

Шифрування і підпис електронних документів здійснюється за допомогою секретного ключа ЕЦП, що знаходиться на спеціально призначеному для цього зовнішньому носієві, наприклад, дискеті, флеш-носієві. Доступ до секретного ключа захищений паролем, відомим лише власникові ключа ЕЦП. Не маючи у розпорядженні секретного ключа і не знаючи пароля доступу до нього, неможливо сформувати ЕЦП під електронним документом.

Виконання нижченаведених рекомендацій є необхідною умовою забезпечення безпеки розрахунків в системі.

Для виключення доступу сторонніх осіб до Ваших секретних ключів ЕЦП необхідно дотримувати наступні заходи безпеки ключових носіїв:

1. Не зберігаєте ключі ЕЦП на жорсткому диску комп'ютера. Зберігаєте ключі ЕЦП лише на Зовнішньому носієві в недоступному для сторонніх осіб місці

2. Пароль доступу до зовнішнього носія з ключем ЕЦП слід зберігати окремо. Не записуйте пароль доступу до секретного ключа на етикетках Зовнішніх носіїв.

3. Підключайте Зовнішній носій з ключем ЕЦП лише у момент підписання Електронних документів. Не залишайте Зовнішній носій з ключем ЕЦП постійно підключеним до комп'ютера

4. Використовуйте Зовнішній носій з ключами ЕЦП лише для входу в Систему і підписання Електронних документів.

5. Не використовуйте зовнішній носій з ключами ЕЦП для яких-небудь інших цілей, зокрема, не зберігаєте на них інформацію довільного вмісту, що не відноситься до роботи в системі.

6. Не копіюйте вміст зовнішнього носія і не передавайте його нікому

навіть на короткий час.

7. Закінчивши роботу в системі або перервавши її (навіть на декілька хвилин), не забудьте витягувати зовнішній носій і прибрати його в доступне лише Вам місце.

8. В разі заміни особи, наприклад, при звільненні співробітника, використовуючого ЕЦП, негайно повідомите про це у відділення банку вашому менеджерові і зробіть генерацію нових ключів ЕЦП.

9. У випадку якщо зовнішній носій з ключами ЕЦП загублений, або у вас є підозра, що такі ключі опинилися у сторонніх осіб, навіть на короткий час, негайно повідомите про це адміністратора системи в банку.

Висновки до третього розділу

До основних рекомендацій щодо удосконалення управління інформаційною безпекою в банківській установі можна віднести удосконалення надійного захисту інформації в банківських системах, каналах передачі даних. Безпечна робота забезпечується на організаційному рівні та технічному рівні. Також слід застосовувати різного типу засоби та методи.

До рекомендацій слід віднести аудит інформаційної безпеки банківської установи. Аудит - це методичний незалежний задокументований процес, метою якого є збір свідчень та їх об'єктивний аналіз для встановлення ступеня відповідності певним критеріям. Під критеріями аудиту розуміють зазначені вище стандарти, внутрішню політику і процедури СУІБ, законодавчу базу, контрактні зобов'язання, норми і оптимальні рекомендації, розроблені на практиці.

Що стосується персоналу, то слід передбачити проведення занять, спрямованих на підвищення обізнаності співробітників відомства щодо безпечного користування сервісами електронної пошти, передачі файлів, перегляду інформаційних ресурсів, розміщених в мережі Інтернет, а також

описати порядок дій користувачів у разі виявлення ознак порушення штатного режиму функціонування інформаційних систем чи елементів ІТС в цілому. А для клієнтів банку слід притримуватись низки правил безпечного користування послугами банківської установи.

ВИСНОВКИ

В даній роботі досліджено та підтверджено актуальність теми управління інформаційною безпекою в банківських установах. Захист доступу до інформації має актуальне значення. При цьому основними завданнями інформаційної безпеки є збереження інформаційної системи банку в цілісності, захист і гарантування повноти і точності інформації, яку він видає, мінімізація руйнувань і модифікації інформації, якщо такі трапляються.

1. Отже, забезпечення безпечної діяльності необхідне для будь-яких підприємств і установ, а особливо це стосується банківських установ, через те, що саме банки мають величезний вплив на розвиток економіки не тільки в рамках держави, але й у всьому світі. Починаючи від державних банківських установ і закінчуючи малими банкам. Різниця полягатиме лише в тому, які засоби і методи й у якому обсязі будуть потрібні для забезпечення їх безпеки.

2. Дослідження показує, що сучасна банківська структура для забезпечення інформаційної безпеки потребує у впровадженні нових методів використання технологій. До основних методів управління інформаційною безпекою банківської установи відносимо: механічні, апаратні і програмні, метод форматування накопичувача, криптографічний метод. До основних засобів захисту інформації відносимо: засоби авторизації користувачів, міжмережеві екрани, віртуальні приватні мережі, засоби контентної фільтрації, засоби антивірусного захисту.

3. Аналіз проблематики, пов'язаної з управлінням інформаційною безпекою банківської установи показав, що необхідно враховувати специфіку даного аспекту безпеки, що полягає у тому, що інформаційна безпека є складовою частиною інформаційних технологій області, що розвивається надзвичайно високими темпами. До основних проблем відносимо: людський фактор, ризики, порушення правил, умисні сторонні дії, фінансові втрати тощо.

Для вирішення багатьох проблем застосовують серію міжнародних стандартів «International Organization for Standardization».

4. Розглянувши необхідність запровадження управління інформаційною безпекою в банку, дійшли висновку, що зі зв'язком стрімкого розвитку IT сфери та постійним змінам в економічному стані світу – необхідно постійно працювати над управлінням інформаційною безпекою та боротьбою із загрозами.

5. Дослідивши низку законів України, прийшли висновку, що Україна не відстає у розвитку в сфері інформаційної безпеки, а постійно оновлює положення згідно із змінами у світі, але все ще залишається над чим працювати. Зокрема є потреба розвивати документацію, що використовується в процесі впровадження системи управління інформаційною безпекою банківської установи. Що в свою чергу поділяються на адміністративні документи, що являються документами верхнього рівня, документи середнього рівня фактично є технічними документами та документи нижнього рівня які вимагаються стандартами або інструкціями.

6. Щодо рекомендації по удосконаленню захищеності доступу до інформаційної діяльності банківської установи, то дослідження пропонує низку засобів і методів по удосконаленню управління інформаційною безпекою. А також - регулярне оновлення програмного забезпечення серверного обладнання, активація використання стандартних міжмережевих екранів, перегляд парольної політики, налаштувати використання захищених протоколів, застосування антивірусного програмного забезпечення, моніторингу працездатності обладнання, розробка регламенту резервного копіювання та здійснення реєстрації та журналювання подій безпеки. Окремо виступає питання аудиту банківської установи, що є дуже важливою частиною в управлінні інформаційною безпекою.

7. У дослідженні також наведенні рекомендації для персоналу та клієнтів банківської установи. Слід передбачити проведення тренінгів, задля розвитку

співробітників, щодо безпечного користування сервісами електронної пошти, передачі файлів, перегляду інформаційних ресурсів, закритої інформації тощо. В свою чергу клієнти банківських установ також мають бути пильними до забезпечення своєї ж безпеки. Основними рекомендаціями є - не працювати з не довірених комп'ютерів, контроль платіжних документів, виділити в окрему довірену зону, використання eToken, зафіксувати IP, СМС аутентифікація та забезпечення безпеки ЕПЦ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аудит інформаційної безпеки інформаційних систем та інформаційно телекомунікаційних систем [Електронний ресурс]. – Режим доступу: http://www.uss.gov .ua /audit-of-information-security.

2. Батаева И. П. Защита информации и информационная безопасность / И. П. Батаева // Журнал. Труды Международного симпозиума «Надежность и качество». Выпуск: том 1. – 2012.

3. Батаева И. П. Информация и банковская деятельность / И. П. Батаева // Журнал. Труды Международного симпозиума «Надежность и качество». Выпуск: том 2. – 2012.

4. Голиков А. М. Основы информационной безопасности / А. М. Голиков. – Томск: Томск, гос. ун-т систем упр. и радиоэлектроники, 2017. – 288 с. [Электронный ресурс]. – Режим доступа: http://www.dut.edu.ua/uploads/l_818_97713647.pdf

5. Громов В. И. Энциклопедия компьютерной безопасности / В. И. Громов, Г. А. Васильев. – М.: РИФ, 2015. – 334 с.

6. Диев С. Д. Организация и современные методы защиты информации / С. Д. Диев, Л. Г. Шаваев – М.: Концерн «Банковский Деловой Центр». 2008 – 472 с.: книга [Электронный ресурс]. – Режим доступа: http://www.kodges.ru/komp/bezop/16785–organizacija–i–sovremennye–metody–zashhity.html

7. Димитрова Т. Е-токин – ефективный инструмент в банковской безопасности / Т. Димитрова // Образование и наука. – 2015. – № 38. – с. 23-27.

8. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты / В. В. Домарев. – К.: Изд-во «ДиаСофт», 2012. – 693с.

9. ДСТУ 3396.0–96 Захист інформації. Технічний захист інформації. Основні положення.

10. Енциклопедія банківської справи України / Ред. кол.: В. С. Стельмах (голова) та ін. – К.: Молодь, Ін Юре, 2011. – 680 с.

11. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу (із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806). – НД ТЗІ 1.1-002-99, ДСТСЗІ СБ України, Київ, 1998.

12. Закон України «Про національну безпеку України» [Електронний ресурс].– Режим доступу: http://zakon3.rada.gov.ua/laws/show/964-15

13. Інформаційна безпека банківської установи [Електронний ресурс]. – Режим доступу: http://tihoma.esy.es/page10.html

14. Інформаційна безпека інформаційно-комунікаційних систем: навчальний посібник. Лабораторний практикум. Частина 2. Комплекси технічного захисту інформації. – К.: НАУ, 2016.

15. Князев А. А. Информационная война / А. А. Князев // Энциклопедический словарь СМИ. – Бишкек: Издательство КРСУ, 2012.

16. Конституція України [Електронний ресурс]. – Режим доступа: http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

17. Конфіденційність доступність і цілісність інформаційної безпеки [Електронний ресурс]. – Режим доступу: https://stboinf.wordpress.com/ 2013/03/12/

18. Лексов И. Компьютерные вирусы / И. Лексов [Електронний ресурс]. – Режим доступу: http://www.victoria.lviv.ua/html/informatika/lecture10.htm

19. Ленков С. В. Методы и средства защиты информации. Том II. Информацион-ная безопасность / С. В. Ленков. – К.: Арий, 2013.

20. Ленков С. В. Основы защиты информации / С. В. Ленков, А. Д. Перегудов, В. А. Хорошко – К.: Арий, 2017. – Том I. Несанкционированное получение информации. – 464 с.

21. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховский: Навч. посібник. – К. : КНТ, 2016. – 280 с.

22. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов / С. И. Макаренко. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.

23. Мартынов А. Управление информационной безопасностью в банках. Особенности, реализация, аудит / А. Мартынов [Електронний ресурс]. – Режим доступу: http://www.softlab.ru/upload/iblock/a49/a490ad221847e7caaeeea7ccbd6ad329.pdf

24. Мельников В. П. Информационная безопасность и защита информации: Учебник / В. П. Мельников, С. А. Клеименов, А. М. Петраков. – М.: Академия, 2012.

25. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/en/v0365500-11

26. Необхідність захисту інформації. Поняття загрози інформаційній безпеці. Види загроз інформаційної безпеки [Електронний ресурс]. – Режим доступу: http://um.co.ua/8/8-6/8-67965.html

27. Об информации, информатизации и защите информации: Федеральный Закон Российской Федерации от 20 февраля 1995 года № 24-ФЗ [Електронний ресурс].– Режим доступу: http://pravo.gov.ru/proxy/ips/?docbody=&link_id=0&nd=102034046

28. Постанова «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/v0095500-17#n12

29. Ретов С. О. Удосконалення системи інформаційної безпеки на підприємстві ТОВ "Нива" / С. О. Ретов [Електронний ресурс]. – Режим доступу: http://ukrefs.com.ua/page,4,112220-Sovershenstvovanie-sistemy-informacionnoiy-bezopasnosti-na-predpriyatii-OOO-Niva-Uinskogo-raiyona.html

30. Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин [Електронний ресурс]. – Режим доступу: http://um.co.ua/8/8-6/9-77981.html

31. Різник Н. С. Теорії та змістово-типологічні характеристики безпеки підприємства / Н. С. Різник, Н. І. Корецька // Економічний форум. – 2013. – № 1. – 486 с. – С. 238-243.

32. Савченко А. Інформаційна безпека банків: шляхи розв'язання проблеми / А. Савченко, І. Івченко // Вісник Національного банку України. – 2010. – № 05 (171). – С. 3-5.

33. Система управління інформаційною безпекою підприємства [Електронний ресурс]. – Режим доступу: http://stud.com.ua/43080/ekonomika/sistema_upravlinnya_informatsiynoyu_bezpekoyu_pidpriyemstva

34. Скиба Б. Ю. Руководство по защите от внутренних угроз информационной безопасности / Б. Ю. Скиба, Б. А. Курбатов – М.: издательство Питер, 2008. – 320 с.

35. Сьомкін С. Н. Основи правового забезпечення захисту інформації. Навчальний посібник для вузів / С. Н. Сьомкін, А. Н. Сьомкін. – М.: Ил., 2008. – 238 с.

36. Тарасов Т. Шляхи запобігання та протидії промисловому шпигунству // Бизнес и безопасность. – 2017. – № 3 – с. 7-11.

37. Тихонов В. А. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты / В. А. Тихонов, В. В. Райх. – М.: Гелиос АРВ, 2006.

38. Тютюнник А. В. Банковское дело. Финансы и статистика / А. В. Тютюнник, А. В. Турбанов. – М.: ИНФРА-М, 2015. – 204 с.

39. Устав Организации Объединённых Наций и Устав Международного Суда [Электронный ресурс]. – Режим доступа: http://zakon2.rada.gov.ua/laws/show/995_010

40. Хорев П. Б. Методы и средства защиты информации в компьютерных сетях / П. Б. Хорев – М.: Академия, 2015. – 248 с.

41. Хорошко В. О. Основи інформаційної безпеки / В. О. Хорошко, В. С. Чередниченко, М. Є. Шелест. – К.: ДУІКТ, 2008. – 138 с.

42. Чипига А. Ф. Оценка эффективности защищенности автоматизированных систем от несанкционированного доступа / А. Ф. Чипига, В. С. Пелешенко. – М., 2014.

43. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. − М.: ДМК Пресс, 2017. – 328 с.

44. Шуйский А. А. Системный анализ в защите информации: Учеб. пособ. для студ. вузов, обучающихся по специальностям в области информационной безопасности / А. А. Шуйский, А. А. Шелупанов. – М.: Гелиос АРВ, 2015.

45. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – СПб.: Наука и техника, 2014.

46. Ярочкин В. И. Информационная безопасность: Учебник для студентов / В. И. Ярочкин – М.: Акад. проект Гаудеамус, 2-е изд., 2014. – 544 с.

47. Bojidar Bojinov. Challenges for ensuring the informationsecurity of commercial banks [Електронний ресурс]. – Режим доступу: https://mpra.ub.unimuenchen.de/75772/1/MPRA_paper_75772.pdf

48. Deloitte - India Banking Fraud Survey – Edition II. – 2015.

49. eToken PASS [Електронний ресурс]. – Режим доступу: http://www.infobezpeka.com/products/ keyforauntification/?view=554

50. eToken PRO (Java) [Електронний ресурс]. – Режим доступу: http://www.infobezpeka.com/products/keyforauntification/?view=552

51. ISO/IEC [Електронний ресурс]. – Режим доступу: https://www.iso.org/isoiec-jtc-1.html

ДОДАТКИ

Додаток А.

Міжнародні стандарти для системи управління інформаційною безпекою

Стандарт	Опис
1. Серія ISO 27000 «Міжнародні стандарти для системи управління інформаційною безпекою»	
ISO/IEC 27000:2009	Визначення і основні принципи
ISO/IEC 27001:2005	Інформаційні технології — Методики безпеки — Системи менеджменту інформаційної безпеки — Вимоги (BS 7799-2:2005)
ISO/IEC 27002:2005	Інформаційні технології — Методики безпеки — Практичні правила управління інформаційною безпекою (попередній код ISO/IEC 17799:2005
ISO/IEC 27003:2010	Настанова з впровадження системи управління інформаційною безпекою
ISO/IEC 27005:2008	Інформаційні технології — Методики безпеки — Управління ризиками інформаційної безпеки (на основі стандарту BS 7799-3:2006)
ISO/IEC 27006:2007	Інформаційні технології — Методики безпеки — Вимоги до організацій, що провадять аудит і сертифікацію систем менеджменту інформаційної безпеки
ISO/IEC 27011:2008	Керівництво з менеджменту інформаційної безпеки для телекомунікацій
ISO/IEC 15408	Загальні критерії оцінки безпеки інформаційних технологій
2. Серія ISO 13335 «Міжнародні стандарти безпеки інформаційних технологій»	
ISO 13335-1:2004	Інформаційні технології — Керівництво по управлінню IT безпекою — Концепції і моделі для управління безпекою інформаційних і телекомунікаційних технологій
ISO 13335-3:1998	Інформаційні технології — Керівництво по управлінню IT безпекою — Методи управління IT безпекою
ISO 13335-4:2000	Інформаційні технології — Керівництво по управлінню IT безпекою — Вибір механізмів захисту
ISO 13335-5:2001	Інформаційні технології — Керівництво по управлінню IT безпекою — Керівництво по управлінню мережевою безпекою

РЕЗУЛЬТАТ

Переваги застосування
Забезпечення безперервності
Мінімізація ризиків
Забезпечення комплексного та централізованого контролю рівня захисту інформації
Забезпечення цілісності, конфіденційності та доступності критичних інформаційних ресурсів інформаційно-комунікаційних систем та мереж
Зниження витрат на інформаційну безпеку

Додаток Б.

Основні проблеми управління інформаційною безпекою в банківських установах