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: **«ПОЛІТИКА ІНФОРМАЦІЙОЇ БЕЗПЕКИ БАНКУ»**

Студент групи УБДМ-61Стадник Ростислав Едуардович _____
(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 Стаднику Ростиславу Едуардовичу

1. Тема роботи: «ПОЛІТИКА ІНФОРМАЦІЙОЇ БЕЗПЕКИ БАНКУ» затверджена наказом ректора від «___» _____ 20__ р. № __.

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

3. Об’єкт дослідження: інформаційна безпека банку.

4. Предмет дослідження: політика інформаційної безпеки банку.

5. Мета дослідження: розробка рекомендацій щодо політики інформаційної безпеки банку.

6. Перелік питань, які мають бути розроблені:
1. Теоретичні засади інформаційної безпеки банку.
2. Забезпечення інформаційної безпеки банку.
3. Вимоги до політики інформаційної безпеки банку.

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

Науковий керівник: Мордас І. В.

Завдання прийнято до виконання: Стадник Р. Е.

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

КАЛЕНДАРНИЙ ПЛАН
виконання магістерської атестаційної роботи
студентом Стадником Ростиславом Едуардовичем

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-61Стадник Ростислав Едуардович _____
(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 – 85 сторінок.

Об’єкт дослідження – інформаційна безпека банку.

Предмет дослідження – політика інформаційної безпеки банку.

Мета дослідження – розробка рекомендацій щодо політики інформаційної безпеки банку.

У магістерській атестаційній роботі проаналізовано теоретичні засади інформаційної безпеки банку; досліджено підходи до забезпечення інформаційної безпеки банку; визначено вимоги до політики інформаційної безпеки банку.

ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА БАНКУ, ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ, ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ, ПОЛІТИКА ІФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ.

ЗМІСТ

ВСТУП……8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ..……10
1.1. Сутність інформаційної безпеки банку……10
1.2. Ризики та загрози інформаційній безпеці банку……12
1.3. Нормативно-правове забезпечення інформаційної безпеки банку……16
Висновки до першого розділу……..25
РОЗДІЛ 2. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ……26
2.1. Методи забезпечення інформаційної безпеки банку……..…26
2.2. Програми забезпечення інформаційної безпеки банку……..39
2.3. Алгоритм забезпечення інформаційної безпеки банку……..46
Висновки до другого розділу……...49
РОЗДІЛ 3. РЕКОМЕНДАЦІЇ ЩОДО ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ……..51
3.1. Вимоги до політики інформаційної безпеки банку……..……..51
3.2. Розробка політики інформаційної безпеки банку……..58
Висновки до третього розділу……66
ВИСНОВКИ……..69
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……72
ДОДАТКИ……77

ВСТУП

Актуальність теми. Стратегія інформаційної безпеки банків дуже сильно відрізняється від аналогічних стратегій інших компаній та організацій. Це зумовлено специфічним характером загроз, а також публічною діяльністю банків, які змушені робити доступ до рахунків досить легким з метою зручності для клієнтів.

Важлива роль у цьому процесі відводиться саме банківському сектору, за допомогою якого здійснюється розподіл та перерозподіл грошових потоків та їх концентрація у пріоритетних галузях економіки; запобігання відпливу капіталів за кордон; забезпечення стабільності національної грошової одиниці; здійснення виваженої політики внутрішніх і зовнішніх запозичень та ін.

Інформація, яка зберігається та обробляється в банківських системах представляє собою реальні гроші. Цілком зрозуміло, що незаконне маніпулювання з такою інформацією може привести до серйозних збитків. Конкурентоспроможність банку залежить від того, наскільки клієнтові зручно працювати з банком, наскільки клієнт довіряє банку, а також наскільки широкий спектр його послуг, включаючи послуги, пов'язані з віддаленим доступом. Тому клієнт повинен мати можливість швидко розпоряджатися своїми грошима. Але така легкість доступу до грошей підвищує ймовірність злочинного проникнення в банківські системи.

З огляду на зазначене тема дипломної роботи є актуальною, а використання її результатів сприятиме підвищенню рівня інформаційної безпеки банків.

Мета і завдання дослідження. Мета роботи полягає у розробці рекомендацій щодо політики інформаційної безпеки банку.

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

1. Проаналізувати теоретичні засади інформаційної безпеки банку.
2. Дослідити підходи до забезпечення інформаційної безпеки банку.
3. Визначити вимоги до політики інформаційної безпеки банку.

Об'єкт дослідження – інформаційна безпека банку.

Предмет дослідження – політика інформаційної безпеки банку.

Методи дослідження. У роботі були використані методи аналізу та синтезу, індукції та дедукції, аналогії, порівняння та ін.

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

Розділ 1 ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ

1.1. Сутність інформаційної безпеки банку

У перекладі з грецької поняття безпека означає «володіти ситуацією» [1]. В економічній літературі безпека банку трактується як: стан стійкої життєдіяльності, за якого забезпечується реалізація мети банку та основних його інтересів, захист від внутрішніх і зовнішніх дестабілізуючих факторів незалежно від умов функціонування; властивість своєчасно й адекватно реагувати на всі негативні прояви внутрішнього і зовнішнього середовища банку; здатність протистояти різним посяганням на власність, діяльність і імідж банку, створювати ефективний захист від внутрішніх і зовнішніх загроз [14]; стан захищеності банку від внутрішніх і зовнішніх загроз; система заходів, які забезпечують захищеність інтересів власників, клієнтів, працівників і керівництва банку від зовнішніх і внутрішніх загроз .

Більш системне визначення поняття «безпека банку» наведено у роботі В. Гамзи та І.Ткачука: «це сукупність зовнішніх і внутрішніх умов банківської діяльності, при яких потенційно небезпечні для банківської системи (окремого банку) дії або обставини попереджені, припинені або зведені до такого рівня, при якому не здатні нанести збиток установленому порядку банківської діяльності (функціонуванню банку, збереженню й відтворенню майна й інфраструктури банківської системи або окремого банку) і перешкодити досягненню банком уставних цілей» [10].

У даному визначенні забезпечення безпеки банку має здійснюватися на двох рівнях: рівні окремого банку на підставі реалізації заходів банківського менеджменту та на рівні банківської системи на підставі реалізації державних заходів, спрямованих на захищеність інтересів банку (банківської системи в цілому) від внутрішніх та зовнішніх загроз. При цьому, безпека банку має комплексний і багатофункціональний характер, а її реалізація дозволяє

реалізувати пріоритетні цілі банку, створити і використати можливості конкурентного середовища для забезпечення його ефективного функціонування та сталого розвитку у довгостроковій перспективі. Як критерій ефективності безпеки банківської діяльності переважна більшість організацій розглядає стабільність фінансового й економічного розвитку банку [5].

Систематизація розглянутих підходів дозволила запропонувати таке визначення поняття «фінансова безпека банку»: це такий стан банку (банківської системи в цілому), що характеризується здатністю протистояти можливим зовнішнім та внутрішнім загрозам банківської діяльності для забезпечення нормального функціонування та розвитку в умовах дестабілізуючого впливу оточуючого середовища та захищеності фінансових інтересів зацікавлених сторін (власників, клієнтів, працівників, керівництва, держави), а основною метою безпеки банку є забезпечення конкурентоспроможності як окремого банку, так і банківської системи в цілому на ринку банківських послуг та недопущення можливості отримання збитків або втрати частини прибутків внаслідок реалізації внутрішніх та зовнішніх загроз.

На думку Т. Болгар [6] та С. Побережного, «ключовими характеристиками фінансової безпеки банку є: забезпечення рівноважного і стійкого фінансового стану банку; сприяння ефективній діяльності банку; дозволяти на ранніх стадіях визначити проблемні місця в діяльності банку; нейтралізувати кризи і запобігати банкрутствам» [30].

Як основні складові фінансової безпеки банку можна визначити: систему управління ризиками, фінансову стійкість, рівень капіталізації та достатність власного капіталу для покриття банківських ризиків, якість кредитного та інвестиційного портфелів і, як наслідок, банківських акти – вів в цілому, рівень рентабельності банківської діяльності, фінансовий потенціал, рівень корпоративного контролю, конкурентоспроможність банку та банківських послуг на ринку, частку іноземного капіталу у статутному капіталі та ін. За цих обставин, державне регулювання фінансової безпеки банку передбачає узгодження та координацію її складових елементів для забезпечення їх

найефективнішого функціонування та недопущення виникнення конфліктів, що можуть становити загрозу фінансовим інтересам держави. Як зазначає С. Побережний, «забезпечення фінансової безпеки банків передбачає виконання низки завдань: ідентифікацію ризиків і пов'язаних з ними потенційних небезпек; визначення індикаторів фінансової безпеки банку; впровадження системи діагностики та моніторингу стану фінансової безпеки; розробку заходів, спрямованих на забезпечення фінансової безпеки банку, як в короткостроковому, так і в довгостроковому періодах; контроль за виконанням запланованих заходів; аналіз виконання заходів, їх оцінка корегування; ідентифікацію загроз банку і корегування індикаторів залежно від зміни стану зовнішнього середовища, цілей і завдань банку» [11].

На думку М. Зубка, «основними завданнями фінансової безпеки банку є: моніторинг і облік факторів, що визначають загрози фінансовій діяльності банку; формування оптимальної структури боргових зобов'язань (банку та його клієнтів); протидія злочинним зазіханням на фінансові ресурси банку; визначення причин та усунення наслідків реалізованих загроз; забезпечення балансу доходів та витрат у діяльності банку; забезпечення ліквідності та платоспроможності банку» [22]. На нашу думку, до зазначених завдань можна додати ще й забезпечення фінансової стійкості і фінансової незалежності банку; збереження фінансових можливостей банку у безпечному стані в умовах дії різноманітних небезпек і загроз.

1.2. Ризики та загрози інформаційній безпеці банку

Процес забезпечення фінансової безпеки банку вимагає здійснення інформаційно – аналітичної роботи, результати якої є необхідною умовою для впровадження моніторингу, оцінки рівня та аналізу факторів, що впливають на рівень його фінансової безпеки. Функціонування системи інформаційно – аналітичного забезпечення є обов'язковим для правильної та оперативної оцінки рівня фінансової безпеки банку, прогнозування можливих внутрішніх та

зовнішніх загроз, дотримання достатності фінансових ресурсів для своєчасного виконання зобов'язань [10].

На думку В. Котковського, що «невід'ємною складовою комплексу заходів по забезпеченню фінансової безпеки банківської діяльності є система страхування депозитів, яка забезпечує захист депозиторів від ризику втрати вкладених коштів або мінімізацію цього ризику у разі банкрутства комерційного банку. З метою побудови ефективної системи гарантування коштів клієнтів в комерційних банках України, доцільно розповсюдити такі умови на кошти, розміщені на рахунках фізичних і юридичних осіб без їх диференціації. Крім того, для забезпечення гарантій ліквідності системи потрібна активна державна підтримка» [25].

На сьогодні немає єдиного підходу до визначення загроз фінансовій безпеці банку. Більшість науковців пропонують власні класифікації таких загроз, зокрема Д. Артеменко, О. Барановський, А. Єрмошенко, М. Зубок, В. Коваленко, С. Побережний, З. Сороківська, В. Шурпаков, О. Хитрін та інші. На наш погляд, найбільш вдалим є поділ загроз на зовнішні (з боку клієнтів, партнерів, конкурентів, держави тощо) та внутрішні (з боку власників, адміністрації, менеджерів підрозділів, спеціалістів, неформальних груп та ін.). Аналіз та систематизація економічної літератури дозволили визначити найбільш характерні загрози фінансовій безпеці банку. Так, до внутрішніх загроз було віднесено: недосконалість організації системи фінансового менеджменту в банку; неефективність проведення основних банківських операцій; недотримання банком показників ліквідності; зловживання та некомпетентність службовців банку (шахрайство у сфері бухгалтерського обліку, фальсифікація витрат, привласнення доходів тощо); слабкість маркетингової політики банку; неефективна система фінансового моніторингу в банку; наявність каналів витоку інформації з банку; низький рівень капіталізації банків; низький рівень залучення іноземної валюти і готівки у національній валюті, що знаходиться у населення, тощо.

До зовнішніх загроз – несприятливі макроекономічні умови, ринкові ризики та глобальні банківські кризи; відсутність стабільності податкової, кредитної та страхової політики; низький рівень довіри до банків; конкуренція у банківському середовищі; недостатня фінансова стійкість банківського сектору; недосконаліть банківського нагляду та регулювання, в тому числі механізму використання монетарних інструментів; висока ступінь залежності банків від зовнішніх джерел фінансування; значні коливання курсу національної валюти відносно інших валют (інфляція, дефляція); відкритість (доступність) міжбанківського ринку; волатильність цін на енергоресурси; політична та геополітична нестабільність; негативні зміни процентних ставок (наприклад, LIBOR, облікової ставки тощо); високий рівень проблемності активів; можливість знецінення майна, що перебуває як забезпечення за кредитними операціями банків (зокрема, через падіння цін на ринку нерухомості, кризу окремих галузей економіки тощо); участь банківської системи у тіньовій діяльності та її криміналізація; недостатнє законодавче врегулювання банківської діяльності; недостатній контроль за діяльністю комерційних банків з боку Національного банку України тощо.

В наші часи загрози інформаційної безпеки можуть з'являтись дуже часто, адже кожного дня зловмисники знаходять нові вразливості, завдяки яким можуть нанести шкоду для компаній чи державних установ. В останній час набирають популярності DDoS -атаки.

Згідно зі статтею Стадника Р.Е. «Одним із найбільш руйнівних хакерських інструментів в останні роки стали так звані розподілені атаки "відмова в обслуговуванні" - DDoS(Distributed Denial of Service). Основна небезпека DDoS -атак – це їх прозорість та «нормальність» Якщо помилку у програмному забезпеченні завжди можна виправити, то повне «згоряння» ресурсів - це дійсно нормальне та буденне явище, з яким неодноразово зіштовхуються адміни. Останнім часом їх, частіше, називають просто DoS-атаками, або розподіленими атаками. Їх завдання - паралізувати роботу web-вузла який атакується.

Виділяють два основних типи атак, які викликають відмову в обслуговуванні. В результаті проведення атаки першого типу, зупиняється робота всієї системи або мережі. Хакер відправляє системі дані або пакети, на які вона не сподівається, і це призводить до зупинки системи або до її перезавантаження. Другий тип DDoS-атаки призводить до переповнення системи або локальної мережі за допомогою величезної кількості інформації, яку неможливо обробити.

Зазвичай DDoS-атаки використовують в трьох цілях:

1 – зведення особистих рахунків (особиста чи ідеологічна образа тощо);

2- "по замовленню" (а такі послуги коштують дуже дорого);

3 – заради розваги.

Згідно з даними сайту websecurity з 2001 по 2013 рік хакери атакували 568 українських державних сайтів і це без врахування інфікованих ресурсів із доменним ім'ям gov.ua. Якщо у 2001 році в Уанеті було лише два пошкоджених ресурси, то у 2013-му їхня кількість збільшилась до 149. В першу чергу це були DDoS атаки.

Щоб забезпечити захист ресурсу від DDoS – атак, мало знати від чого потрібно захищати ресурс. Вкрай важко знать, як це робити, тим паче, від кожного виду атак є свій захист. Малого того, для того, щоб попередити атаку і для того, щоб їй протистояти використовуються різні види захисту. Всі заходи захисту від DDoS – атак можна поділити на пасивні (які запускаються один раз та працюють самі по собі) та активні (для нормального функціонування котрих необхідно присутність або контроль збоку людини),а також превентивні (ті, які використовуються для того , щоб попередити виникнення DDoS - атаки) і реакційні (ті, які використовуються при виникненні загрози або усунення наслідків DDoS - атаки).

На закінчення можна зазначити, що шахраї, які створюють ботнет, все рідше діють поодинці, а входять у великі злочинні співтовариства. При цьому власники ботнетів стають партнерами і об'єднують ресурси для організації DDoS-атак» [35].

1.3. Нормативно-правове забезпечення інформаційної безпеки банку

Одним з головних принципів, що має бути закладений у систему нормативно – правового забезпечення національної безпеки, є принцип, відповідно до якого унеможливлювалася будь – яка узурпація усіх функцій одним з уповноважених державних органів із забезпечення національної безпеки, домінування одного органа над іншим. «Лише таке законодавство являє собою умову створення відповідного природі розумної людини громадянського суспільства – вільного демократичного правового суспільства, орієнтованого на конкретну людину, яке створює атмосферу поваги до правових традицій і законів, загальногуманістичним ідеалам, яке забезпечує свободу творчої і підприємницької діяльності, створює можливість досягнення добробуту і реалізації прав людини і громадянина, яке органічно відпрацьовує механізми обмеження і контролю за діяльністю держави» [6].

Передусім, слід визначити саме поняття "нормативно – правове забезпечення національної безпеки" та аргументувати доцільність його вживання.

Поняття "нормативно – правове забезпечення національної безпеки" включає його нормативне регулювання і виконання права як засобу управління стосовно сфери національної безпеки. Воно розуміє під цим також сприяння пошуку шляхів удосконалення існуючих та створюваних нових правових норм, необхідних для виконання принципово нових завдань в сфері національної безпеки.

Нормативно – правове забезпечення національної безпеки – процес створення і підтримки в необхідних межах конструктивних організацій но – функціональних характеристик системи національної безпеки за допомогою впорядковуючого впливу нормативно – правових засобів.

У більшості випадків автори подеколи ототожнюють правове забезпечення із законодавчим, або нормативно – правовим; подеколи йдеться про нормативно – правове регулювання, а не забезпечення. З приводу цього зазначимо: право не

зводиться до норм. Окрім норм, воно включає в себе природне право і суб'єктивні права. Призначення норм за даного випадку полягає у тому, щоб соціально – правові претензії в сфері національної безпеки трансформувати у суб'єктивні права – юридичну форму можливих духовних і матеріальних благ. Таким чином, право охоплює сферу не лише належного (нормативні та індивідуальні приписи і рішення), а й сущого (реальне використання юридичних можливостей, реальне використання обов'язків). Найбільш чіткою для розмежування і напевно вірного розуміння даних понять (заков і право) є формула: "Право створюється суспільством, а закон – державою" [17].

Саме тому, ураховуючи зазначене, якщо вживати термін "правове забезпечення національної безпеки", то слід говорити не лише про нормативну сторону даного процесу, а й розглядати питання впливу, взаємозв'язку та трансформації природного та суб'єктивного права. Ще одна ремарка стосується тієї обставини, що вживання терміну "законодавче забезпечення національної безпеки" є також не зовсім точним, через те, що суспільні відносини в сфері національної безпеки є настільки різноманітними і багатоплановими, що застосування лише законів як регуляторів даного роду відносин, суттєво звужує можливість держави щодо виконання своїх функцій. Саме тому нами акцентується увага і на Концепції національної безпеки, Доктринах, законах, кодексах, положеннях, стратегіях, програмах і планах. Таким чином, арсенал юридичних засобів не звужуються нами лише до законів. Відтак застосування терміну "нормативно – правове забезпечення національної безпеки" найбільш повно і точно відображає сутність та зміст розглядуваного нами питання – врегулювання суспільних відносин у сфері національної безпеки за допомогою юридичного інструментарію.

Основу нормативно – правового забезпечення національної безпеки складають формування та підтримка його нормативно – правової бази як юридичного засобу досягнення реальної упорядкованості системи національної безпеки.

Нормативна база являє собою організаційно – функціональний образ системи національної безпеки, виражений юридичною мовою і який відповідає її цільовому призначенню. При цьому правові норми забезпечують моделювання як самої системи національної безпеки, так і ЇЇ підсистем, нормування та формалізацію їх функціональних, організаційних та інформаційних структур, а також самі виконують інформаційну функцію.

Вихідною, управляючою, правовою інформацією для функціонування системи національної безпеки є Конституція України, а також закони та шдзаконні нормативні акти, що визначають функції та завдання державних і недержавних суб'єктів сил забезпечення національної безпеки як в цілому, так і по конкретних напрямах їх діяльності, підсистемах і рівнях управління.

Сили забезпечення національної безпеки не лише застосовують норми права, а й, відповідно до своєї компетенції, видають відомчі нормативні акти на основі та на виконання діючих законів, указів та розпоряджень президента, постанов та розпоряджень Кабінету Міністрів України.

Нормотворча діяльність суб'єктів сил забезпечення національної безпеки е конкретною формою управління відповідною системою. Вона полягає не тільки в заповненні прогалин правового забезпечення, що виникають в результаті недостатньої реалізації правотворчої здатності. Така діяльність базується, передусім, на свідомому прагненні правомочного органу врегулювати певні відносини в сфері національної безпеки, які цього потребують.

Система нормативно – правового забезпечення національної безпеки являє собою сукупність законів і під законних нормативних актів, які створюють нормативно – правове поле для функціонування системи національної безпеки і виконання нею свого призначення.

У широкому розумінні йдеться про Конституцію України, Закон України "Про основи національної безпеки України", закони України, укази та розпорядження Президента України, міжнародні правові акти, пов'язані із забезпеченням як національної, так і регіональної та міжнародної безпеки, постанови та розпорядження Кабінету Міністрів України, які визначають

компетенцію суб'єктів системи забезпечення національної безпеки, а також відомчі нормативні акти у формі наказів, директив, настановлень, положень, статутів, правил, інструкцій [20].

Усю нормативну базу, якою керується система забезпечення національної безпеки можна поділити на два рівні. На першому рівні, правова база створюється в рамках системи національної безпеки і має загальнообов'язковий для всіх характер (Конституція України, закони та постанови Верховної Ради України, укази та розпорядження Президента України, постанови та розпорядження Кабінету Міністрів України). На другому рівні, створюється відомча нормативна база, яка уточнює і конкретизує з урахуванням специфіки кожного суб'єкта сил забезпечення національної безпеки його функції та завдання.

Нормотворчість являє собою правову форму діяльності суб'єктів СЗНБ, яка здійснюється відповідно до їх компетенції, на основі і на виконання законів та підзаконних нормативних правових актів. їх основне призначення полягає у створенні правових норм, які встановлюють, змінюють або відміняють правові відносини, визначаються зміст діяльності по забезпеченню національної безпеки і надають їм загальнообов'язкової сили. Отже нормотворчість в системі забезпечення національної безпеки слід розглядати як процес створення відомчих нормативних актів при відповідному забезпеченні технологій їх підготовки та прийняття.

Нормотворча діяльність має своїми цілями забезпечити:

• юридичне закріплення існуючих у галузі відносин та їх право ве регулювання;

• формування нових відносин, відсутніх у поточний момент, але бажаних чи необхідних з погляду виконання перспективних завдань;

• ліквідацію відносин та ситуацій, віджилих та гальмуючих розвиток нових ігрогресивних тенденцій.

Питання функціонування як самої системи національної безпеки, а більш коректно і доцільно казати за даного випадку як про систему забезпечення

національної безпеки, так і окремих її суб'єктів знаходить своє правове закріплення головним чином в законах і положеннях, що встановлюють правовий статус суб'єктів сил забезпечення національної безпеки. Водночас, і на цьому ми вже акцентували увагу, доки не буде відпрацьована методологічно вивірена та така, що відповідає реаліям сьогодення Концепція національної безпеки, затверджена законом, казати про застосування системного підходу, а також про реальне втілення його у життя поки залишається марним. Таким чином, реалізація правової політики у сфері національної безпеки щодо впровадження системного підходу до формування базису нормативно – правового забезпечення національної безпеки є неможливою і неефективною без оновленої Концепції національної безпеки. І в даному аспекті прийнятий Закон України "Про основи національної безпеки України" не володіє достатніми можливостями щодо заповнення цієї прогалини і вирішення окреслених питань.

Нормативно – правове забезпечення становить собою складний і багатошаровий процес, отже постає необхідність у виокремленні певних його завдань, до яких належать:

• забезпечення точного розподілу функцій між суб'єктами системи забезпечення національної безпеки, їхніх прав і обов'язків, налагодження системи взаємодії;

• розподіл функцій щодо збирання, оброблення інформації та надсилання результатів аналізу на відповідні управлінські рівні системи забезпечення національної безпеки;

• раціональна побудова системи прийняття управлінських рішень із закріпленням персональної відповідальності за їх виконання.

Розробниками міжнародних стандартів є Міжнародна Організація із Стандартизації ISO, Міжнародна Електротехнічна Комісія IEC та Британський інститут стандартів BSI, вони формують спеціалізовану систему всесвітньої стандартизації. На сьогодні в питаннях інформаційної безпеки прийняті, зокрема, такі міжнародні стандарти:

1. Серія ISO 27000 «Міжнародні стандарти для системи управління інформаційною безпекою»:
2. − ISO/IEC 27000:2009. Визначення і основні принципи;
3. − ISO/IEC 27001:2005. Інформаційні технології – Методики безпеки – Системи менеджменту інформаційної безпеки – Вимоги (BS 7799-2:2005);
4. − ISO/IEC 27002:2005. Інформаційні технології – Методики безпеки – Практичні правила управління інформаційною безпекою (попередній код ISO/IEC 17799:2005;
5. − ISO/IEC 27003:2010. Настанова з впровадження системи управління інформаційною безпекою;
6. − ISO/IEC 27005:2008. Інформаційні технології – Методики безпеки – Управління ризиками інформаційної безпеки (на основі стандарту BS 7799-3:2006); Financial space № 3 (3) 2011 63 БАНКІВСЬКИЙ МЕНЕДЖМЕНТ − ISO/IEC 27006:2007. Інформаційні технології – Методики безпеки – Вимоги до організацій, що провадять аудит і сертифікацію систем менеджменту інформаційної безпеки;
7. − ISO/IEC 27011:2008. Керівництво з менеджменту інформаційної безпеки для телекомунікацій;
8. − ISO/IEC 15408. Загальні критерії оцінки безпеки інформаційних технологій.
9. 2. Серія ISO 13335 «Міжнародні стандарти безпеки інформаційних технологій»: − ISO13335-1:2004. Інформаційні технології – Керівництво по управлінню IT безпекою – Концепції і моделі для управління безпекою інформаційних і телекомунікаційних технологій;
10. − ISO13335-3:1998. Інформаційні технології – Керівництво по управлінню IT безпекою – Методи управління IT безпекою;
11. − ISO13335-4:2000. Інформаційні технології – Керівництво по управлінню IT безпекою – Вибір механізмів захисту;

− ISO13335-5:2001. Інформаційні технології – Керівництво по управлінню IT безпекою – Керівництво по управлінню мережевою безпекою. НБУ

послідовно впроваджує міжнародну політику в сфері забезпечення інформаційної безпеки банків.

Постанова Правління НБУ № 474 зобов'язує всі українські банки привести у відповідність свої системи менеджменту інформаційної безпеки до вимог стандарту ISO/IEC 27001.

Згідно з цією постановою з дня її опублікування набирають чинності два галузеві стандарти: Стандарт організації України. Настанова «Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги» (ISO/IES 27001:2005, MOD) та Стандарт організації України.

Настанова «Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою». Перший стандарт є прийнятий зі змінами стандарт ISO/ IEC 27001:2005. Другий стандарт є прийнятий зі змінами міжнародний стандарт ISO/IEC 27002:2005 Важливим документом є також «Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України від 01.03.2011». У цьому документі сказано, що система управління інформаційною безпекою є сучасним процесом забезпечення безпеки інформаційних ресурсів організації, яка побудована на кращих світових практиках. Стандарти Національного банку України основані на міжнародних стандартах ISO 27001 та ISO 27002 з додаванням вимог із захисту інформації, зумовлених конкретними потребами сфери банківської діяльності і правовими вимогами, які вже висунуто в нормативних документах Національного банку України. Відповідність системи управління інформаційною безпекою стандартам Національного банку України СОУ Н НБУ 65.1 СУІБ 1.0:2010 та СОУ Н НБУ 65.1 СУІБ 2.0:2010 гарантує банку відповідність міжнародним стандартам ISO 27001 та ISO 27002.

Необхідність впровадження в банках України стандартів з управління інформаційною безпекою продиктована вимогами Базельського комітету Basel II з управління та зменшення операційних ризиків банків. Ці Методичні рекомендації розроблені на основі міжнародного стандарту ISO/IEC 27003:2010

з урахуванням особливостей банківської діяльності, стандартів та вимог Національного банку України з питань інформаційної безпеки.

З 31 березня 2019 фінансові організації, що використовують засоби захисту інформації, подають щорічну звітність НБУ, це зазначено в постанові Правління Національного Банку України, «Положення про порядок перевірки стану інформаційної безпеки в банківських та інших установах, які використовують засоби захисту інформації Національного банку України

I. Загальні положення

1. Це Положення розроблено відповідно до статей 7, 15, 56 Закону України "Про Національний банк України", статті 66 Закону України "Про банки і банківську діяльність", Законів України "Про платіжні системи та переказ коштів в Україні", "Про захист інформації в інформаційно-телекомунікаційних системах" і нормативно-правових актів Національного банку України у сфері інформаційної безпеки.

2. Терміни та скорочення в цьому Положенні вживаються в значеннях, визначених Законом України "Про електронні довірчі послуги", Положенням про захист електронних банківських документів з використанням засобів захисту інформації Національного банку України, затвердженим постановою Правління Національного банку України від 26 листопада 2015 року N 829 (зі змінами) (далі - Положення про захист), Правилами організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України, затвердженими постановою Правління Національного банку України від 26 листопада 2015 року N 829 (у редакції постанови Правління Національного банку України від 05 жовтня 2018 року N 106) (далі - Правила N 829), Інструкцією про міжбанківський переказ коштів в Україні в національній валюті, затвердженою постановою Правління Національного банку України від 16 серпня 2006 року N 320, зареєстрованою в Міністерстві юстиції України 06 вересня 2006 року за N 1035/12909 (зі змінами).

3. Це Положення регламентує порядок здійснення контролю за виконанням організаціями вимог щодо використання ЗЗІ, установлених Правилами N 829.

4. Національний банк України (далі - Національний банк) здійснює контроль за використанням організаціями ЗЗІ (далі - контроль) шляхом:

1) аналізу інформації, документів, звітів, отриманих від організацій;

2) здійснення виїзних перевірок.

5. Національний банк має право вимагати від організації надання інформації для здійснення контролю шляхом направлення запиту.

Керівник організації зобов'язаний забезпечити надання на запит Національного банку достовірної інформації у вигляді письмових пояснень, документів в електронній (уключаючи електронний журнал ПМГК) та/або паперовій формі у строк, в обсязі, за форматом та за структурою, що визначені в такому запиті.

6. Керівник організації зобов'язаний забезпечити подання звіту щодо використання ЗЗІ (далі - Звіт) згідно з додатком до цього Положення.

Звіт подається організаціями до Національного банку один раз на рік протягом одного місяця, наступного за звітним періодом (рік), у паперовій або електронній формі. У разі подання Звіту в паперовій формі такий Звіт засвідчується власноручним підписом керівника організації. Подання Звіту в електронній формі здійснюється у форматі pdf із кваліфікованим електронним підписом керівника організації і такий Звіт надсилається засобами електронної пошти Національного банку.

7. Національний банк забезпечує нерозголошення інформації, отриманої ним під час здійснення контролю, третім особам, за винятком випадків, передбачених законодавством України» [32].

Висновки до першого розділу

Можна зробити висновок, що інформаційна безпека – стан інформаційної системи, у якому вона може протистояти впливу внутрішніх і зовнішніх ризиків. Сьогодні існує гостра необхідність побудови повноцінної системи інформаційної безпеки. Зокрема, гострим постає питання інформаційної безпеки банківських систем не лише для України, а й для світу в цілому. Для банків ця проблема є дуже важливою, оскільки щомісяця в світі звідти відбувається витік інформації, результатом чого є не лише втрата довіри клієнтів (отже і зниження конкурентоспроможності), а й значні збитки в десятки і навіть сотні мільйонів доларів. Існує багато сучасних методів захисту інформації у банках, використання яких помітно зменшило кількість основних каналів витоку інформації протягом останніх двох років.

В Україні з метою вирішення даного питання НБУ прийняв Постанову Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України, проте це лише крок до подолання проблеми, що склалася. Але для отримання помітних результатів не достатньо прийняття нормативних постанов, необхідна взаємодія нормативно – правового, організаційно – економічного та морально – етичного елементів інформаційної системи. Лише поєднання ефективної дії цих сегментів дозволить забезпечити довгостроковий прогнозований розвиток інформаційної безпеки не лише банківських установ, а й держави в цілому.

РОЗДІЛ 2. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ

2.1 . Методи забезпечення інформаційної безпеки банку

На думку А.Бегун та С.Побережного, що «ключовими характеристиками фінансової безпеки банку є: забезпечення рівноважного і стійкого фінансового стану банку; сприяння ефективній діяльності банку; дозволяти на ранніх стадіях визначити проблемні місця в діяльності банку; нейтралізувати кризи і запобігати банкрутствам» [30].

Згідно Енциклопедії банківської справи України, що «під *методом* прийнято розуміти спосіб здійснення певної діяльності у вигляді послідовних дій, виконуваних на основі чітко контрольованого плану. Методи забезпечення безпеки банку варіюються залежно від специфіки підлягають вирішенню завдань і від компетенції беруть участь суб'єктів. У свою чергу, вибір *засобів* забезпечення безпеки банку, тобто прийомів або спеціальних знарядь, зумовлений методами, в рамках яких їх планується використовувати» [15].

Діяльність з забезпечення інформаційної безпеки здійснюється за допомогою різних способів, засобів і прийомів, які у своїй органічній сукупності складають методи. Метод передбачає певну послідовність дій на підставі конкретного плану. Методи можуть значно змінюватися і варіюватися в залежності від тину діяльності, в якій вони використовуються, а також сфери застосування.

Важливими методами аналізу стану забезпечення інформаційної безпеки є методи опису та класифікації. Для здійснення ефективного захисту системи державного управління слід, по – перше, описати, а лише потім класифікувати різні види загроз та небезпек, ризиків та викликів і відповідно сформулювати систему заходів по здійсненню управління ними.

У якості розповсюджених методів аналізу стану забезпечення інформаційної безпеки використовуються методи дослідження причинних

зв'язків. За допомогою цих методів виявляються причинні зв'язки між загрозами, ризиками, викликами та небезпеками; здійснюється пошук причин, які стали джерелом і спричинили актуалізацію тих чи інших чинників небезпеки, а також розробляються заходи по їх нейтралізації. У числі даних методів причинних зв'язків можна назвати наступні: метод схожості, метод відмінності, метод сполучення схожості і відмінності, метод змін, що супроводжують, метод залишків.

Вибір методів аналізу стану забезпечення інформаційної безпеки залежить від конкретного рівня і сфери організації захисту. В залежності від загрози уможливлюється завдання щодо диференціації як різних рівнів загроз, так і різних рівнів захисту. Що стосується сфери інформаційної безпеки, то у ній, зазвичай, виділяють: фізичний, програмно – технічний, управлінський, технологічний, рівень користувача, мережний, процедурний. Розглянемо дещо детальніше кожний з цих рівнів.

На фізичному рівні здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються, і управлінських технологій. На програмно – технічному рівні здійснюється ідентифікації і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності.

На рівні управління здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях управління з боку єдиної системи забезпечення інформаційної безпеки органів державного управління. На технологічному рівні здійснюється реалізації політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій. На рівні користувача реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на суб'єктів державного управління, унеможливлення інформаційного впливу з боку соціального середовища. На рівні мережі дана політика реалізується у форматі координації дій органів державного управління, які

пов'язані між собою однією метою. На процедурному рівні вживаються заходи, що реалізуються людьми. Серед них можна виділити наступні групи процедурних заходів: управління персоналом, фізичний захист, підтримання роботоздатності, реагування на порушення режиму безпеки, планування реанімаційних робіт.

Згідно з роботою Бондаренко М.Ф., «можна виокремити декілька типів методів забезпечення інформаційної безпеки:

– однорівневі методи будуються на підставі одного принципу управління інформаційною безпекою;

– багаторівневі методи будуються на основі декількох принципів управління інформаційною безпекою, кожний з яких слугує вирішення власного завдання. При цьому приватні технології не пов'язані між собою і спрямовані лише на конкретні чинники інформаційних загроз;

– комплексні методи – багаторівневі технології, які об'єднані до єдиної системи координуючими функціями на організаційному рівні з метою забезпечення інформаційної безпеки виходячи з аналізу сукупності чинників небезпеки, які мають семантичний зв'язок або генеруються з єдиного інформаційного центру інформаційного впливу;

– інтегровані високоінтелектуальні методи – багаторівневі, багатокомпонентні технології, які побудовані на підставі могутніх автоматизованих інтелектуальних засобів із організаційним управлінням» [7].

Загальні методи забезпечення інформаційної безпеки активно використовуються на будь – якій стадії управління загрозами. До таких стадій належать: прийняття рішення з визначення області та контексту інформаційної загрози і складу учасників процесу протидії; ухвалення загальної стратегії і схеми дій в політичній, економічній і соціальній сферах життєдіяльності; забезпечення адекватного сприйняття загрози та небезпеки у більш низьких організаційних ланках системи державного управління; виділення необхідних політичних, економічних, соціальних, адміністративних і організаційних ресурсів, достатніх для реалізації програми відбиття інформаційної загрози і

збереження сталого розвитку інформаційних ресурсів системи державного управління: трансформації результатів оцінки ризиків у відповідну політику безпеки, включаючи національну.

Специфіка методів, що використовуються, значно залежить від суб'єкта діяльності, об'єкта впливу, а також цілей, що переслідуються. Так, методи діяльності індивіда у зв'язку із його обмеженою можливістю з забезпечення інформаційної безпеки здебільшого зводяться до джерела загрози, апелювання до суспільної думки, а також до держави, яка має вживати рішучих заходів із нейтралізації інформаційних загроз. Саме суспільство почасти використовує у своїй діяльності методи соціального регулювання, надання допомоги окремим індивідам і суспільним організаціям, яким спричинена шкода внаслідок виявлення загрози.

Причому, на жаль, слід констатувати, що в нашій країні не на достатньому рівні усвідомлюють небезпеку саме в інформаційній сфері, немає штатних одиниць в органах державного управління по забезпеченню інформаційної безпеки, не проводиться підготовка відповідних фахівців для органів державного управління.

Вельми важливим є застосування аналітичних методів пізнання і дослідження стану суспільної свідомості у сфері інформаційної безпеки. Наприклад, усвідомлення важливості забезпечення інформаційної безпеки на рівні індивіда, суспільства і організації заважає розповсюджений міф про те, що захист інформації і криптографія одне й те ж саме. Водночас таке розуміння є наслідком використання застарілих підходів до інформаційної безпеки, коли інформаційна безпеки лише ототожнюються із захистом інформації шляхом її шифрування.

Нині важливою умовою забезпечення інформаційної безпеки є не стільки секретність, конфіденційність інформації, скільки її доступність, цілісність, захист від загроз. Отже, система має відповідно реагувати та гарантувати ефективну діяльність у цьому напрямі.

Іншим завданням захисту є забезпечення незмінності інформації під час її зберігання або передачі, тобто забезпечення її цілісності. Таким чином конфіденційність інформації, яка забезпечується за допомогою криптографічних методів не є головною вимогою при проектуванні систем захисту інформації органів державного управління. Виконання процедур криптокодування і декодування може уповільнити передачу даних та зменшити доступ до них, через те, що працівник органу державного управління буде позбавлений можливості своєчасного та швидкого доступу до цих даних та інформації, через функціонування механізму захисту. Саме тому, забезпечення конфіденційності інформації має відповідати можливості доступу до неї. Таким чином, управління в сфері інформаційної безпеки має здійснюватися на підставі принципу доступності та безпеки. Система забезпечення інформаційної безпеки в першу чергу має гарантувати доступність і цілісність інформації, а її конфіденційність у випадку необхідності.

Також зазначимо, що вплив хакерів та їх можливість суттєво вплинути на інформаційні системи дещо перебільшена. Здебільшого були зламані ті системи, які мали поганий захист. Так, наприклад, багато компаній в Україні, які мають солідний грошовий обіг і достатні фінансові джерела, не мають не те щоб цілісної системи безпеки взагалі, а й навіть окремо функціонуючої підсистеми забезпечення інформаційної безпеки. Здебільшого забезпечення інформаційної безпеки зводиться до того, що в системних блоках блокується доступ до флоппі – дисків і тим самим унеможливлюється несанкціонований запис інформації. Окрім цього, системний адміністратор встановлює спеціальні програми – фільтри, що відсіюють можливість доступу до внутрішньої мережі ззовні. Можна перераховувати й інші методи захисту інформації, водночас, нині ототожнення забезпечення інформаційної безпеки із забезпеченням безпеки комп'ютерних систем є просто концептуальною помилкою. Тому не є дивиною, що на сьогодні більша частина українських банків втратила внаслідок власної недбалості чимало коштів. І характерною рисою українського

суспільства є те, що жоден з банків жодного разу не визнав факту вчиненого кіберзлочину проти себе.

У даному аспекті можна зауважити на ще одну проблему: зневага до вимог інформаційної безпеки та брак необхідних знань. Здебільшого під час робочого дня працівники, виконуючи свої службові обов'язки, відкривають паралельні вікна в Інтернеті, та самі, не усвідомлюючи того, відкривають доступ не лише до інформації" що зараз обробляється, а в цілому до комп'ютерної мережі усієї системи органів державного управління, починаючи від Кабінету Міністрів України, закінчуючи місцевими органами виконавчої влади. Отже, одним із найкращих засобів захисту інформації від нападу – не допускати його.

Втім не слід плекати надію на створення абсолютної системи інформаційної безпеки, оскільки, як зазначалося нами вище, ми стоїмо на тій позиції, що загроза та небезпека є атрибутивними компонентами системи інформаційної безпеки, отже їх існування та реалізація, а також негативні наслідки є природним компонентом системи інформаційної безпеки. Саме вони дають змогу побачити недоліки в системі управління інформаційною безпекою, і водночас слугують імпульсом до вдосконалення, тобто до розвитку. Отже, важливим метод забезпечення інформаційної безпеки є метод розвитку.

Захист інформації не обмежується технічними методами, на що зазначає велике коло дослідників. Для ефективного забезпечення інформаційної безпеки важливим є різноманітні моделі та методи оцінки загроз та небезпек. їх варіативність занадто лабільна та залежить як від рівня розвитку тієї чи іншої цивілізації, так і від контексту оцінки, що проводиться, наявності всебічних даних по факторам загроз, алгоритму вирахування коефіцієнту імовірності настання та розміру негативних наслідків. Наявність конкретних даних з цього питання дозволяє досить точно визначити ступінь впливу інформаційної зброї, рівень загроз та небезпек.

Як зазначив Єрмошенко А.М. «Основним методом аналізу інформаційних ризиків є кількісний ті якісний аналіз, факторний аналіз та інші. Мета якісної оцінки ризиків – ранжувати інформаційні загрози та небезпеки за різними

критеріями, система яких дозволить сформувати ефективну систему впливу на них.

Важливим методом забезпечення інформаційної безпеки є також метод критичних сценаріїв. У зазначених сценаріях аналізуються ситуації, коли уявний супротивник паралізує систему державного управління і відповідно знижує здатність підтримувати державне управління в межах оптимальних параметрів. При чому аналіз подій в світі дає усі підстави стверджувати, що інформаційні війни стають органічною частиною політики національної безпеки багатьох розвинених країн» [18].

Також можна зазначити на метод моделювання, за допомогою якого можна проводити навчання з інформаційної безпеки. Позитивний досвід цього є у США, де на базі однієї з відомих корпорацій постійно провадяться оперативно – дослідницькі навчання, щоб моделювати різні форми інформаційних атак у ході інформаційної війни. Серед методів забезпечення інформаційної безпеки важливе значення має метод дихотомії. Для протидії загрозам інформаційній безпеці вживаються необхідні заходи як в напрямку надання певного впливу на джерело загрози, так і в напрямку укріплення об'єкта безпеки. Відповідно виділяють дві предметні області протидії. Одна з них утворюється сукупністю джерел загроз, а інша – сукупністю заходів із забезпечення інформаційної безпеки органу державного управління.

Вплив на джерело загрози інформаційної безпеки спрямований на зміну чинників та умов, здатних нанести шкоду об'єкту безпеки. Метою захисту є переконання супротивника у недоцільності здійснення загроз. Що стосується органів державного управління, то джерело загроз може бути спрямовано на зміну міждержавних відносин, укріплення довіри між державами, створення умов, за яких здійснення небезпечних дій щодо об'єкта безпеки стає невигідним унаслідок виникнення небажаних наслідків або неможливим. Основним предметом за даного випадку є інформація, яка є у супротивника у вигляді відомостей, знань, оцінок. У свою чергу, інформація, що надходить від супротивника і становить собою загрозу, може бути піддана впливу для зміни її

здатності завдавати шкоду, нейтралізації, трансформації або ліквідації її небезпечних властивостей. Вплив на інформаційну інфраструктуру важливий у тому випадку, коли загрозу може представляти середовище розповсюдження небезпечної інформації.

Методи впливу на інформацію у формі повідомлень можна поділити також на електронні та неелектронні. Електронні методи впливу застосовуються у тих випадках, коли повідомлення закріплюються на електромагнітних носіях, котрі призначені для оброблення за допомогою засобів обчислювальної техніки. Вони полягають у знищенні, викривленні, копіюванні повідомлень, які зберігаються на цих пристроях. Такі дії можуть бути вчинені лише за допомогою технічного та програмного забезпечення. Неелектронні методи за своєю суттю мають той самий зміст, але реалізуються без використання засобів обчислювальної техніки для впливу на повідомлення, закріплення на інших, передусім паперових, носіях інформації.

Методи впливу на інформаційну інфраструктуру можуть бути розділені на інформаційні та неінформаційні. Інформаційні методи впливу орієнтовані на порушення формування інформаційно – телекомунікаційних систем, мереж зв'язку, засобів автоматизації управління, систем автоматизованої обробки інформації, і таким чином, на попередження нанесення шкоди предметам суспільних відносин, що захищаються.

У цілому ж слід зазначити, що обрання цілей і методів протидії конкретним загрозам та небезпекам інформаційній безпеці становить собою важливу проблему і складову частину діяльності з реалізації основних напрямів державної політики інформаційної безпеки. У межах вирішення даної проблеми визначаються можливі форми відповідної діяльності органів державної влади, що потребує проведення детального аналізу економічного, соціального, політичного та інших станів суспільства, держави і особи, можливих наслідків вибору тих чи інших варіантів здійснення цієї діяльності.

На думку М. Зубка, що «основними завданнями фінансової безпеки банку є: моніторинг і облік факторів, що визначають загрози фінансовій діяльності

банку; формування оптимальної структури боргових зобов’язань (банку та його клієнтів); протидія злочинним зазіханням на фінансові ресурси банку; визначення причин та усунення наслідків реалізованих загроз; забезпечення балансу доходів та витрат у діяльності банку; забезпечення ліквідності та платоспроможності банку» [22]. На нашу думку, до зазначених завдань можна додати ще й забезпечення фінансової стійкості і фінансової незалежності банку; збереження фінансових можливостей банку у безпечному стані в умовах дії різноманітних небезпек і загроз.

Відповідно до логіки забезпечення банківської безпеки всі застосовувані в зазначених цілях методи можуть бути зведені в дві основні групи. У першу з них входять методи законодавчого та нормативного правового регулювання, другу групу складають методи реалізації законодавчих та інших нормативних правових приписів.

Метою цього параграфа є розгляд методів і засобів реалізації правових та інших нормативних приписів, які застосовуються комерційними банками та їх підрозділами. Оскільки методи і засоби, що застосовуються іншими суб'єктами (органами державної влади та НБУ), широко висвітлені в спеціальній літературі, то вони будуть згадуватися лише в тій мірі, в якій діяльність цих суб'єктів у сфері забезпечення банківської безпеки стикається з діяльністю банку і його підрозділів.

Завдання реалізації банком законодавчих та інших нормативних приписів в області забезпечення безпеки виконуються за допомогою застосування системи методів, серед яких прийнято виділяти:

- методи організаційні;
- методи технологічні;
- методи захисту інформації обмеженого доступу;
- методи адміністративного контролю;
- методи фінансового контролю;
- методи криміналістики.

Кожен з названих методів може бути розділений на складові його підвиди за безпосередньої сфері застосування, що використовують його підрозділам і інших підстав.

Організаційні методи забезпечення безпеки включають в себе спеціальні методи здійснення виробничої, управлінської, фінансової, комерційної, кадрової та іншої функціональної діяльності банку, що мають на меті попередити заподіяння шкоди як в результаті навмисних дій, так і внаслідок помилки. В рамках організаційних методів: формуються спеціальні підрозділи захисту інтересів банку; проводиться вдосконалення структури керівних і контролюючих органів; приймаються рішення про обмеження й розмежуванні повноважень посадових осіб щодо обсягу і складу банківських операцій, у розпорядженні грошовими коштами та іншим майном банку; розмежовуються повноваження операціоністів і касирів при здійсненні розрахунково – касових операцій; встановлюється індивідуальна відповідальність конкретних осіб за забезпечення процедур виконання окремих операцій та порядку зберігання цінностей; організовується система звітності банку і система роботи з персоналом.

Суб'єктом застосування зазначених методів є банк в особі керівних органів, наділених правом прийняття відповідних рішень.

Засобами реалізації зазначених методів є організаційні рішення, закріплені у формі розпорядчих документів банку.

В рамках технологічних методів розробляються безпечні технології банківських операцій, нс дозволяють злочинцям використовувати відомі практиці способи вчинення злочинів. У їх число входять технології відкриття рахунків, укладання договорів, касового обслуговування клієнтів банку, роботи пунктів обміну валюти, оформлення, видачі та оплати цінних паперів і т.д.

Профілактичний ефект методів технологічного характеру повинен укладатися, з одного боку, в продуманої послідовності і способи виконання відповідних операцій, а з іншого – у встановленні заборони на їх порушення. Внаслідок цього протиправні дії (і в ряді випадків навіть підготовка до них)

набувають характеру грубого порушення встановленого порядку конкретною особою. Приховати таке порушення практично неможливо, і процес його виявлення при належній організації роботи займає дуже незначний проміжок часу.

Технологічні методи забезпечення безпеки банку ґрунтуються на відповідних рекомендаціях НБУ, розробках власних підрозділів банку, наукових і практичних рекомендаціях фахівців у галузі боротьби зі злочинами у фінансовій сфері (наприклад, в сфері вексельного обігу). Реалізуються зазначені методи керівними органами банку, а також його структурними підрозділами в рамках відповідних напрямків банківської діяльності. *Засобами* їх реалізації є технологічні рішення, закріплені розпорядчими документами.

Методи захисту конфіденційності інформації обмеженого доступу дуже різноманітні і охоплюють широкий спектр дій організаційного, програмно – апаратного і контрольного (перевірочного) характеру. В цілому вони можуть бути зведені в чотири основні групи, кожна з яких має на меті вирішення відносно самостійних завдань, а саме:

1) закриття вільного доступу до інформації, віднесеної до банківської та інших видів охороняється законом таємниці;

2) виявлення, попередження і припинення спроб неправомірного заволодіння відомостями і документами, щодо яких встановлено режим конфіденційності;

3) організація захисту інформації обмеженого доступу, що обробляється засобами обчислювальної техніки;

4) організація захисту інформації обмеженого доступу від витоку технічними каналами.

Кожна з названих груп включає в себе ряд самостійних методів, розгляд яких виходить за рамки цього параграфа.

Засобами забезпечення конфіденційності інформації служать нормативні правові документи розпорядчого, рекомендаційного та заборонного характеру, а також спеціальні комп'ютерні програми та пристрої.

Суб'єктом застосування методів і засобів захисту інформації є спеціальні підрозділи захисту інформації банку.

Методи адміністративного контролю у сфері забезпечення безпеки банку мають на меті перевірку наявності та правильного функціонування системи підбору і розстановки кадрів, утримання ув'язнених з працівниками трудових угод (контрактів), наявності інструкцій, що регламентують посадові обов'язки співробітників.

Адміністративними методами забезпечується проведення операцій тільки уповноваженими на те особами і в суворій відповідності з певними банком повноваженнями і процедурами прийняття рішень з проведення операцій.

Методи фінансового контролю покликані забезпечити проведення операцій у суворій відповідності до прийнятої і закріпленої документами політикою банку стосовно до різних видів фінансових послуг та їх адекватного відображення в обліку і звітності.

Фінансовий контроль повинен з достатнім ступенем надійності забезпечити: фіксацію операцій відповідно до встановлених вимог; реальне відображення стану активів і пасивів банку та складання передбачених форм звітності; ведення фінансових документів з достатньою повнотою, їх відповідність фактичним обставинам; здійснення перевірок з встановленою періодичністю.

Суб'єктом реалізації методів адміністративного та фінансового контролю є служба внутрішнього контролю банку.

Засобами адміністративного та фінансового контролю є: формальна і фактична перевірки; підтвердження; обстеження; опитування; аналітичні тести; логічне й арифметичне перевірки.

На думку Стадника Р.Е, «SSL (Secure Socket Layer) — протокол шифрування даних, якими обмінюються клієнт і сервер, — став найбільш

поширеним методом захисту в Інтернеті. Колись він був розроблений компанією Netscape. Безпечний обмін забезпечується за рахунок шифрування і аутентифікації цифрового сертифіката. Цифровий сертифікат — файл, який унікальним чином ідентифікує сервери. Зазвичай цифровий сертифікат підписується і завіряється спеціалізованими центрами. Їх називають центрами сертифікації або засвідчувальними центрами.

Що таке SSL-сертифікат?

Багато хто напевно чули про SSL-сертифікати, але не всі чітко уявляють, що це таке і для чого вони потрібні. По суті, SSL-сертифікат — цифровий підпис вашого сайту, що підтверджує його автентичність. Використання сертифіката дозволяє захистити як власника сайту, так і його клієнтів. SSL-сертифікат дає можливість власнику застосувати до свого сайту технологію SSL-шифрування.

Таким чином, призначення сертифіката SSL — забезпечити безпечне з'єднання між сервером і браузером користувача, надійно захистити дані від перехоплення і підміни. Сертифікат використовується для шифрування даних та ідентифікації сайту за встановлення захищеного з'єднання HTTPS.

Інформація передається в зашифрованому вигляді, і розшифрувати її можна тільки за допомогою спеціального ключа, який є частиною сертифіката. Тим самим гарантується збереження даних, дотримання закону про персональних даних. Відвідувачі сайту вправі очікувати, що захист їх інформації, якщо вона важлива, буде забезпечена за допомогою SSL-сертифіката. Вони можуть покинути ваш сайт, якщо бачать, що він не захищений. Якщо сайт має SSL-сертифікат, то в рядку стану браузера відображається значок у вигляді замку.

Як працює HTTPS (схема дії SSL):

— Користувач заходить на захищений сайт;

— Виконується перевірка DNS і визначення IP-адреси хоста веб-сайту;

— Запис веб-сайту знайдена, перехід на веб-сервер хоста;

— Запит захищеного SSL-з'єднання з хоста веб-сайту;

— Хост відповідає валідним SSL сертифікатом;

— Встановлюється захищене з'єднання, передані дані зашифровані.

Яку вигоду дає використання SSL-сертифіката банкам? Оскільки при використанні сертифікатів та протоколу SSL прийняті і надіслані при відвідуванні сайтів дані шифруються, застосовується процедура аутентифікації, це дає користувачам впевненість в тому, що запроваджувані ними персональні дані, такі як номери телефонів та банківських карток, не потраплять не в ті руки. Завдяки своїй унікальності SSL-сертифікати також значно ускладнюють використання кібершахраями фішингових схем.

Власник сайту може не турбуватися про те, що дані клієнтів витечуть на бік в результаті перехоплення або атаки типу «людина посередині», і репутація банку і навіть подальше існування його опиниться під загрозою» [36].

2.2. Програми забезпечення інформаційної безпеки банку в Україні

Організація забезпечення безпеки банку здійснюється на основі принципу централізованого управління стратегічними напрямами даної діяльності на рівні керівництва банку.

Для оцінки захищеності банківських інформаційних мереж проводиться обстеження, яке можна умовно розділити на такі етапи:

–збір інформації про мережу (наприклад, визначення типу операційної системи атакуючих хостів);

–визначення загроз інформації й уразливих місць;

–проникнення в мережу;

–оцінка ризику, зв’язаного зі знайденими уразливими місцями і можливістю їхнього використання для одержання несанкціонованого доступу до мережі;

– розробка рекомендацій із формування системи захисту інформації і відповідної політики безпеки;

– за узгодженням із керівництвом банку пропонується таке впровадження, настроювання і гарантійний супровід комплексної системи захисту інформації (мережних і обчислювальних ресурсів). У випадку неможливості такого обстеження як альтернативу можна запропонувати скористатися спеціалізованим програмним забезпеченням, призначеним для пошуку відомих уразливих місць мережних сервісів і некоректних параметрів конфігурації операційної системи. У процесі аналізу захищеності розглядаються конкретні елементи інформаційної системи, що вимагають захисту й уходять у політику безпеки, прийняту в банку, відповідно до важливості (ранжирування) оброблюваної, збереженої і переданої інформації, а також безпосередньо інтегровані з глобальною мережею Internet.

До спеціальних заходів забезпечення інформаційної безпеки належать: організація і ведення комерційної розвідки, формування інформаційних ресурсів банку; інформаційно – аналітичні дослідження клієнтів, партнерів і конкурентів банку; взаємодія з правоохоронними органами з питань забезпечення безпеки діяльності банку; вживання заходів з протидії, виявлення, локалізації дій та актів недобросовісної конкуренції та промислового шпигунства; проведення службових розслідувань у банку; проведення заходів з дезінформації конкурентів; забезпечення впливу на недобросовісних клієнтів, боржників і зловмисників з відшкодування банку понесених з їх вини шкоди. Згідно з стандартом ISO/IEC 27001 практична реалізація заходів інформаційної безпеки повинна відбуватись за допомогою:

– встановлення політики системи управління інформаційної безпекою;

– забезпечення відповідності цілей системи управління заходам інформаційної безпеки;

– встановлення ролей і обов’язків, пов’язаних із інформаційною безпекою;

– доведення до персоналу організації важливості забезпечення та дотримання політики інформаційної безпеки; – надання достатніх ресурсів для забезпечення підтримки інформаційної безпеки;

– побудова системи управління ризиками для забезпечення належного рівня інформаційної безпеки;

– забезпечення проведення внутрішнього аудиту системи управління інформаційною безпекою;

– здійснення перевірок управлінських рішень, що запроваджуються керівництвом, щодо забезпечення належного рівня інформаційної безпеки. Реалізація та підтримка заходів інформаційної безпеки забезпечується силами підрозділів безпеки банків і спеціалізованих фірм в організацій у галузі безпеки, а також спеціалізованих інформаційно – комунікаційних технологій і технічних засобів захисту інформації. Одним із важливих аспектів при формуванні системи інформаційної безпеки в банках є побудова системи управління ризиками банківської діяльності.

Зазначимо, що відповідно до методичних рекомендацій щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків за стандартами Національного банку України, «система управління ризиками банківської діяльності повинна будуватись на основі міжнародного стандарту *ISO/IEC 27005 «Information technology – Security techniques – Information security risk management»* (Управління ризиками ін – формаційної безпеки) з урахуванням особливостей банківської діяльності, стандартів і вимог Національного банку України з питань інформаційної безпеки. Особливим напрямом забезпечення інформаційної безпеки в банках є захист банківських інформаційних систем. Тому при розробленні архітектури та створенні інфраструктури банківської інформаційної системи слід забезпечити її захищеність від загроз. Вирішення цієї проблеми полягає в детальному аналізі таких взаємопов’язаних видів робіт, як проектування та впровадження банківської інформаційної системи, її атестація, аудит та обстеження на предмет безпеки» [11].

Заходи захисту інформації в засобах і мережах її передачі та обробки в основному передбачають використання апаратних, програмних і криптографічних засобів захисту:

Апаратні. Організаційні забезпечують регламентацію доступу і використання технічних засобів передачі та обробки інформації; Організаційно – технічні забезпечують блокування можливих каналів витоку інформації через технічні засоби забезпечення виробничої і трудової діяльності за допомогою спеціальних технічних засобів, що встановлюються на елементи конструкцій будівель і споруд, приміщень і технічних засобів, потенційно створюючи канали витоку інформації; Технічні забезпечують використання в процесі виробничої діяльності спеціальних, захищених від побічних випромінювань технічних засобів передачі та обробки конфіденційної інформації

Програмні. Спеціалізовані, забезпечують ідентифікацію об'єктів і суб'єктів, розмежування доступу до банківських інформаційних ресурсів, контроль і реєстрацію дій з банківською інформацією і програмами; універсальні.

Криптографічні. Забезпечують ідентифікацію середовища, з якого буде запускатися програма, аутентифікацію середовища, з якого запущена программа, відклик на запуск з несанкціонованого середовища, реєстрацію санкціонованого копіювання, протидії вивченню алгоритмів роботи системи забезпечують такий захист інформації, при якому у разі перехоплення її та обробки будь – якими способами, вона може бути дешифрована тільки протягом часу, необхідного їй для втрати своєї цінності.

На практиці всі заходи з використання апаратних засобів захисту розподіляються на три групи: організаційні, організаційно – технічні, технічні. Організаційні заходи апаратного захисту – це заходи обмежувального характеру, які передбачають регламентацію доступу і використання технічних засобів передачі та обробки інформації. Організаційно – технічні заходи забезпечують блокування можливих каналів витоку інформації через технічні засоби забезпечення виробничої і трудової діяльності за допомогою спеціальних технічних засобів, що встановлюються на елементи конструкцій будівель і споруд, приміщень і технічних засобів, потенційно створюючи канали витоку інформації.

Технічні заходи – це заходи, що забезпечують використання в процесі виробничої діяльності спеціальних, захищених від побічних випромінювань технічних засобів передачі та обробки конфіденційної інформації. Під програмними засобами захисту розуміють систему спеціальних програм, включених до складу програмного забезпечення комп'ютерів і інформаційних систем, що реалізують функції захисту конфіденційної інформації від неправомірних дій і програми їх обробки.

Програмні засоби забезпечують захист інформації від несанкціонованого доступу до неї, копіювання її або руйнування.

При захисті від несанкціонованого доступу за допомогою програмних засобів здійснюється:

- ідентифікація об'єктів і суб'єктів;
- розмежування доступу до інформаційних ресурсів;
- контроль і реєстрація дій з інформацією і програмами.

Захист інформації від копіювання забезпечується виконанням таких функцій:

– ідентифікація середовища, з якого буде запускатися програма;

– аутентифікація середовища, з якого запущена програма;

– реакція на запуск з несанкціонованого середовища;

– реєстрація санкціонованого копіювання;

– протидія вивченню алгоритмів роботи системи.

Під криптографічними заходами розуміють використання спеціальних пристроїв, програм, виконання відповідних дій, які роблять сигнал, переданий зовсім незрозумілим для сторонніх осіб. Криптографічні заходи забезпечують такий захист інформації, при якому у разі перехоплення її та оброблення будь – якими способами вона може бути дешифрована тільки протягом часу, необхідного їй для втрати своєї цінності. Для цього використовуються різні спеціальні засоби шифрування документів, мови, телеграфних повідомлень.

При побудові моделі використовується ряд специфічних прийомів:

● порівняння – процес, який забезпечує первинну оцінку інформації на основі зіставлення її елементів з відомими нам моделями і знаходження подібності між ними;

● аналіз – процес розподілу відбитої у вигляді предметів, подій, явищ інформації на складові елементи з наступним детальним розглядом окремих їх властивостей. У забезпеченні цього процесу провідна роль відводиться свідомості і підсвідомості;

● синтез – об'єднання групи властивостей, які притаманні відповідного предмета, об'єкту, в єдине ціле, створення моделей відомих нам об'єктів, процесів і явищ (стану, діяльності) з окремих елементів, прогнозування розвитку в часі, прогнозування по – ведінки окремих людей;

● узагальнення – ідентифікація раніше невідомих об'єктів, явищ з відомими в яких – небудь загальних ознаках. В узагальненні міститься як корисний, так і небезпечний компонент. Корисний – можливість об'єднання предметів і явищ у великі групи на основі невеликих груп базових ознак. Але при цьому виникає загроза спотворення об'єктивного стану цих предметів і явищ внаслідок дуже великого скорочення незначних ознак узагальнюючої моделі;

● виключення – процес, у якому звертається увага на відповідні аспекти особистого досвіду аналітика і виключаються інші. Це дозволяє в ситуаціях, які часто повторюються, швидко знаходити необхідну форму реакції, концентруючи увагу на який – небудь відповідної частини доступного досвіду. Така властивість дає можливість виключити надходження у свідомості зайвих зовнішніх стимулів;

● абстрагування – розгляд предмета, явища, елемента інформації у відриві від будь – якої реальності;

● трансформація – перетворення інформації, яка сприймається, відповідно до моделі, яку формують. Трансформація лежить в основі фантазії, прогнозу, будь – якої творчої діяльності.

Нині на ринку представлена достатня кількість програмного забезпечення, що відноситься до категорії засобів пошуку «злому» мереж. Це: 1. Internet Security Scanner (фірма Internet Security Systems). 2. NetRecon (фірма Axent). 3. NetProbe (фірма Qualix). 4. Ballista (фірма Secure Networks). 5. NetGuard (фірма Network Guardians). 6. NetSonar (фірма WheelGroup).

- «**NetRecon** використовує запатентовану технологію progressive scanning, яка дозволяє застосувати отриману інформацію від одного сервера до іншого. Symantec NetRecon забезпечує оцінку вразливості мережі за допомогою прогресивної технології сканування. Його унікальний механізм аналізу першопричин ілюструє точну послідовність кроків, зроблених для виявлення вразливих місць. NetRecon відображає дані про вразливості під час їх сканування, а потім надає відповідні звіти, щоб адміністраторам не довелося шукати за обсягами даних. Звіти можна підлаштувати під технічну чи виконавчу аудиторію, а часті оновлення безпеки за допомогою Symantec LiveUpdate забезпечують останні підписи та попередження про вразливість» [43].

- **CyberCop** компанії Network Associates

«Багато людей неправильно інформовані щодо CyberCop. Спочатку CyberCop був створений в компанії Network General (розробниками програми Sniffer) на основі технології виявлення атак, ліцензованої у компанії WheelGroup. CyberCop використовував Web / Java інтерфейс. Network Associates купила Network General (точніше McAfee Associates і Network General об'єдналися), а Cisco купила компанію WheekGroup. З невідомої причини Cisco відмовилася поновлювати ліцензійну угоду (бо компанія Cisco випускає конкуруючу систему виявлення атак NetRanger) і наскільки відомо Network Associates більше не пропонує CyberCop.

Однак NAI любить назву CyberCop і використовує його для нових продуктів. У компанії Secure Networks вона придбала систему аналізу захищеності Ballista і назвала її CyberCop Scanner.

Також NAI пропонує систему, звану CyberCop Server, яка відноситься до класу систем виявлення атак на рівні хоста і функціонує під управлінням Sun і

Windows NT. Цей продукт заснований на системі Stalker, розробленої компанією Haystack і придбаною компанією NAI.

- **RealSecure** компанії Internet Security Systems, Inc. (ISS)

Це єдине ПО, яке працює на великій кількості Windows і UNIX-платформ. Система створена в 1996 році. (Виявляє атаки, як на рівні мережі, так і на рівні операційної системи).

-**NetRanger** компанії WheelGroup / Cisco

На відміну від Cybercop і RealSecure, які контролюють трафік в режимі прослуховування трафіку (promiscuous), NetRanger - це маршрутизатор, який переглядає трафік, що проходить через нього. Компанія WheelGroup в 1998 була куплена Cisco, тому можна припустити, що Ви побачите це ПО, представлене у всіх інших маршрутизаторах останньої» [42].

2.3. Алгоритм забезпечення інформаційної безпеки банку.

Згідно постанові від 28.09.2017 № 95 « «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України», банк, у разі застосування криптографічного захисту, зобов'язаний використовувати криптографічні алгоритми з такого переліку:

1) асиметричні алгоритми:

- алгоритм Діффі – Геллмана (далі – алгоритм DH) для узгодження сеансових ключів шифрування;
- алгоритм цифрового підпису (далі – алгоритм DSA) для цифрових підписів;
- алгоритм Діффі – Геллмана на еліптичних кривих (далі – алгоритм ECDH) для узгодження сеансових ключів шифрування;
- алгоритм цифрового підпису на еліптичних кривих (далі – алгоритм ECDSA) для цифрових підписів;

– алгоритм Ривест – Шаміра – Адлемана (далі – алгоритм RSA) для цифрових підписів і узгодження сеансових ключів шифрування або аналогічних ключів;
– алгоритм цифрового підпису [ДСТУ 4145 – 2002 "Інформаційні технології.

Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння", затверджений наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 року № 31 (далі – ДСТУ 4145 – 2002)] для цифрових підписів;

2) алгоритми безпеки гешування SHA – 224, SHA – 256, SHA – 384, SHA – 512, "Купина" (ДСТУ 7564:2014 "Інформаційні технології. Криптографічний захист інформації. Функція гешування", прийнятий наказом Міністерства економічного розвитку і торгівлі України від 02 грудня 2014 року № 1431) або більш криптостійкі;

3) алгоритми симетричного шифрування:
– алгоритм "Advanced encryption standard" (AES) із використанням довжини ключа 128, 192 і 256 біт або більше;
– алгоритм криптографічного перетворення (ДСТУ ГОСТ 28147:2009 "Система оброблення інформації. Захист криптографічний. Алгоритм криптографічного перетворення", прийнятий наказом Державного комітету України з питань технічного регулювання та споживчої політики від 22 грудня 2008 року № 495);
– алгоритм "Калина" (ДСТУ 7624:2014 "Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення", прийнятий наказом Міністерства економічного розвитку і торгівлі України від 29 грудня 2014 року № 1484).

Банк, який застосовує алгоритм DH для узгодження сеансових ключів шифрування, зобов'язаний використовувати розмір модуля не менше ніж 2048 біт.

Банк, який застосовує алгоритм DSA для цифрових підписів, зобов'язаний використовувати розмір модуля не менше ніж 2048 біт.

Банк, який застосовує алгоритм на еліптичних кривих, зобов'язаний використовувати еліптичні криві з ДСТУ 4145 – 2002 або з Федерального стандарту оброблення інформації (США) (Federal information processing standards, FIPS186 – 4).

Банк, який застосовує алгоритм ECDH для узгодження сеансових ключів шифрування, зобов'язаний використовувати розмір поля/ключа не менший, ніж 160 біт.

Банк, який застосовує алгоритми ECDSA, ДСТУ 4145 – 2002 для цифрових підписів, зобов'язаний використовувати розмір поля/ключа не менший, ніж 160 біт.

Банк, який застосовує алгоритм RSA для цифрових підписів і ключів шифрування сеансу або аналогічних ключів, зобов'язаний використовувати розмір модуля не менше ніж 2048 біт.

Банк, який застосовує алгоритм RSA для цифрових підписів і ключів шифрування сеансу або аналогічних ключів, зобов'язаний використовувати різні ключові пари для передавання ключів шифрування сеансу (або аналогічних ключів) та для цифрових підписів.

Банк зобов'язаний використовувати останню версію протоколу захисту на транспортному рівні та реалізацію цього протоколу, що підтримує безпечне повторне погодження з'єднання для захисту з'єднань, які управляються протоколом Transmission control protocol (TCP). Якщо безпечне повторне погодження з'єднання не підтримується, то ця процедура має бути відключена» [31].

Банку забороняється використання анонімного (без автентифікації) алгоритму DH.

Банк, який застосовує стандарти для шифрування "Secure multipurpose internet mail extension" (далі – S/MIME), зобов'язаний використовувати цей стандарт не нижче версії 3.0.

Банк зобов'язаний використовувати набір протоколів для забезпечення захисту даних, що передаються за допомогою протоколу Інтернету (набір протоколів Internet protocol security, IPsec) у режимі ESP (Encapsulating security payload) (якщо банк не використовує криптографічний протокол захисту на транспортному рівні).

Банк зобов'язаний використовувати кабелі типу "вита пара" не нижче категорії 5E та/або оптично – волоконні кабелі для організації структурованої кабельної системи (далі – СКС).

Банк зобов'язаний забезпечити наявність та актуальність такої документації до СКС:

1) схеми (креслення) розміщення обладнання СКС та кабельних каналів;

2) схеми підключення обладнання СКС;

3) таблиці маркування кабелів СКС та кабельних з'єднань (кабельний журнал). Банк зобов'язаний забезпечити персоналізований та контрольований доступ до комутаційних вузлів СКС [16].

Висновки до другого розділу

Інформаційна безпека в банківському секторі є комплексним завданням, спрямованим на забезпечення безпеки його інформаційних ресурсів, що передбачає встановлення загроз і зниження ризиків банківської діяльності, організацію ефективної інформаційно та технічної підтримки управління цими процесами на основі використання сучасних інформаційно – комунікаційних технологій і технічних засобів.

Необхідність впровадження в банках України стандартів з управління інформаційною безпекою продиктована вимогами Базельського комітету

Basel II з управління та зменшення операційних ризиків банків. Тому система управління інформаційною безпекою, яка покликана забезпечити безпеку інформаційних ресурсів банків і банківського сектору в цілому, повинна спиратись на національні законодавчі норми та стандарти з управління інформаційною безпекою, а також використовувати досвід кращих світових практик і міжнародних стандартів і рекомендацій.

Процес формування системи інформаційної безпеки в банківському секторі України та затвердження відповіднх стандартів зумовлений викликами сьогодення й активно розвивається, тому питання формування системи інформаційної безпеки як на рівні банків, так і на державному рівні є актуальними й потребують подальших досліджень.

Сьогодні банки використовують спеціальні програмні комплекси зі сканування рівня інформаційної захищеності комп'ютерних мереж. Серед таких комплексів виступають спеціалізована мова Vulnerability Description Language, Internet SafeSuit (Internet Security Systems) та ін. Для контролю за виходом банківської інформації через «зломи» інформаційних мереж комп'ютерними злочинцями використовують відповідне програмне забезпечення.

РОЗДІЛ 3. РЕКОМЕНДАЦІЇ ЩОДО ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ

3.1 Вимоги до політики інформаційної безпеки банку

Страхарчук А. Я. розглядає політику інформаційної безпеки, як «набір законів, правил і практичних рекомендацій, на базі яких здійснюється керування, захист і розподіл критичної інформації в системі» [38].

Бодюл Є. М. під поняттям «політика інформаційної безпеки банківської установи» розуміє, «науково обґрунтовану систему поглядів на визначення основних напрямів, умов і порядку практичного вирішення задач інформаційного захисту банківської установи від протиправних дій» [5].

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

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

– виявлення та мінімізація потенційних загроз інформаційній безпеці;
– захист інформаційних активів організації;
– забезпечення безпеки та конфіденційності інформації про клієнтів;
– забезпечення стабільної та ефективної діяльності банківської установи.

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

– перелік законодавчих, регуляторних, нормативних вимог;
– затвердження переліку відомостей, що містять інформацію з обмеженим доступом;
– встановлення правил доступу до інформаційних ресурсів та програмно
– технічних комплексів;

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

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

– проведення політики ідентифікації та автентифікації ресурсів;

– політика криптографічного захисту інформації;

– політика «чистогоекрана» та «чистого столу»;

– проведення внутрішнього аудиту та вдосконалення системи управління інформаційної безпеки.

Залежно від стану інформаційної безпеки в банку Артемов А.В. виділяє «чотири основні типи політики інформаційної безпеки банку:

1. *програмна політика безпеки* використовуються при оцінці стану інформаційної небезпеки в банку і розробляється з метою визначення напрямів реструктуризації основних компонентів забезпечення інформаційної безпеки і їх реалізації. Програмна політика безпеки банку визначає множину стратегічних напрямків забезпечення інформаційної безпеки, види і обсяг ресурсів, які виділяються для реалізації політики;

2. формування *проблемно – орієнтованої політики* інформаційної безпеки банку здійснюють у випадку інформаційної загрози в банку. Об'єктом застосування проблемно – орієнтованої політики безпеки є окрема проблема або задача в області забезпечення безпеки інформації в фінансово – кредитній організації. Необхідність розробки проблемно – орієнтованої політики безпеки часто вимагає у відповідь як появу і використання в організації нових технологій, так і виникнення нових загроз та слабкостей. Частіше за все проблемно – орієнтована політика безпеки уточнює, конкретизує положення програмної політики безпеки чи об'єктової політики безпеки;

3. *системно – орієнтована політика* інформаційної безпеки банку використовується при стані інформаційного ризику, визначає напрямок, методи та процедури забезпечення інформаційної безпеки. Даний тип політики обмежений областю взаємодії самої системи і середовища її експлуатації. Для

розробки пов’язаного та повного набору правил безпеки розробник повинен використовувати спеціальні прийоми, за допомогою яких на основі аналізу задач захисту формулюються правила безпеки;

4. *системна політика* містить загальні вимоги до безпеки інформації та рішення щодо забезпечення режиму інформаційної безпеки. Повинна містити правила безпеки відносно фізичної безпеки, аутентифікації, ідентифікації та управління доступом, правила застосування криптографічних засобів, правила забезпечення антивірусного захисту та інші питання моніторингу актуальності сформульованих та уточнених задач захисту в процесі експлуатації системи (стан інформаційної безпеки банку)» [1].

Основними принципами Політики, є підтримання належного захисту інформації із забезпеченням цілісності, конфіденційності, доступності та спостережності. Це в першу чергу стосується Інформації з обмеженим доступом.

Банк підтримує ризик – орієнтовний підхід, який забезпечує розуміння, моніторинг та зменшення ризиків операційної діяльності. Деталі ризик – орієнтованого підходу описані в політиці управління інформаційною безпекою.

Всі працівники Банку забов'язнані та виконують вимоги інформаційної безпеки в роботі.

Під час розроблення, впровадження та функціонування програмно – технічних комплексів, враховуються вимоги інформаційної безпеки.

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

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

Про кожний Інцидент інформаційної безпеки працівники Банку негайно інформують безпосереднього керівника. Документами з інформаційної безпеки Банку передбачені процедури аналізу та реакції на той чи інший Інцидент

інформаційної безпеки. За результатами аналізу вживаються заходи щодо недопущення повторення подібних інцидентів.

При забезпеченні інформаційної безпеки Банк керується ризик – орієнтованим підходом, який забезпечує розуміння, моніторинг та зменшення ризиків діяльності. Банк обробляє ризики інформаційної безпеки відповідно до внутрішньої методології, на підставі оцінки ймовірності реалізації ризиків та важкості їх наслідків, визначає три рівні ризиків: високий, середній та низький. Банк має право прийняти ризик будь – якого рівня, проте рішення про прийняття високого рівня ризику має прийматись керівництвом на підставі повної поінформованості, аналізу загроз та, за умов здійснення дієвих заходів зі зменшення рівня ризику (в тому числі впровадження компенсаційних заходів).

В цій Політиці терміни та скорочення вживаються в такому значенні: Керівництво Банку (керівництво) – Голова та Члени Правління Банку, Голова та Члени Спостережної Ради.

Інформаційні активи – всі комп'ютерні системи, програмне забезпечення та інше периферійне обладнання, яке використовується для обробки або зберігання даних, а також інформація, що обробляється за їх допомогою.

Інформаційна безпека (ІБ) – сукупність процесів та заходів, які мають на меті забезпечення цілісності, конфіденційності, доступності та спостережності інформації.

Інформаційні системи (ІС) – комп'ютерні системи, програмне забезпечення, телекомунікаційне та периферійне обладнання. Власник інформаційної системи (далі – власник ІС) – підрозділ Банку, що використовує цю систему для забезпечення процесів підрозділу та має ухвалену керівництвом Банку відповідальність щодо контролювання впровадження, розвитку, підтримування, використання та безпеки цієї системи.

Заходи безпеки – засоби керування ризиком, включаючи політики, процедури, інструкції, практики та організаційну структуру, які можуть носити адміністративний, технічний, управлінський чи юридичний характер.

Загроза – будь – які обставини чи події, що можуть спричинити порушення політики ІБ та нанесення збитку Банку. Вразливість – нездатність протистояти реалізації певної загрози або ж сукупності загроз.

Ризик ІБ (ризик) – ймовірність того, що визначена загроза, впливаючи на вразливості системи або групи систем, може спричинити шкоду Банку.

Система управління інформаційною безпекою (СУІБ) – частина загальної системи управління Банку, заснована на підході оцінки ризиків, призначена для створення, впровадження, експлуатації, контролю, аналізу, підтримки і покращення інформаційної безпеки Банку.

Забезпечення ІБ та СУІБ Банку ґрунтуються на таких фундаментальних принципах:

– принцип законності: СУІБ Банку виконує вимоги чинного законодавства України, а також застосовує міжнародні норми в галузі ІБ.

– принцип узгодженості: цілі та завдання ІБ відповідають стратегічним цілям та завданням Банку.

– принцип єдності: управління інформаційної безпекою є невід'ємною частиною управління Банком.

– принцип ефективності: засоби захисту інформаційних активів впроваджуються відповідно до їхньої критичності, тобто категорії класифікації та рівня ризику інформаційного активу.

– принцип практичності: засоби захисту інформаційних активів повинні бути практичними та підтримувати баланс між працездатністю і захищеністю ІС.

– принцип безперервності: ІБ є постійним процесом протистояння загрозам та управління ризиками, характерними для сфери діяльності Банку.

– принцип відповідальності: керівництво Банку всіх рівнів, працівники, бізнес–партнери та інші треті сторони, які мають доступ до інформаційних активів Банку, повинні дотримуватися вимог нормативних документів

Банку в області ІБ та нести персональну відповідальність за їхнє невиконання.

– принцип комплексності та системності: ІБ Банку забезпечується на правовому, адміністративному, організаційному та програмно – технічному рівнях, а також на підставі комплексного застосування засобів захисту інформації та взаємодії всіх підрозділів Банку.

Складові політики інформаційної безпеки:

1. визначення критичних бізнес – процесів/банківських
2. продуктів;
3. надання доступу до інформації;
4. контроль доступу;
5. парольний захист;
6. антивірусний захист;
7. захист мережі банку;
8. віддалений доступ до ресурсів мережі;
9. ідентифікація та автентифікація ресурсів СУІБ;
10. криптографічний захист інформації;
11. політика «чистого екрана» та «чистого стола»

Інформаційна безпека будь – якої організації ґрунтується на системі заходів безпеки, що здійснюються відповідно до вимог безпеки. Основними джерелами вимог інформаційної безпеки організації є:

1) результат оцінювання ризиків для організації, який враховує загальну бізнес – стратегію та цілі (під час оцінювання ризику ідентифікують загрози ресурсам СУІБ і оцінюють вразливість та ймовірність подій і визначають величину потенційного впливу);

2) правові вимоги, визначені законодавством, договорами і угодами організації з партнерами;

3) власний набір принципів, цілей та бізнес – вимог щодо оброблення інформації, який розроблено організацією для підтримки свого функціонування.

Важливим є 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).

Особливу увагу слід звернути на умови угод та договорів з третіми сторонами. Відповідно до п. 6.2 стандарту СОУ Н НБУ 65.1 СУІБ 2.0:2010 безпека інформації та засобів оброблення інформації банку не повинна знижуватися через уведення в експлуатацію продуктів або послуг зовнішньої сторони. Якщо є бізнес – потреба в роботі із зовнішніми сторонами, яка може вимагати доступу до інформації або засобів оброблення інформації банку, або в отриманні від зовнішньої сторони чи наданні їй продукту та послуги, тоді банк повинен виконувати оцінку ризику для визначення вимог щодо заходів безпеки та наслідків порушення безпеки. Заходи безпеки мають бути погоджені та визначені в угоді із зовнішньою стороною. Ці питання розглядаються не тільки для договорів про надання послуг клієнтам банку (системи типу «клієнт – банк», інтернет – банкінг, мобільний банкінг тощо), а також при отриманні послуг зовнішніх сторін (розробка та супроводження програмного забезпечення, придбання та технічне обслуговування обладнання, надання послуг зв’язку тощо).

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

Вразливості, які можуть стати причиною негативної дії загроз інформаційній безпеці банку можуть розглядатися на таких рівнях:

- банк в цілому;
- процеси та процедури;
- системи управління;
- персонал;

- фізичне середовище;
- конфігурація програмно – технічних комплексів, обладнання тощо;
- залежність від зовнішніх організацій.

При цьому некоректно запроваджені чи не дієві заходи безпеки є одним із видів вразливостей, що зменшують рівень безпеки банку в цілому і кожного бізнес – процесу / банківського продукту окремо.

Документи Політики розробляються Управлінням захисту електронної інформації та іншими підрозділами Банку за відповідними напрямками діяльності. Постійний контроль впровадження, виконання, вдосконалення та підтримки Політики в актуальному стані покладений на Комітет.

3.2. Розробка політики інформаційної безпеки банку

При розробці політики інформаційної безпеки фінансово – кредитної установи необхідно враховувати об'єктивні проблеми, які можуть постати на шляху реалізації політики інформаційної безпеки банку. Такими проблемами можуть стати закони країни і міжнародного співтовариства, внутрішні вимоги, етичні норми суспільства.

«Методичними рекомендаціями щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України серед джерел вимог з інформаційної безпеки визначено:

- 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.

Виділяють основні етапи розробки політики інформаційної безпеки:

– визначення та оцінка інформаційних активів;

– визначення загроз безпеці;

– оцінка інформаційних ризиків;

– визначення відповідальності;

– створення комплексного документа;

– реалізація;

– управління програмою безпеки» [24].

По Артеменко Д.А., «основою для формування політики інформаційної безпеки банківської установи можна визначити:

– характеристику об’єкта застосування;

– аналіз поточного стану захисту інформаційної інфраструктури банку;

– облік можливих негативних факторів впливу та ймовірність їх реалізації;створення методології ухвалення управлінських рішень щодо забезпечення інформаційної безпеки» [2].

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

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

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

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

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

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

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

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

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

Всі розроблені документи з питань інформаційної безпеки доступні працівникам банку у межах їх повноважень і призначені надавати допомогу у виконанні вимог інформаційної безпеки.

Зміст політики розміщується на корпоративному сайті банку після її затвердження належним чином. Перегляд політики здійснюється за потреби, але не менш ніж раз на рік, під час перегляду СУІБ керівництвом банку. Ця політика набирає чинності з дати затвердження рішенням Спостережною радою. Дана редакція політики втрачає свою чинність з дати набрання чинності наступної / нової редакції або на підставі рішення Спостережної Ради. У разі невідповідності будь – якої частини політики чинному законодавству України або нормативно – правовим актам Національного банку України, у тому числі у зв'язку з прийняттям нових актів законодавства України або нормативно – правових актів Національного банку України, ця політика діє лише в тій частині, яка не суперечить нормативно – правовим актам Національного банку України та чинному законодавству України.

Документація СУІБ.

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

1. *Адміністративні документи* є обов'язковою відправною точкою підготовки до впровадження СУІБ. До них належать:

- наказ про створення спеціального керівного органу з питань інформаційної безпеки (за необхідністю);
- положення про спеціальний керівний орган з питань інформаційної безпеки (за його наявністю);
- у разі відсутності спеціального керівного органу з питань інформаційної безпеки наказ про покладення обов'язків цього органу на існуючий керівний орган;
- наказ про впровадження та функціонування СУІБ;
- наказ про призначення керівника проекту впровадження та функціонування СУІБ;
- положення про службу захисту інформації (підрозділ інформаційної безпеки);
- положення про службу безпеки (охорона, пропускний та внутрішньо – банківський режим тощо);
- посадові інструкції відповідальних за впровадження та функціонування СУІБ осіб;
- організаційна структура банку.

Ці документи оформляються відповідно до правил внутрішнього діловодства банку і залежно від особливостей роботи банку можуть бути поєднаними між собою. Наприклад, якщо підрозділ захисту інформації входить

до складу одного структурного підрозділу разом з фахівцями з фізичної безпеки, то створюється тільки одне положення про підрозділ банківської безпеки. Відповідно назви підрозділів формуються згідно з внутрішніми правилами банку.

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

До першої групи належать два основних документа, що визначають стратегію розвитку банку та загальну політику інформаційної безпеки. Стратегія розвитку банку містить основні стратегічні цілі банку, зокрема й ті, які пов’язані з впровадженням нових бізнес – процесів/банківських продуктів із використанням новітніх технологій і потребують захисту інформації. Наявність такого документу дозволяє забезпечити планування розвитку інфраструктури банку та заходів безпеки, які повинні бути передбачені у СУІБ для зменшення операційних ризиків банку. Політика інформаційної безпеки банку вміщує основні цілі безпеки та принципи забезпечення безпеки банку. Обидва документа мають бути короткими (2 – 3 стор.), прийнятними для зрозуміння всіма працівниками банку та бути достатньо конкретними.

До другої групи документів верхнього рівня належать документи, які описують основу побудови СУІБ:

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

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

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

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

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

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

Останнім документом створюється політика щодо застосовності, у якій надається перелік заходів безпеки відповідно до стандарту Національного банку України з доповнений додатковими заходами безпеки (за необхідності з поясненням причин проведення і коротким описом їх реалізації в банку).

Зазначений вище перелік другої групи документів верхнього рівня є неповним і необов'язковим, він може бути скороченим або доповненим іншими документами. Під час прийняття рішення щодо переліку цих документів слід враховувати те, що короткі, чіткі та зрозумілі документи є більш зручними і ефективним ніж один великий за обсягом і складно структурований документ, з яким важко працювати і який важко оновлювати 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.

3. *Документи середнього рівня* фактично є технічними документами, які спрямовані на опис способів реалізації заходів безпеки для захисту ресурсів СУІБ від загроз. Саме документи цього рівня описують конкретні операції, які мають виконуватися різними користувачами, питання розподілу повноважень та відповідальності по кожної операції, встановлюють строки виконання кожної операції, визначають 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 та ін. Основними користувачами документів середнього рівня є керівники відповідних підрозділів, відповідальні особи за окремі ресурси СУІБ, адміністратори.

Як зазначав Кавун С.В. «Перелік документів середнього рівня формується згідно із Додатком А стандарту Національного банку України СОУ Н НБУ 65.1 СУІБ 1.0:2010, до них в основному належать описи різноманітних процедур щодо:

А.6. Організації інформаційної безпеки;

А.7. Управління ресурсами СУІБ;

А.8. Безпеки людських ресурсів;

А.9. Фізичної безпеки та безпеки інфраструктури;

А.10. Управління комунікаціями та функціонуванням;

А.11. Контролю доступу;

А.12. Придбання, розроблення та підтримки інформаційних систем;

А.13. Управління інцидентами інформаційної безпеки;

А.14. Управління безперервністю бізнесу;

А.15. Відповідності.

4. *Документи нижнього рівня* можна поділити на дві групи.

До першої групи належать 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 необхідно забезпечити їх збереження та захист від знищення та несанкціонованої модифікації.

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

Під час перегляду наявних документів, підготовки нових та доопрацьованих документів рекомендується всі необхідні документи формувати за єдиними правилами, що забезпечить легкість їх сприйняття користувачами.

Серед загальних рекомендацій щодо формування документів можна виділити такі:

– усі документи формувати у єдиному стилі;

– документи повинні бути простими для розуміння та максимально короткими;

– для спрощення розуміння використовувати блоксхеми, рисунки, таблиці;

– за можливістю поєднувати загальні правила для користувачів в одному документі;

– відображати вимоги з інформаційної безпеки в посадових інструкціях;

– у залежності від технології документообігу банку слід вибирати найбільш оптимальний варіант поширення документів в електронному або паперовому вигляді (у разі використання електронних документів слід забезпечити їх цілісність протягом усього періоду використання);

– постійно переглядати перелік документації з метою його оптимізації та зменшення обсягу конкретних документів;

– створювати журнали для записів тільки там, де цього потребують стандарти та чинні правила бізнесу (за можливістю рекомендується автоматизувати процедуру ведення журналів)» [23].

Висновки до третього розділу

Метою політики інформаційної безпеки банку є впровадження та ефективне функціонування системи управління інформаційною безпекою, яка буде забезпечувати безпечність та надійність функціонування бізнес – процесів, захист інформації та ресурсів Банку від зовнішніх та внутрішніх

загроз та загроз, які пов’язані з навмисним та ненавмисними діями співробітників Банку, забезпечувати безперервну роботу Банку, сприяти мінімізації ризиків операційної діяльності Банку та створювати позитивну репутаціюБанку при роботі з Клієнтами.

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

При розробці політики інформаційної безпеки фінансово – кредитної установи необхідно враховувати об’єктивні проблеми, які можуть постати на шляху реалізації політики інформаційної безпеки банку. Такими проблемами можуть стати закони країни і міжнародного співтовариства, внутрішні вимоги, етичні норми суспільства.

Політика підтримується в актуальному стані та переглядається за необхідності, але не рідше одного разу на рік.

Причинами внесення змін до політики, є зміни в інформаційній інфраструктурі та/або впровадження нових інформаційних технологій, доповнення законодавчих, нормативно — правових актів НБУ та інших документів.

Політика інформаційної безпеки Банку (далі – Політика) передбачає подальше планування розвитку інфраструктури Банку та заходів безпеки, які повинні бути передбачені у Системі управління інформаційною безпекою (далі – СУІБ) для зменшення операційних ризиків Банку.

Політика розробляється відповідно до вимог законодавства України, нормативно – правових актів Національного банку України (в тому числі стандартів СОУ Н НБУ 65.1 СУІБ 1.0:2010 та СОУ Н НБУ 65.1 СУІБ 2.0:2010), а також вимогам міжнародних та внутрішньодержавних платіжних систем та систем переказу коштів.

Національний банк України запровадив галузеві стандарти управління інформаційною безпекою. Ці документи фактично дублюють міжнародні стандарти I50/IEC 27001 та I80/IEC 27002, які визначають вимоги і правила впровадження системи управління інформаційною безпекою.

Постанова № 474 Національного банку України прийнята відповідно до статті 7 Закону України «Про Національний банк України», статті 10 Закону України «Про захист інформації в інформаційно – телекомунікаційних системах» і статті 10 Закону України «Про стандартизацію», з метою підвищення рівня інформаційної безпеки в банківській системі України.

Всі розроблені документи з питань інформаційної безпеки доступні працівникам Банку у межах їх повноважень і призначені надавати допомогу у виконанні вимог інформаційної безпеки.

Крім того впровадження стандартів з питань управління інформаційною безпекою не може бути разовою акцією. Це фактично безперервний процес розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення СУІБ. Саме тому методологічною основою управління інформаційною безпекою, відповідно до стандартів серії ISO 27000, є процесний підхід.

ВИСНОВКИ

Отже, інформаційна безпека – стан інформаційної системи, у якому вона може протистояти впливу внутрішніх і зовнішніх ризиків. Сьогодні існує гостра необхідність побудови повноцінної системи інформаційної безпеки. Зокрема, гострим постає питання інформаційної безпеки банківських систем не лише для України, а й для світу в цілому. Для банків ця проблема є дуже важливою, оскільки щомісяця в світі звідти відбувається витік інформації, результатом чого є не лише втрата довіри клієнтів, а й значні. Існує багато сучасних методів захисту інформації у банках, використання яких помітно зменшило кількість основних каналів витоку інформації протягом останніх двох років.

Інформаційна безпека в банківському секторі є комплексним завданням, спрямованим на забезпечення безпеки його інформаційних ресурсів, що передбачає встановлення загроз і зниження ризиків банківської діяльності, організацію ефективної інформаційно та технічної підтримки управління цими процесами на основі використання сучасних інформаційно – комунікаційних технологій і технічних засобів.

Необхідність впровадження в банках України стандартів з управління інформаційною безпекою продиктована вимогами Базельського комітету Basel II з управління та зменшення операційних ризиків банків. Тому система управління інформаційною безпекою, яка покликана забезпечити безпеку інформаційних ресурсів банків і банківського сектору в цілому, повинна спиратись на національні законодавчі норми та стандарти з управління інформаційною безпекою, а також використовувати досвід кращих світових практик і міжнародних стандартів і рекомендацій.

Процес формування системи інформаційної безпеки в банківському секторі України та затвердження відповіднх стандартів зумовлений викликами сьогодення й активно розвивається, тому питання формування системи

інформаційної безпеки як на рівні банків, так і на державному рівні є актуальними й потребують подальших досліджень.

Сьогодні банки використовують спеціальні програмні комплекси зі сканування рівня інформаційної захищеності комп'ютерних мереж. Серед таких комплексів виступають спеціалізована мова Vulnerability Description Language, Internet SafeSuit (Internet Security Systems) та ін. Для контролю за виходом банківської інформації через «зломи» інформаційних мереж комп'ютерними злочинцями використовують відповідне програмне забезпечення.

Метою політики інформаційної безпеки банку є впровадження та ефективне функціонування системи управління інформаційною безпекою, яка буде забезпечувати безпечність та надійність функціонування бізнес – процесів, захист інформації та ресурсів Банку від зовнішніх та внутрішніх загроз та загроз, які пов'язані з навмисним та ненавмисними діями співробітників Банку, забезпечувати безперервну роботу Банку, сприяти мінімізації ризиків операційної діяльності Банку та створювати позитивну репутаціюБанку при роботі з Клієнтами.

При розробці політики інформаційної безпеки фінансово – кредитної установи необхідно враховувати об'єктивні проблеми, які можуть постати на шляху реалізації політики інформаційної безпеки банку. Такими проблемами можуть стати закони країни і міжнародного співтовариства, внутрішні вимоги, етичні норми суспільства.

Політика підтримується в актуальному стані та переглядається за необхідності, але не рідше одного разу на рік.

Причинами внесення змін до політики, є зміни в інформаційній інфраструктурі та/або впровадження нових інформаційних технологій, доповнення законодавчих, нормативно — правових актів НБУ та інших документів.

Політика інформаційної безпеки Банку передбачає подальше планування розвитку інфраструктури Банку та заходів безпеки, які повинні бути

передбачені у Системі управління інформаційною безпекою для зменшення операційних ризиків Банку.

Політика розробляється відповідно до вимог законодавства України, нормативно – правових актів Національного банку України, а також вимогам міжнародних та внутрішньодержавних платіжних систем та систем переказу коштів.

Національний банк України запровадив галузеві стандарти управління інформаційною безпекою. Ці документи фактично дублюють міжнародні стандарти, які визначають вимоги і правила впровадження системи управління інформаційною безпекою.

Всі розроблені документи з питань інформаційної безпеки доступні працівникам Банку у межах їх повноважень і призначені надавати допомогу у виконанні вимог інформаційної безпеки.

Крім того впровадження стандартів з питань управління інформаційною безпекою не може бути разовою акцією. Це фактично безперервний процес розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення СУІБ. Саме тому методологічною основою управління інформаційною безпекою, відповідно до стандартів серії ISO 27000, є процесний підхід.

Для отримання помітних результатів не достатньо прийняття нормативних постанов, необхідна взаємодія нормативно – правового, організаційно – економічного та морально – етичного елементів інформаційної системи. Лише поєднання ефективної дії цих сегментів дозволить забезпечити довгостроковий прогнозований розвиток інформаційної безпеки не лише банківських установ, а й держави в цілому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Артемов А. В. Информационная безопасность. Курс лекций / А. В. Артемов. – К., 2014 – 205 с.
2. Барановський О. І. Банківська безпека: проблема виміру / О. І. Барановський // Економічне прогнозування. – 2015. – № 1. – С. 7-32.
3. Аникин И. В. Методы и средства защиты компьютерной информации / И. В. Аникин, В. И. Глова, А. Н. Нигматуллина // Учебноепособие. Казань: Изд-во Казан. гос. техн. ун – та, 2016.– 212 с.
4. Бєгун А.В. Щодо питань про сучасні методи регулювання безпеки / А. В. Бєгун, В. Ф. Гречанінов, В. П. Клименко // Математичні машини і системи. – 2013. – № 4. – К. : ІПММС, 2013. – С. 135-146.
5. Бодюл Є. М. Інформаційна безпека банку / Є. М. Бодюл // Протидія злочинам, які вчиняються з використанням комп'ютерних мереж [Текст]: тези доповідейМіжнародної науково – практичної конференції (м. Севастополь, 1-2 жовтня 2010 року) / Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України».– Суми : ДВНЗ «УАБС НБУ», 2010.– С. 53-55.
6. Болгар Т. М. Фінансова безпека банків в умовах ринкової трансформації економіки України: автореф. дис. на здобуття наук. ступеня канд. екон. наук: спец. 08.00.08 / Т. М. Болгар. – Суми: ДВНЗ «УАБС НБУ», 2014. – 22 с.
7. Бондаренко М. Ф. Визначення та обґрунтування суті політики інформаційної безпеки / М. Ф. Бондаренко, О. В. Потій, Ю. І. Горбенко та ін.// Радиотехника.– 2012.– № 134.– С. 9-25.
8. Васильчак С. В. Організація безпеки банківської діяльності в Україні / С. В. Васильчак, С. Ф. Вінтоняк // Науковий вісник ЕЛТУ України. – Вип. 21. – С. 153-157.
9. Винников А. С. Банк России и банковскаябезопасность / А. С. Винников // Регион.– № 2. – С. 45-52.

10. Гамза В.А. Безопасность банковской деятельности / В.А. Гамза, И.Б. Ткачук, И.М. Жилкин. – К., 2015. – 212 с.
11. Галузевий стандарт України: Інформаційнітехнології. Методи захисту. Система управлінняінформаційною безпекою (Вимоги Iso/Iec 27001:2005, Mod) [Електронний ресурс] / НБУ – Режим доступу: http://auditagency.com.ua
12. Голобородько Ю. О. Теоретичні підходи до розкриття сутності та складових фінансової безпеки банківських установ / Ю. О. Голобородько // Науковий вісник НЛТУ України. – 2012. – Вип. 22.12. – С. 194-198.
13. Дмитров С. О. Управліннясфінансовою безпекою комерційного банку / О. С. Дмитров // Фінансовийпростір. – № 2 (6). – 2012. – С. 11-15.
14. Домарєв В. В. Обґрунтування основних функцій системи управліннясінформаційною безпекою / В. В. Домарєв, Д. В. Домарєв, С. Б Гордієнко. // Вісник Державного університетуінформаційно – комунікаційнихтехнологій.– 2012.– Т. 10, № 2.– С. 102-104.
15. Енциклопедія банківської справи України / ред. В. С. Стельмах; Національний банк України, Інститут незалежних експертів. – К.: Молодь: Ін Юре, 2017. – 680 с.
16. Євченко Н. Г. Вплив податкових ризиків на фінансову безпеку банку / Н. Г. Євченко, О. А. Криклій // Проблеми і перспективи розвитку банківської системи України: збірник наукових праць. – Суми: ДВНЗ «УАБС НБУ», Вип. 25. – С. 45-52.
17. Єпіфанов А. О. Фінансова безпека підприємств і банківських установ: монографія / За заг. редакцією д-ра екон. наук, проф. А. О. Єпіфанова, [А. О. Єпіфанов, О. Л. Пластун, В. С. Домбров – ський та ін.]. – Суми: ДВНЗ «УАБС НБУ». – 295 с.
18. Єрмошенко А. М. Визначення поняття фінансової безпеки страховика та її категорій / А. М. Єрмошенко // Актуальні Проблеми Економіки. – 2018. – № 4. – С. 46-51.

19. Закон України «Про банки і банківськудіяльність» від 17.01.2001 // Відомості Верховної Ради України. – № 4.
20. Закон України «Про захист інформації в інформаційно – телекомунікаційних системах» // Відомості Верховної Ради (ВВР), 1994, № 31, ст.286 (із змінами та доповненнями).
21. Зачосова Н. В. Особливості забезпечення фінансової безпе – ки комерційних банків в Україні / Н. В. Зачосова // Науковий вісник: Фінанси, банки, інвестиції – № 4. – С. 74-78.
22. Зубок М. І. Безпека банківської діяльності: навч. посібн. / М. І. Зубок. – К.: Вид-во КНЕУ, 2016 – 190 с.
23. Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2008. – 352 с.
24. Банківська безпека: Підручник / КорченкоА.О., Скачек Л.М, Хорошко В.О. /За заг. ред. докт. техн. наук, проф. О.В.Хорошка. – К.: ПВП «Задруга», 2014 – 185 с..
25. КорченкоА.О. Банківська безпека: Підручник / КорченкоА.О., Скачек Л.М, Хорошко В.О. / За заг. ред. докт. техн. наук, проф. О.В.Хорошка. – К.: ПВП «Задруга», 2014 –185 с.
26. Котковський В. С. Чинники забезпечення фінансової складової безпеки банківської діяльності / В. С. Котковський, В. В. Орлов // Вісник економіки транспорту і промисловості. – № 38. – 2012. – С. 50-54.
27. Литовченко О. Ю. Теоретико – методичне підґрунтя до управ – ління фінансовою безпекою банку / О. Ю. Литовченко, Б. М. Самойлов [Електронний ресурс]. – Режим доступу: www. rusnauka.com.
28. Макаренко Є.А. Міжнароднаінформаційна безпека: сучасні виклики та загрози / Є. А. Макаренко, М. А. Ожеван, М. М. Рижков та ін. – К.: Центр Вільної преси, 2016. – 916 с.
29. Петренко С. А. Политикиинформационнойбезопасности / С. А. Петренко, В. А. Курбатов.– М.: КомпанияАйТи, 2015. – 400 с.

30. Побережний С. М. Фінансова безпека банківської діяльності: навч. посібн. / С. М. Побережний, О. Л. Пластун, Т. М. Болгар – Суми: ДВНЗ «УАБС НБУ», 2010. – 112 с.
31. Постанова від 28.09.2017 р. № 95 «Про затвердження Положення про організаціюзаходівіз забезпечення інформаційної безпеки в банківськійсистемі України» [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/en/v0095500 – 17/page
32. Постанова Правління Національного Банку України «Про внесення змін до Положення про порядок перевірки стану інформаційної безпеки в банківських та інших установах, які використовують засоби захисту інформації Національного банку України» від 13 лютого 2019 року N 38. URL: https://ips.ligazakon.net/document/view/pb19045?an=2 (дата звернення 10.11.2019)
33. Про основи національної безпеки України: Закон України: № 964 – IV від 19 червня 2003 року: Відомості Верховної Ради України. – 2003. – № 39. – ст. 351.
34. Сороківська З. До питання фінансової безпеки банку в умовах світової економічної кризи / З. Сороківська // Економічний аналіз. – 2011. – Вип. 8. – Ч.1. – С. 404-408.
35. Стадник Р.Е. DDOS-атаки як загроза інформаційній безпеці / Р.Е. Стадник // Матеріали Науково-технічної конференції «Актуальні проблеми забезпечення інформаційної безпеки держави». – К., 2015. – С. 94-95.
36. Стадник Р.Е. Сертифікат безпеки / Р.Е. Стадник // Збірник матеріалів II Міжнародної науково-техніної конференції студентства та молоді «Світ телекомунікації та інформатизації». – К., 2016. – С. 107-108.
37. Стельмах В. С. Енциклопедіябанківської справи України / ред. В. С. Стельмах; Національний банк України, Інститут незалежних експертів. – К. : Молодь : Ін Юре, 2017 – 680 с.

38. Страхарчук А. Я. Інформаційні системи і технології в банках: Навч. посіб. / А. Я. Страхарчук, В. П. Страхарчук. – К.: УБС НБУ: Знання, 2010.– 515 с.
39. Черевко О. В. Джерела виникнення загроз інформаційній безпеці банківських установ / О. В. Черевко, В. М. Андрієнко, І. Ю. Напора // Вісник Черкаського університету. Серія: Економічнінауки.– 2016.– № 3. – С. 120-127.
40. Фадєєв Д. А. Фінансова безпека банківськоїдіяльності в Україні / Д. А. Фадєєв [Електронний ресурс]. – Режим досту – www.rusnauka.com
41. Янковський А. 5 ключових проблем у сфері інформаційної безпеки [Електронний ресурс] / А. Янковський. – Режим доступу: http://cripo.com.ua
42. CityForum. URL: http://citforum.ru/security/internet/faq/faq_ids402.shtml (дата звернення 12.10.2019)
43. Symantec. URL: https://www.symantec.com/products/endpoint (дата звернення 08.11.2019)

ДОДАТКИ

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПАТ «ПЕРШИЙ ІНВЕСТИЦІЙНИЙ БАНК»

1. Вступ

Політика інформаційної безпеки ПАТ «ПЕРШИЙ ІНВЕСТИЦІЙНИЙ БАНК» (надалі - Політика) – це внутрішній нормативний документ, який описує та регламентує систему управління інформаційною безпекою ПАТ «ПЕРШИЙ ІНВЕСТИЦІЙНИЙ БАНК» (надалі – Банк). Політику складено у відповідності до вимог законодавства України та рекомендацій стандартів Національного банку України СОУ Н НБУ 65.1 СУІБ 1.0:2010 «Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги» (ISO/IES 27001:2005, MOD) та СОУ Н НБУ 65.1 СУІБ 2.0:2010 «Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою» (ISO/IES 27002:2005, MOD), а також міжнародних стандартів ISO/IEC 27001:2005 та ISO/IEC 27002:2005.

Інформація є ресурсом, який, як і інші важливі бізнес-ресурси, має певну цінність для Банку а, отже, потребує відповідного захисту.

Інформаційна безпека передбачає захист інформації від різноманітних загроз для підтримки безперервності бізнесу, скорочення збитків, збільшення прибутку на інвестований капітал і розширення можливостей бізнесу.

Яку б форму не обрала інформація, і які б кошти не використовувалися для її передачі та зберігання, необхідно завжди забезпечувати відповідний рівень її захисту.

В рамках даної Політики під інформаційною безпекою мається на увазі забезпечення наступних характеристик інформації:

- конфіденційність: надання доступу до інформації тільки тим, у кого є на це право;
- цілісність: захист точності і повноти інформації і методів її обробки;
- доступність: забезпечення доступу до інформації і пов'язаних з нею ресурсів авторизованими користувачами по мірі необхідності.

Інформаційна безпека досягається шляхом впровадження сукупності необхідних засобів захисту, в число яких можуть входити політики, рекомендації, інструкції, організаційні структури та програмні функції.

У разі невідповідності будь-якої частини цієї Політики чинному законодавству України, нормативно-правовим актам Національного банку України, у т.ч. у зв’язку із внесенням до них змін та доповнень, прийняттям нових законодавчих актів України, підрозділи Банку керуються даною Політикою у частині, що не суперечить чинному законодавству. 1 Політика описує прийняту та впроваджену Банком політику щодо захисту інформаційної безпеки. Політика інформаційної безпеки Банку є обов’язковою для використання всіма підрозділами Банку.

2. Терміни та скорочення Термін / скорочення Тлумачення

Банк - ПАТ «ПЕРШИЙ ІНВЕСТИЦІЙНИЙ БАНК»

Бізнес-процес - структурована послідовність дій з виконання певного виду діяльності на всіх етапах життєвого циклу банківської діяльності, метою якої є отримання заданого результату, що має цінність для Банку.

Загроза - потенційна причина небажаного інциденту, яка може призвести до шкоди для системи або організації. Інформаційна безпека захист інформації від широкого діапазону загроз з метою забезпечення безперервності бізнесу, мінімізації ризику бізнес- процесів і отримання максимальної рентабельності інвестицій і бізнес-можливостей.

КУІБ - спеціальний колегіальний орган Банку з питань інформаційної безпеки.

Несанкціонована мособа, об'єкт або процес - особа, об’єкт або процес, які не контролюються Банком та/або не задовольняють вимоги, які до них висуваються.

Ресурси СУІБ - ресурси (ресурси користувачів – людські, інформаційні; технологічні ресурси - ПТК та засоби їх підтримки, автоматизовані робочі місця ПТК та зовнішніх систем), які використовуються в рамках критичних бізнес-процесів, та ресурси забезпечення роботи інформаційних технологій (мережеве обладнання, засоби антивірусного захисту тощо).

Санкціонований об'єкт об’єкт - який контролюється Банком та/або задовольняє вимоги, які до нього висуваються.

СУІБ - система управління інформаційною безпекою - частина загальної системи управління, яка ґрунтується на підході, що враховує бізнес-ризики, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

Всі визначення термінів, що застосовані в цій Політиці, вжиті лише для зручності подання інформації та використовуються виключно для застосування та тлумачення цієї Політики.

Всі інші терміни, які вживаються в цій Політиці, застосовуються у значеннях, визначених законодавчими та нормативно-правовими актами України.

3. Ціль політики

Ціллю Політики є впровадження та ефективне функціонування системи управління інформаційною безпекою, яка буде забезпечувати безпечність та надійність функціонування бізнес-процесів, захист інформації та ресурсів Банку від зовнішніх та внутрішніх загроз та загроз, які пов’язані з навмисними та

ненавмисними діями співробітників Банку, забезпечувати 2 безперервну роботу Банку, сприяти мінімізації ризиків операційної діяльності Банку та створювати позитивну репутацію Банку при роботі з Клієнтами.

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

4. Сфера застосування

Дія Політики розповсюджується на весь Банк у цілому та використовується для всіх бізнес- процесів Банку, які можуть негативно впливати на результати діяльності Банку своєю відсутністю або функціонуванням з помилками.

5. Предмет політики та опис дій

Дана політика визначає основні принципи і заходи щодо забезпечення та розвитку інформаційної безпеки в усіх підрозділах ПАТ «ПЕРШИЙ ІНВЕСТИЦІЙНИЙ БАНК», що дозволяють гарантувати захист інформаційних ресурсів для забезпечення ефективності та безперервності бізнес-діяльності відповідно до рекомендацій серії стандартів інформаційної безпеки ISO 27000, а також відповідає вимогам законодавства України та рекомендаціям стандартів Національного банку України СОУ Н НБУ 65.1 СУІБ 1.0:2010 «Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги» (ISO/IES 27001:2005, MOD) та СОУ Н НБУ 65.1 СУІБ 2.0:2010 «Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою» (ISO/IES 27002:2005, MOD), а також міжнародних стандартів ISO/IEC 27001:2005 та ISO/IEC 27002:2005.

Основними принципами інформаційної безпеки, яких дотримується Банк, є підтримання належного захисту інформації із забезпеченням її:

- Цілісності - властивість захищеності, безпомилковості та повноти ресурсів СУІБ
- Конфіденційності - властивість інформації не ставати доступною та розкритою для несанкціонованих осіб, об'єктів або процесів.
- Доступності - властивість доступності та можливості використання ресурсів СУІБ на вимогу санкціонованого об'єкта.
- Спостережності - властивість системи (автоматизованої, контролю доступу, моніторингу тощо) фіксувати діяльність ідентифікованих користувачів і процесів. Це в першу чергу стосується інформації з обмеженим доступом, до якої відносяться відомості що становлять банківську та комерційну таємницю, персональні дані та іншу конфіденційну інформацію.

Серед основних об'єктів на які розповсюджується дія інформаційної безпеки Банку розглядаються наступні види ресурсів:

- **інформаційні ресурси** - інформація та дані у будь-якому вигляді, що отримуються, зберігаються, обробляються, передаються, оголошуються, у тому числі знання співробітників, партнерів Банку, бази даних та файли, документація, посібники користувача, навчальні матеріали, описи процедур, архівована інформація тощо;
- **програмне забезпечення** - прикладне програмне забезпечення, системне програмне забезпечення, сервісне програмне забезпечення та будь-яке інше програмне забезпечення, незалежно від форми отримання (придбання, власної розробки, таке, що вільно розповсюджується), яке використовується у Банку співробітниками та системами для роботи та взаємодії з клієнтами та іншими внутрішніми та зовнішніми системами тощо;
- **фізичні ресурси** - співробітники, апаратні засоби IT (сервери, робочі станції, міжмережеві екрани, принтери, копіювальні

апарати, телекомунікаційне обладнання, обладнання зв'язку, маршрутизатори, АТС, факси, модеми тощо), носії даних (стрічки, диски тощо), меблі, приміщення, виробниче обладнання, інші технічні засоби тощо; 3

- **сервісні ресурси** - обчислювальні та комунікаційні сервіси (Інтернет, електронна пошта, канали зв'язку тощо), інші технічні сервіси (опалення, освітлення, енергозбереження, кондиціювання повітря, системи сигналізації та моніторингу), усі послуги, пов'язані з отриманням, наданням, використанням, передачею та знищенням ресурсів, усі юридичні та фізичні особи, організації, установи та підприємства (а також їх співробітники), послугами яких користується Банк для отримання, використання, передачі та знищення ресурсів.

Для кожного ресурсу визначаються можливі ризики інформаційної безпеки та шляхи їх мінімізації, тобто Банк використовує ризик-орієнтований підхід, який забезпечує розуміння, моніторинг та зменшення ризиків операційної діяльності.

Політика базується на вимогах законодавчих, регуляторних та нормативних документів з інформаційної безпеки.

Банком використовуються наступні підходи щодо забезпечення інформаційної безпеки:

- створено та затверджено перелік відомостей, що містять інформацію з обмеженим доступом;
- створено та затверджено перелік критичних бізнес-процесів;
- встановлено правила доступу до інформаційних ресурсів та програмно-технічних комплексів;
- забезпечується контроль фізичного та логічного доступу до всіх визначених ресурсів;
- забезпечується парольний захист програмних та сервісних ресурсів;

- забезпечується антивірусний захист програмних та сервісних ресурсів;
- забезпечується захист мережі;
- забезпечується віддалений доступ до ресурсів мережі (локальної, мережі Інтернет, мереж інших організацій);
- забезпечується ідентифікація та автентифікація всіх визначених ресурсів;
- забезпечується криптографічний захист інформації.

Всі співробітники Банку обізнані та виконують вимоги інформаційної безпеки в роботі.

Під час розроблення, впровадження та функціонування програмно-технічних комплексів враховуються вимоги інформаційної безпеки.

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

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

Для зменшення ризиків виникнення інцидентів інформаційної безпеки Керівництво Банку створює співробітникам Банку умови для систематичного навчання нормам та заходам інформаційної безпеки.

У Банку складаються, діють, систематично тестуються та оновлюються плани безперебійного функціонування діяльності Банку на випадок різних непередбачуваних критичних ситуацій.

6. Ролі та відповідальність

Керівництво Банку чітко розуміє, що інформаційна безпека Банку є основою життєдіяльності Банку та сприяє (організаційно та фінансово) впровадженню, контролю та підтримці вимог прийнятої Політики.

У Банку створений та постійно працює Комітет з управління інформаційною безпекою ПАТ «ПЕРШИЙ ІНВЕСТИЦІЙНИЙ БАНК» (далі – КУІБ), рішення якого є обов’язковими для виконання усіма співробітниками Банку.

Документи системи управління інформаційною безпекою розробляються відділом інформаційної безпеки служби безпеки та іншими структурними підрозділами Банку за відповідними напрямками діяльності.

Документи системи управління інформаційною безпекою доступні співробітникам Банку у межах їх повноважень і призначені надавати допомогу у виконанні вимог інформаційної безпеки.

Постійний контроль впровадження, виконання, вдосконалення та підтримки Політики в актуальному стані покладається на відділ інформаційної безпеки служби безпеки.

Кожний співробітник Банку бере участь у підтримці відповідного рівня інформаційної безпеки Банку в межах своїх обов’язків та повноважень, несе відповідальність за їх порушення в межах, встановлених чинним законодавством України та внутрішньобанківськими нормативними документами.

7. Перегляд документу

Перегляд даної Політики повинен проводитися не рідше, ніж 1 раз на 12 місяців. Внесення змін/доповнень до Політики інформаційної безпеки здійснюється після узгодження з наступними керівниками:

• власником ресурсу/процесу;

• відповідальним за інформаційну безпеку. Внесення змін/доповнень до Політики інформаційної безпеки здійснюється відповідальною особою у наступних випадках:

• при змінах в документах, на підставі яких розроблено Політику;

• при впровадженні нових документів, що змінюють/впливають на процеси, описані в Політиці;

• при зміні ролей, відповідальності та процесів, що встановлює дана Політика;

• щорічно, за необхідності актуалізації найменувань документів, на які посилається дана Політика;

• у разі прийняття відповідного рішення колегіальним органом Банку.

Цей документ набуває чинності на наступний робочий день з дня затвердження, якщо інше не зазначено у рішенні Колегіального органу, яким документ затверджується. Зміни та доповнення до цього документу набувають чинності на наступний робочий день з дня затвердження, якщо інше не зазначено у рішенні Колегіального органу, яким документ затверджується. Усі зміни та доповнення до цього документу є його невід'ємною частиною. Дана редакція цього документу втрачає свою чинність з дати набрання чинності наступної/ нової редакції цього документу або на підставі рішення Колегіального органу.

8. Перелік взаємопов'язаних документів

Ця Політика пов'язана з наступними документами (розроблене на підставі та посилається): Стандарт організації України, Настанова: Методи захисту в банківській діяльності:

• Система управління інформаційною безпекою, СОУ Н НБУ 65.1 СУІБ 1.0:2010, Вимоги (ISO/IEC 27001:2005, MOD);

• Звід правил для управління інформаційною безпекою, СОУ Н НБУ 65.1 СУІБ 2.0:2010 (ISO/IEC 27002:2005, MOD).