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: **«СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ»**

Студент групи УБЗМ-71 Жижура Геннадій Олександрович _____
(підпис)

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

Нормоконтроль: к.в.н., доц. Якименко Юрій Михайлович _____
(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 Жижурі Геннадію Олександровичу

1. Тема роботи: «СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ 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: система забезпечення інформаційної безпеки банку.

5. Мета дослідження: надання рекомендацій щодо впровадження та функціонування системи забезпечення інформаційної безпеки банку.

6. Перелік питань, які мають бути розроблені:
1.Проаналізувати основи інформаційної безпеки.
2.Дослідити напрями забезпечення інформаційної безпеки банківської установи.
3.Надати рекомендації щодо удосконалення забезпечення інформаційної безпеки банку.

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

Науковий керівник: Мордас І. В.

Завдання прийнято до виконання: Жижура Г. О.

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

КАЛЕНДАРНИЙ ПЛАН

виконання магістерської атестаційної роботи
студентом Жижурою Геннадієм Олександровичем

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.	11.03.2020	
2.	Збір та аналіз літератури.	18.03.2020	
3.	Написання 1-го розділу роботи.	01.04.2020	
4.	Написання 2-го розділу роботи.	15.04.2020	
5.	Написання 3-го розділу роботи.	29.04.2020	
6.	Формулювання висновків за результатами проведеного дослідження.	06.05.2020	
7.	Оформлення роботи.	12.05.2020	
8.	Оформлення презентації.	14.05.2020	
9.	Отримання рецензії на роботу.	20.05.2020	
10.	Захист в ДЕК.	__.06.2020	

Студент групи УБЗМ-71 Жижура Геннадій Олександрович _____
(підпис)

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

Нормоконтроль: к.в.н., доц. Якименко Юрій Михайлович _____
(підпис)

РЕФЕРАТ

Робота містить вступ, три розділи з підрозділами, висновки та список використаних джерел. Загальний обсяг роботи – 62 сторінки.

Об’єкт дослідження – інформаційна безпека банку.

Предмет дослідження – система забезпечення інформаційної безпеки банку.

Мета дослідження – надання рекомендацій щодо впровадження та функціонування системи забезпечення інформаційної безпеки банку.

У магістерській атестаційній роботі досліджено основи інформаційної безпеки; проаналізовано особливості забезпечення інформаційної безпеки банківської установи; визначено напрями удосконалення забезпечення інформаційної безпеки банку.

ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА БАНКУ, ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ БАНКУ.

ЗМІСТ

ВСТУП

Актуальність теми. На сьогоднішній час саме інформація відіграє ключову роль в процесі подальшого розвитку цивілізацій. Особлива значущість інформації проявляє себе саме для банківської сфери, яка напряму зв'язана з її особливістю, тобто неможливістю проведення банківської діяльності саме без інформації. Варто стверджувати, що саме інформація та грошові кошти є рушієм всієї банківської діяльності. Тому ще більш важливим питанням стають проблеми захисту інформації, які є базою для проведення банківської діяльності.

Проблеми забезпечення банківської інформаційної безпеки є одними з провідних, при цьому, не треба бути навіть фахівцем, щоб зрозуміти значущість й важливість даних питань. Так як, навіть задумуючись над тим фактом, що кожен із нас має певне конкретне відношення, і не один раз у житті стикався з банківськими сегментами послуг, передусім, зацікавлений у захисті таких відомостей, та із особливою обережністю до них ставиться. Так інформаційна безпека являє собою формування інформаційних ресурсів банків та організацію їх гарантованого захисту. Цього можна досягати шляхом створення в банках систем збору й обробки інформації, здійснення відповідних заходів стосовно її розподілу та зберігання, визначення статусу та категорій банківської інформації, правил й порядку доступу до неї, додержання всіма працівниками, акціонерами та клієнтами банків правил й норм роботи із банківською інформацією, своєчасного виявлення можливих каналів й спроб витоку інформації й їхнім перетинанням.

Об'єкт дослідження – інформаційна безпека банку.

Предмет дослідження – система забезпечення інформаційної безпеки банку.

Мета дослідження – надати рекомендації щодо впровадження та функціонування системи забезпечення інформаційної безпеки банку.

Відповідно до поставленої мети передбачається вирішити наступні *завдання*:

1. Проаналізувати основи інформаційної безпеки.
2. Дослідити напрями забезпечення інформаційної безпеки банківської установи.
3. Навести рекомендації щодо удосконалення забезпечення інформаційної безпеки банку.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані наступні методи: аналізу та синтезу, систематизації, порівняння та ін.

РОЗДІЛ 1. ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Визначення інформаційної безпеки

Під ІБ (інформаційною безпекою) треба розуміти захищеність інтересів суб'єктів (учасників) інформаційних відносин. Нижче будуть описані її основні складові – доступність, цілісність, конфіденційність. Буде приведена статистика порушень ІБ, описані найбільш характерні випадки.

Але перш ніж говорити стосовно інформаційної безпеки необхідно з'ясувати, що щ таке інформація.

Термін інформація вживається сьогодні дуже різнобічно й широко. Важко знайти таку галузь знань, де б він не використовувався. Величезні інформаційні потоки захльостують людей буквально. Обсяг наукових знань, за оцінкою фахівців, наприклад, подвоюється кожні п'ять років.

Та що ж таке є інформація? В літературі дається наступне визначення:
Інформація – це дані стосовно предметів, людей, фактів, подій, процесів й явищ незалежно від їхнього форми представлення.

Відомо й те, що інформація сьогодні може мати різноманітну форму, а саме, дані, що закладені в комп'ютерах, листи, досьє, формули, пам'ятні записи, креслення, діаграми, прототипи й моделі продукції, судові документи, дисертації й ін.

Як і будь-який продукт, інформація має своїх споживачів, що її потребують, а тому володіє конкретними споживчими якостями й має також і своїх виробників або власників.

Спеціальне законодавство у галузі безпеки стосовно інформаційної діяльності представлено зараз низкою законів. В їхньому складі важливе місце займає базовий Закон «Про інформатизацію, інформацію і захист інформації», який закладає основи юридичного означення усіх найбільш важливих компонентів будь-якої інформаційної діяльності, серед яких:

- інформація й інформаційні системи;

- суб’єкти - учасники інформаційних процесів;
- правовідносини споживачів - виробників інформаційної продукції;
- власники (власники джерел) інформації - оброблювачі і споживачі на базі відносин власності при умові забезпечення гарантій інтересів держави й людей.

Спектр інтересів суб'єктів, зв'язаних з використанням інформаційних систем, можна розділити на наступні категорії показані на рис.1.1: забезпечення доступності, цілісності і конфіденційності інформаційних ресурсів та інфраструктури, що її підтримує.

Рис. 1.1 Основні складові інформаційної безпеки

Іноді в число основних складових ІБ включають захист від несанкціонованого копіювання інформації, але, на наш погляд, це дуже специфічний аспект з сумнівними шансами на успіх, тому ми не станемо його виділяти.

Пояснимо поняття доступності, цілісності і конфіденційності.

Доступність - це можливість протягом прийнятного часу одержати потрібну інформаційну послугу.

Інформаційні системи створюються для отримання певних інформаційних послуг. Якщо за тими або іншими причинам надати ці послуги користувачам стає неможливо, це, очевидно, завдає збитку всім суб'єктам інформаційних відносин. Тому, не протиставляючи доступність решті аспектів, ми виділяємо її як найважливіший елемент інформаційної безпеки.

Особливо яскраво основна роль доступності виявляється в різного роду системах управління - виробництвом, транспортом тощо. Зовні менш драматичні, але також вельми неприємні наслідки - і матеріальні, і моральні -

може мати тривала недоступність інформаційних послуг, якими користується велика кількість людей (продаж залізничних та авіаквитків, банківські послуги тощо).

Під цілісністю розуміється несуперечливість й актуальність інформації, захищеність її від несанкціонованої зміни й руйнування.

Цілісність можна поділити на статичну (тобто незмінність інформаційних об'єктів) і динамічну (що відноситься до коректного виконання складних дій (транзакцій)). Засоби контролю динамічної цілісності застосовуються, зокрема, при аналізі потоку фінансових повідомлень з метою виявлення крадіжки, переупорядковування або дублювання окремих повідомлень.

Цілісність виявляється найважливішим аспектом ІБ в тих випадках, коли інформація служить "керівництвом до дії". Рецептура ліків, наказані медичні процедури, набір і характеристики комплектуючих виробів, хід технологічного процесу - все це приклади інформації, порушення цілісності якої може опинитися в буквальному розумінні смертельним. Неприємно і спотворення офіційної інформації, будь то текст закону або сторінка Web-сервера якої-небудь урядової організації.

Конфіденційність - це захищеність інформації від несанкціонованого доступу до неї.

Конфіденційність – найбільш опрацьований у нас в країні аспект інформаційної безпеки. На жаль, практична реалізація заходів по забезпеченню конфіденційності сучасних інформаційних систем натрапляє на серйозні труднощі. По-перше, відомості про технічні канали просочування інформації є закритими, так що більшість користувачів позбавлене можливості скласти уявлення про потенційні ризики. По-друге, на шляху призначеної для користувача криптографії як основного засобу забезпечення конфіденційності стоять численні законодавчі перепони і технічні проблеми.

Якщо повернутися до аналізу інтересів різних категорій суб'єктів інформаційних відносин, то майже для всіх, хто реально використовує ІС, на першому місці стоїть доступність. Практично не поступається їй за важливістю

цілісність - який сенс в інформаційній послузі, якщо вона містить спотворені відомості?

Нарешті, конфіденційні моменти є також у багатьох організацій (навіть у згадуваних вище учбових інститутах прагнуть не розголошувати дані про екзаменаційні білети до іспиту та окремих користувачів, наприклад, паролі) [7].

1.2 Загрози інформаційній безпеці та їх класифікація

Розвиток інформаційного суспільства і, як результат, перетворення в різних сферах суспільних відносин, включаючи і економічні, призвели до появи ряду позитивних і негативних наслідків. До позитивних наслідків відносять такі: пришвидшення передачі інформації значного обсягу, прискорення її обробки та впровадження, своєрідну трансформацію інформації, яка в наш час ототожнюється з цифровим або віртуальним простором.

Б. Кормич зазначає, що основні дії щодо збирання, зберігання, передачі та розповсюдження інформації здійснюються за допомогою спеціальних технічних засобів і технологій. Відповідно з розвитком науки та техніки ці інформаційні засоби і технології перетворилися на один із найважливіших компонентів інформаційних процесів, одночасно із самою інформацією та суб'єктами інформаційних відносин . Значною мірою, розвиток вищезгаданих інформаційних засобів й технологій має одночасні негативні прояви, як то збільшення фактів протизаконного збору і використання інформації, несанкціонованого доступу до інформаційних ресурсів, незаконного копіювання інформації в електронних системах, викрадення інформації з бібліотек, архівів, банків і баз даних, порушення технологій обробки інформації, запуску програм-вірусів, знищення та модифікації даних у інформаційних системах, перехоплення інформації в технічних каналах її витоку .

У відповідності до Закону України "Про засади національної безпеки в Україні" до загроз національній українській безпеці й національним

українським інтересам у інформаційній галузі відноситься наступне: прояви обмежити свободу слова й доступ людей до інформації; поширення шляхом засобів масової інформації культів жорстокості, порнографії й насильства; комп'ютерний тероризм й комп'ютерна злочинність; розголошення інформації, що складає державну й іншу, що передбачена законодавчо, таємницю, а також інформації конфіденційного характеру, що належить державі чи спрямована на реалізацію потреб й національних українських інтересів держави й суспільства; намагання маніпуляцій суспільною свідомістю, передусім, шляхом поширення упередженої, недостовірної або неповної інформації.

Загрози можуть здійснюватися:

– технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали;

– каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

– несанкційованим доступом шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів.

Як критерій можна використати: спосіб впливу на інформацію або шляхи реалізації загроз [9].

Постанова Кабінету Міністрів України „Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" містить п. 16 Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, який визначає, що для забезпечення захисту інформації в системі створюється комплексна система захисту інформації (далі – система захисту), яка призначається для захисту інформації від:

– витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;

– несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів;

– спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування.

Як критерій можна використати: спосіб впливу на інформацію або шляхи реалізації загроз.

Державний стандарт України „Захист інформації. Технічний захист інформації. Терміни та визначення." ДСТУ 3396.2-97 містить ряд термінів пов'язаних з інформаційною безпекою та які мають пряме відношення до класифікації загроз.

Класифікація загроз відповідно має наступний вигляд: загрози витоку інформації; загрози порушення цілісності інформації; загрози блокування інформації. Загальний критерій не визначено.

1.3 Захист інформації в системі забезпечення інформаційної безпеки

Стосовно систем забезпечення української інформаційної безпеки, то засадами для функціонування й формування систем забезпечення української інформаційної безпеки є:

- діяльність й формування оптимальної структури систем інформаційної української безпеки, організація функціонування цих систем в цілому, аналіз функціонування їхніх окремих елементів;

- комплексне визначення терміну інформаційна безпека та складових її елементів, концептуальне й світоглядне закріплення у доктрині, концепції, планах, програмах й інших таких документах;

- створення ясного механізму, ціллю якого б була координація діяльності елементів систем забезпечення української інформаційної безпеки на кожному рівні державного управління;

- формування одного методологічного підходу, а також прийняття й вироблення одного цілісної й узгодженої законодавчої бази стосовно питань інформаційної української безпеки;

- забезпечення й підготовка найкращими професійними фахівцями всіх складових елементів підсистем інформаційної безпеки.

Головним завданням систем забезпечення української інформаційної безпеки є створити умови для організації здійснення управління системами інформаційної безпеки.

До головних завдань систем забезпечення української інформаційної безпеки належать:

- формування умов із метою забезпечити інформаційний суверенітет в країні;

- створення умов із метою активно залучити засоби масової інформації в боротьбу із зловживаннями службовим становищем, корупцією й іншими явищами, що мають загрозу для національної української безпеки;

- участь в удосконаленні процесу державного регулювання розвитком інформаційної галузі шляхом формування економічних й юридичних (нормативно-правових) передумов для розвитку ресурсів й інформаційної національної інфраструктури, упровадження новітніх передових технологій в цій галузі, наповнення світового й внутрішнього інформаційного простору правдивою інформацією стосовно України;

- забезпечити неухильне додержання конституційних прав громадян на доступ до інформації, свободу слова, недопущення неправомірного втручання державних органів влади (включаючи органи місцевого самоврядування), їхніх

посадових осіб в функціонування засобів масової інформації, переслідування журналістів за їхні політичні позиції й дискримінації у інформаційній галузі;

- вжиття комплексу заходів стосовно захищеності інформаційного національного простору й протистояння монополізації інформаційної галузі в Україні;

- забезпечення інформаційно-аналітичних потенціалів країни;

- забезпечення інформаційних безпек всіх складових компонентів систем державного управління;

- реалізація політики держави стосовно інформаційної безпеки;

- попередження, припинення й виявлення розвідувальної й інших видів діяльності окремих організацій чи осіб, а також спеціальних служб, що спрямовується на нанесення шкоди й збитку інформаційній українській безпеці;

- попередження, припинення й виявлення інформаційного тероризму й інших видів діяльності, що спрямовується на підривання функціонування систем державного управління;

- моніторинг (прогноз, спостереження й оцінка) стану інформаційної безпеки з причин впливу небезпек й загроз як ззовні, так і зсередини систем державного управління;

- ведення активної оперативно-розшукової, розвідувальної й контррозвідувальної діяльності із метою забезпечити інформаційну безпеку для відпрацювання оперативних, тактичних й стратегічних рішень в галузях державного управління стосовно інформаційної безпеки й вироблення механізмів їхньої реалізації;

- протистояння технічному проникненню в інформаційні системи державних органів управління із метою проведення терористично-диверсійної й розвідувальної діяльності, а також вчинення злочинів;

- забезпечення збереженості державної таємниці;

- запобігання можливій протиправній й іншій негативній діяльності суб’єктів (учасників) систем забезпечення національної української безпеки зсередини систем на шкоду їм;

- організація цивільного демократичного контролю над функціонуванням систем державних органів управління і т. ін.

До ключових функцій СЗІБ можемо віднести:

- прийняття й розроблення політичних рішень, нормативно-правових й законодавчих актів стосовно забезпечення систем управління інформаційними національними ресурсами й удосконалення механізмів стосовно реалізації юридичних норм вітчизняного законодавства;

- здійснення й визначення повноважень системами державних органів управління стосовно оперативного управління (розпорядження, користування, володіння) інформаційними державними ресурсами;

- реалізація й розроблення нормативно-методичного забезпечення й організаційних заходів регіональних й відомчих структур у галузі використання й формування інформаційних ресурсів при умові скоординованої діяльності вищезгаданих структур;

- реалізація й розроблення фінансово-економічних основ використання інформаційних ресурсів й регулювання процесів їхнього формування;

- проведення державної реєстрації інформаційного ресурсу, забезпечення цілісності й повноти створення похідних й первинних інформаційних ресурсів на базі використання інформації, яка створюється (виникає) в процесі функціонування державних органів управління;

- введення методологічно й технологічно єдиних основ формування інформаційного ресурсу за результатами функціонування державних органів управління (окрім інформаційного ресурсу, що має відомості, які відносяться до державної таємниці й до іншої інформації характеру із обмеженим доступом);

- оптимізація політики держави стосовно інформатизації щодо забезпечення виробничо-технологічних, науково-технічних й організаційно-економічних умов формування й використання інформаційних технологій й інших компонентів інформаційної інфраструктури із метою розвитку, формування й ефективного застосування інформаційних ресурсів, а також сприяння доступу

суб'єктів управління (уповноважених на це) до інформаційних світових ресурсів й інформаційних глобальних систем;

- забезпечення раціонального й ефективного застосування інформаційних ресурсів в функціонуванні державних органів управління;

- забезпечення роботи комплексних ефективно діючих систем захищеності інформаційних ресурсів систем державних органів управління;

- забезпечення застосування й розробки економічних, правових й організаційних механізмів стосовно засобів й форм обігу інформаційних українських ресурсів (ринку інформаційних технологій, інформації, засобів обробки інформаційних послуг й інформації);

- забезпечення захищеності систем державного управління від спотвореної, хибної й недостовірної інформації;

- кадрове забезпечення діяльності систем державного управління інформаційними національними ресурсами;

- правове й адміністративне забезпечення роботи систем державного управління;

- регулювання інформаційного співробітництва, що спрямоване на забезпечення взаємовигідного й рівноправного використання інформаційних національних ресурсів в процесах міжнародного обміну, проведення єдиної політики держави стосовно наукової підтримки систем державного управління розвитком, використанням й формуванням інформаційних національних ресурсів;

- інформаційно-аналітичне забезпечення процесів прийняття управлінських рішень в галузях управління інформаційним ресурсом;

- контроль над установленими правилами й порядком розвитку, формування й використання інформаційного ресурсу;

- нагляд за дотриманням законодавчих норм в сферах розвитку, формування й використання інформаційного ресурсу та проведення правосуддя в сфері інформаційних суспільних відносин.

Висновки до першого розділу

У першому розділі визначено інформаційну безпеку, проаналізовано загрози інформаційній безпеці та їх класифікацію, показано роль захисту інформації в системі забезпечення інформаційної безпеки.

РОЗДІЛ 2. ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВСЬКОЇ УСТАНОВИ

2.1 Особливості інформаційної безпеки банківської установи

Основними характеристиками інформаційної безпеки банків виступають:

– об’єктами безпеки є: інформація про персонал (керівництво, відповідальні виконавці, співробітники); інформація щодо технологій, які використовуються банком; інформаційні ресурси (інформація щодо діяльності та фінансового стану клієнта, що стала відома банку у процесі обслуговування; інформація щодо всіх операцій банку та фінансова звітність банку; конфіденційні електронні мережі банку);

– головною метою системи інформаційної безпеки є забезпечення стійкого функціонування банку і запобігання погроз його безпеці, захист від протиправних посягань, розголошення, утрати, витоку, перекручування і знищення службової інформації, порушення роботи технічних засобів, забезпечення виробничої діяльності, включаючи і засоби інформатизації;

– до основних завдань, які повинна вирішувати інформаційна безпека банку, належать: забезпечення доступу керівництва банку до конфіденційної ринкової інформації; запобігання витоку і руйнуванню конфіденційної банківської інформації; забезпечення поширення у зовнішньому середовищі вигідної для банку «конфіденційної» інформації.

Використовуючи дослідження сутності інформаційних ризиків банківської діяльності авторів роботи «Інформаційні ризики в банківській діяльності» , зосередимо увагу на визначенні поняття і специфічних рис саме цих видів ризику. Отже, основні відомості про інформаційні ризики перелічимо на рис. 2.1.

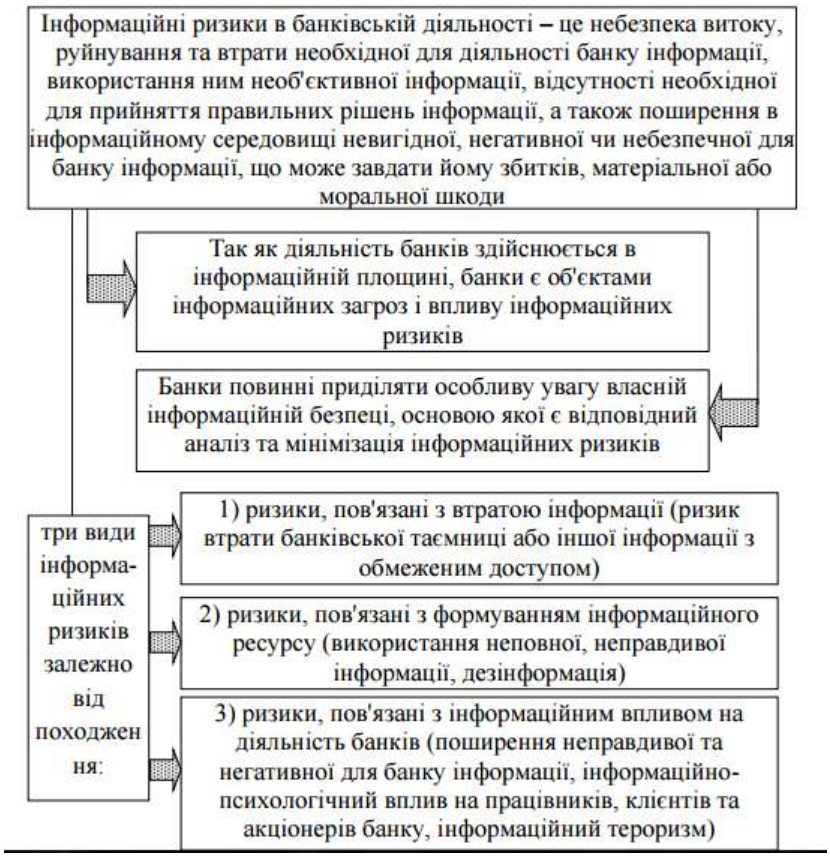

Рис. 2.1 Інформаційні ризики банківської діяльності

Забезпечити інформаційну безпеку банківських установ – це нагальна і актуальна проблема їхнього розвитку й функціонування, адже вона несе в собі потенціали ефективного використання і збереження інформаційних, фінансових й матеріальних ресурсів банків, формування умов для реалізації банками їхніх стратегічних інтересів, а також нейтралізації та своєчасного виявлення потенційних й реальних загроз.

Основними небезпеками, загрозами й ризиками інформаційній безпеці банків є:

– порушення (втрата) конфіденційності ресурсів й інформації, тобто розкриття змісту інформаційних ресурсів несанкціонованим користувачем;

– порушення (втрата) цілісності ресурсів й інформації через впливи як штучного, так і природного характеру;

– порушення (втрата) або неякісний доступ до ресурсів й інформації зі сторони користувачів, можливості доступів до інформації зловмисників;

– недостатньо неякісна спостережуваність власників або/та користувачів за ресурсами й інформацією.

Серед об’єктів інформаційної безпеки банків є:

– інформаційні ресурси (файли, банки й бази даних тощо);
– обладнання автоматизованих систем (фізичні ресурси);
– програмне забезпечення (прикладне, системне, інші допомагаючі програми);
– підтримуюча інфраструктура та сервіс (обслуговуючі засоби обчислювальної техніки, забезпечення потрібних умов експлуатації, енергопостачання і т. ін.).

Одним із важливих нормативних документів банку з інформаційної безпеки повинне бути Положення про комерційну таємницю і конфіденційну інформацію. У ньому вказують склад відомостей, що становлять комерційну таємницю та конфіденційну інформацію банку, порядок їх захисту в установах банку, хто відповідає за організацію заходів захисту, відповідальність за розголошення таких відомостей. У наказі мо-же вказуватись склад комісії, яка розглядатиме і визначатиме цінність банківської інформації, подаватиме пропозиції керівнику банку відомості щодо надання відповідній інформації статусу комерційної таємниці чи конфіденційної інформації.

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

інформації з обмеженим доступом. Окремим наказом по банку може оголошуватись список осіб, яким у повному обсязі може доводитись інформація, що становить банківську і комерційну таємницю та є конфіденційною.

Нормативна база банку з питань інформаційної безпеки є основою для правового захисту як таємниць банку, так і всієї його діяльності [13].

2.2 Принципи забезпечення інформаційної безпеки банку

В реформаторських умовах української економіки роль й значення банківських секторів в забезпеченні господарської стабілізації та безпеки країни постійно зростає.

Обов'язковою умовою функціонування й побудови банківських систем є всебічне комплексне забезпечення безпеки в усіх видах банківської діяльності, головною складовою яких є безпека економічної (господарської) інформації.

Напротязі минулих років банківські системи пережила значні зміни, що обумовлюються глобалізацією фінансових ринків, розширенням асортименту банківських продуктів й послуг, розвитком інформаційних технологій, впровадженням інноваційних технологій у процесах управління банками. У свою чергу, це ще більше загострює ситуацію стосовно забезпечення надійної захищеності інформації.

Питання, що пов'язані із захищеністю економічної (господарської) інформації банків, набувають останнім часом особливої актуальності через те, що банки є надзвичайно вразливими до таких видів загроз як наявність витоків інформації. Це все передбачає необхідність побудови відповідних систем її захищеності й викликає необхідність перегляду діючих підходів стосовно забезпечення безпеки саме інформації банків.

Проблеми безпечного функціонування держави й її банківського сектору зокрема сьогодні є предметом наукових розробок та пошуків як вітчизняних, так й іноземних практиків й теоретиків.

Під інформаційною безпекою треба розуміти захищеність інформації й підтримуючої інфраструктури від навмисних чи випадкових дій штучного чи природного характеру, що можуть нанести неприйнятний збиток суб'єктам (учасникам) інформаційних відносин, зокрема користувачам й власникам інформації й підтримуючої інфраструктури.

Безпека банків є одним із основних елементів менеджменту, що має комплексний та багатофункціональний характер.

Серед основних принципів забезпечення інформаційної безпеки систем банків є:

1. Всебічний й постійний аналіз інформаційних систем із метою виявити уразливості існуючих інформаційних активів підприємств й банків.

2.Своєчасне виявлення проблем, які потенційно здатні впливати на інформаційну безпеку підприємств й банків, корегування моделей порушника й загроз.

3.Впровадження й розробка заходів захищеності, що є адекватні характеру з'ясованих загроз, із урахуванням видатків на їхню реалізацію й сумісності таких заходів із діючими банківськими технологічними процесами. Заходи при цьому, які приймаються, щоб забезпечити інформаційну безпеку, не повинні ускладнити досягнення статутної мети підприємств й банків, а також підвищити трудомісткість технологічних процесів оброблювання інформації й створити додаткові складнощі для клієнтів.

4. Розподіл й персоніфікація відповідальності й ролей між користувачами інформаційних систем підприємств чи банків, виходячи з принципів одноосібної й персональної відповідальності за проведені операції.

5. Контроль ефективності здійснених заходів захищеності.

6. Принцип (чотирьох очей), що полягає в тому, що надкритичні дії й операції підтверджуються або здійснюються мінімум двома з уповноважених осіб.

7. Знання підприємствами або банками своїх персоналу і клієнтів.

Найбільш небезпечними загрозами стосовно інформаційної внутрішньої безпеки треба назвати:

- крадіжка обладнання;
- шахрайство;
- саботаж;
- викривлення інформації;
- втрата інформації;
- збої у інформаційних системах;
- порушення конфіденційності інформації і т. ін.

Найбільш небезпечною загрозою інформації є витік інформації й порушення її конфіденційності, оскільки банки цього побоюються з двох причин. По-перше, витік персональних даних й конфіденційної інформації банку кожен раз підриває його репутацію, оскільки в очах його клієнтів, партнерів й інвесторів банк набуває іміджу організації, що не в змозі у своїх власних стінах навести порядок. У результаті таких дій відбувається міграція клієнтів й конкурентів та відтік інвестицій. По-друге, такого роду інциденти можуть призвести чи призводять до втрати (зниження) конкурентспроможності банку, якщо база клієнтів або інтелектуальна власність, наприклад, попадуть до рук конкурентів.

Отже, наслідками витоку конфіденційної інформації в банках є втрата клієнтів, зниження конкурентоздатності, погіршення іміджу й прямі фінансові збитки банків загалом. Із проблемами витоку інформації боротись можна, але повністю перемогти її неможливо, оскільки ні технічні, ні апаратні засоби не в змозі забезпечити необхідну захищеність, бо техніка є безсилою проти витонченого людського розуму.

Однією із систем, яка забезпечує захищеність інформації є Data Loss Prevention (DLP) – це система й низка інших засобів, які захищають інформацію від витоків, контролюють або перекривають ті чи інші канали, за якими інформація може залишити інформаційні системи, такі як відчужувані носії

інформації, мережеві з'єднання за різними протоколами, принтери, мобільні комп'ютери і т.д.

У банків не завжди вистачає умінь й коштів для перекриття всіх можливих каналів. Ті носії, що залишаються без потрібного контролю, є провідниками відповідної частити випадкових витоків.

По відношенню до навмисних витоків, ситуація є значно гіршою. Знаючи, які саме канали ймовірних витоків контролюються, внутрішні зловмисники намагаються їх оминути й переслати конфіденційні дані по незахищених вільних каналах. Тому, на вірогідність навмисних витоків слабо впливає неповне перекриття параметрів інформаційних систем. Щоб ефективно протистояти як навмисним, так і випадковим витокам, система DLP (з підтримкою організаційних заходів) повинна, зрозуміло що, охоплювати усі без винятку носії (канали).

Табл.2.1.

Головні канали витоків інформації

	К-ть	%	К-ть	%
Мобільний комп'ютер	49	11,9	40	10,5
Носії інформації (CD/DVD, флешносії)	23	5,6	32	8,4
Настільний комп'ютер, сервер, НЖМД	41	9,9	90	23,6
Інтернет (вкл. e-mail)	97	23,5	82	21,4
Паперовий документ	84	20,3	78	20,4
Архівний носій	48	11,6	6	1,6
Інший	36	8,7	25	6,5
Не встановлено	35	8,5	29	7,6

Серед відмінностей, як видно із табл. 2.1, в першу чергу привертає увагу категорія "сервери й жорсткі диски, настільні комп'ютери". У цій категорії число витоків істотно зросло.

Витоки через мобільні носії й мобільні комп'ютери були надзвичайно популярні років 2-3 тому й раніше. В минулих роках кількість інцидентів із ними знизилася. У поточному році спостерігається незначне їх зростання, але

воно знаходиться у рамках статистичної похибки. Падіння кількості витоків, що пов’язані із відчужуваними носіями пояснюється, без сумніву, впровадженням засобів шифрування. При крадіжці або втраті зашифрований носій витоком не вважається. Впровадження засобів шифрування сьогодні, на жаль, уповільнилося. Вони так і не стали обов’язковими для флеш-накопичувачів, компакт-дисків й службових ноутбуків. Шифрування, на наш погляд, впровадили тільки свідомі співробітники й очолювані ними структури (підрозділи). Інші ж цією мірою захисту нехтують, оскільки не можуть наочно собі уявити наслідки витоків, та й самі витоки теж. Воно рятує повністю від негативних наслідків при втраті мобільного носія чи ноутбука. Усі знають, що наслідки ці є неприємними (особливо в Великобританії й США). Але ймовірність інцидентів є малою, і пересічні громадяни не вірять, що саме з ними це трапиться. Тому запровадити шифрування носіїв можливо лише за допомогою примусу, встановивши при цьому покарання за відсутність шифрування (усіх мобільних носіїв). Така практика поки що введена тільки у невеликій кількості банків. І держоргани в тому числі нехтують шифруванням, хоча на мобільних носіях (ноутбуках) таких організацій зберігається часто військова й державна таємниця.

Запровадження шифрування мобільних носіїв, за оцінкою аналітиків з InfoWatch, буде продовжуватися, однак дуже повільно. Вже зроблено все, що можна було добровільно запровадити. Подальше поширення шифрування можливим є лише за рахунок адміністративних ресурсів – спочатку на галузевому й корпоративному рівнях, а потім, можливо, й на державному. Проте кількість використовуваних мобільних носіїв (флеш-накопичувачів й ноутбуків) постійно зростає. Саме за рахунок цього число мобільних витоків знову може вирости.

Стосовно паперових документів, то проконтролювати їх складніше, ніж електронні. Після виходу аркушу з принтера можна стежити за ним лише в ручному режимі, за допомогою організаційних процедур й людей. Програмні й технічні методи захищеності, які є дешевшими й звичнішими, перестають

працювати. За умов відносної дороговартості робочої сили й відносного здешевшання технічних рішень не дивно, що контроль над паперовими носіями на Заході слабкіший за контроль над комп'ютерною інформацією. До того, є і багато недосконалих засобів захищеності від витоків (ми не можемо назвати їх повноцінними системами DLP), що не контролюють такі канали як відправка на друк. В таких випадках конфіденційна інформація виходить легко з-під контролю. Найбільш типові паперові витоки - це збої при автоматичному роздруковуванні листів, що адресовані великому числу клієнтів. Відомо, що адреси на конверті або на листі друкуються теж автоматично, і конверти часто заклеюються автоматично. Якщо є невелике зміщення, то і адресати на конверті (в адресах) або в листах перестають збігатися, а листи із чужими персональними даними надходять стороннім людям. Аби знизити кількість паперових витоків, необхідними є двоє заходів. По-перше, потрібна система DLP, що блокуватиме відправку на друк забороненої інформації й перевірятиме відповідність адресата й поштової адреси. По-друге, потрібний комплекс організаційних заходів стосовно обліку руху паперових документів із конфіденційною інформацією. Ці заходи є достатньо дорогими (особливо на тлі незначної вартості самих принтерів), тому кількість інцидентів із паперовими носіями буде зменшуватися дуже повільно - за рахунок, в основному, відмови від використання взагалі паперу.

Отже, основні проблеми захищеності банків від загроз зумовлюються недостатньою їхньою увагою до власної безпеки економічної (господарської) інформації. Реалізація вищеописаних заходів дозволить зменшити ризики витоків конфіденційних даних й не втратити довіри клієнтів та не стати черговим об'єктом статистики інцидентів у галузі інформаційної безпеки [14].

2.3 Формування системи інформаційної безпеки в банківському секторі України

Система інформаційної безпеки повинна забезпечити безпечність і надійність функціонування банківської системи та окремих її елементів. Тому впровадження та функціонування системи інформаційної безпеки є комплексним завданням, спрямованим на забезпечення безпеки інформаційних ресурсів, і стосується всіх банків, їхніх підрозділів і власників бізнес-процесів у банківській системі.

Загальну схему системи інформаційної безпеки відповідно до стандарту ISO/IEC 27001 подано на рис. 2.2.

Рис. 2.2. Схема системи інформаційної безпеки відповідно до стандарту ISO/IEC 27001

При формуванні системи інформаційної безпеки в банківській сфері особливу увагу потрібно приділити забезпеченню належного рівня інформаційної безпеки на рівні банків як основних елементів банківської системи. У процесі розроблення концепції управління банківською діяльністю варто виділити основні процеси функціонування банку й виключити

можливість витоку інформації, її несанкціонованого використання, нанесення збитків, упущення вигоди з боку всіх зацікавлених сторін і в напрямі досягнення основних цілей банківської діяльності. Реалізація цих положень гармонійно вписується в концепцію корпоративного управління банківською діяльністю, до якої сьогодні залучаються дедалі більше банків .

Рис. 2.3 Взаємозв'язок системи інформаційної безпеки із загальною системою корпоративного управління банком

Головним критерієм ефективності та якості інформаційної безпеки банку є стійкість його фінансового та економічного розвитку згідно з планами і завданнями незалежно від зміни ситуації. Мета безпеки досягається через виконання відповідних завдань, до яких належать такі: захист законних інтересів банку і його співробітників; профілактика і попередження правопорушень та злочинних посягань на власність і персонал банку; своєчасне виявлення реальних і потенційних загроз банку, вжиття заходів з їх нейтралізації; виявлення внутрішніх і зовнішніх причин і умов, які можуть сприяти заподіянню банку, його працівникам, клієнтам та акціонерам матеріальної, моральної та іншої шкоди, перешкоджати їх нормальній діяльності; оперативне реагування елементів структури банку на появу загрози і негативні тенденції розвитку зовнішньої і внутрішньої обстановки; виявлення і формування причин і умов, сприятливих для реалізації банком своїх основних

інтересів; виховання та навчання персоналу банку з питань безпеки; ослаблення шкідливих наслідків від акцій конкурентів або злочинців з підриву безпеки банку; збереження та ефективне використання фінансових, матеріальних та інформаційних ресурсів банку тощо.

Організація забезпечення безпеки банку здійснюється на основі принципу централізованого управління стратегічними напрямами даної діяльності на рівні керівництва банку. При цьому надійність і ефективність безпеки визначаються через реалізацію відповідних вимог.

Табл.2.2.

Вимоги до ефективності організації безпеки банківської діяльності

Неперервність безпеки	Забезпечення безпеки не може бути одноразовим актом. Це — безперервний процес, що включає обґрунтування і реалізацію найраціональніших форм, методів, способів і шляхів створення, вдосконалення та розвитку системи безпеки, безперервне управління нею, контроль за функціонуванням
Плановість безпеки	Заходи безпеки не повинні бути епізодичними або відставати від фактичних подій. Плановість передбачає рівень і характер безпеки
Конкретність безпеки	Захисту підлягають конкретні об'єкти, загроза яким може завдати шкоди банку
Активність безпеки	Постійне прагнення до виявлення загроз банку, своєчасної та ефективної їх нейтралізації
Універсальність безпеки	Заходи безпеки повинні перекривати всі можливі напрями виникнення загроз незалежно від місця їх дії
Комплексність безпеки	Для забезпечення безпеки слід застосовувати всі форми і методи захисту та протидії загрозам у повному обсязі

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. Концепція захисту банківських інформаційних систем містить низку

законодавчих ініціатив, наукових, технічних і технологічних рішень, які дозволяють забезпечити надійний рівень інформаційної безпеки .

Табл. 2.3.

Трирівнева модель проблеми захищеності банківських інформаційних систем

Система цілей	*Загальна мета:*	захист банківської інформаційної системи
	Цілі:	– безпека; – безвідмовність; – ділова взаємодія
Засоби	*Настанови:*	– захищеність; – конфіденційність; – цілісність; – готовність до роботи; – точність; – керованість; – безвідмовність; – прозорість; – зручність використання
	Підтвердження:	– внутрішня оцінка; – акредитація; – зовнішній аудит
Виконання	*Забезпечення:*	– закони, норми; – характер організації банківської діяльності; – договори, зобов'язання; – внутрішні принципи; – міжнародні стандарти банківської діяльності
	Реалізація:	– методи взаємодії із зовнішнім і внутрішнім середовищем; – методи здійснення банківських операцій; – аналіз банківських ризиків; – методи розроблення та впровадження банківських інформаційних систем; – експлуатація та супровід банківських інформаційних систем; – навчання персоналу

Засоби захисту інформації в засобах і мережах її передачі та обробки в основному передбачають використання апаратних, програмних і криптографічних засобів захисту (табл. 2.4).

Табл. 2.4.

Засоби захисту інформації

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

За критерієм призначення апаратні засоби захищеності поділяються на засоби виявлення й засоби захищеності від несанкціонованого доступу. Треба зазначити той факт, що універсального засобу, який дозволив би виконати усі функції, сьогодні немає, тому у відповідності до видів засобу несанкціонованого доступу для кожної функції існують засоби захисту й пошуку. В таких умовах заходи стосовно протистояння незаконному вилученню інформації з допомогою апаратних засобів захищеності достатньо дорогі й трудомісткі та вимагають спеціального підготування фахівців з безпеки.

В практичній роботі усі заходи із використання апаратних засобів захищеності можна розподілити на три окремі групи: технічні, організаційно-технічні й організаційні.

Технічні заходи апаратної захищеності – це ті заходи, які забезпечують застосування в процесі практичної діяльності спеціальних технічних засобів обробки й передачі конфіденційної інформації, що захищені від побічних випромінювань.

Організаційно-технічні заходи апаратної захищеності – це ті заходи, які забезпечують блокування ймовірних каналів витоків інформації шляхом технічних засобів забезпечення трудової й виробничої діяльності із застосуванням спеціальних технічних засобів, які встановлюються на окремі елементи конструкцій споруд, приміщень, будівель й технічних засобів, які потенційно створюють канали витоків інформації.

Організаційні заходи апаратної захищеності – це ті заходи, що мають обмежувальний характер, які передбачають регламентацію використання й доступу технічних засобів обробки й передачі інформації.

Під програмними засобами захищеності розуміється система спеціальних програм, що включені в склад програмного забезпечення інформаційних систем й комп’ютерів, що реалізують функцію захищеності конфіденційної інформації від програм їх обробки й неправомірних дій. Програмні засоби забезпечують захищеність інформації від копіювання інформації, її руйнування або несанкціонованого доступу до її.

При захищеності від несанкціонованого доступу із застосуванням програмних засобів здійснюється:

- розмежування доступів до інформаційних ресурсів;
- ідентифікація суб’єктів й об’єктів;
- реєстрація й контроль дій з програмами й інформацією.

Захищеність інформації від її копіювання забезпечується здійсненням таких функцій:

- аутентифікація середовища, із якого програма запущена;

- реакція на запуск із несанкціонованого (недозволеного) середовища;

- ідентифікація середовища, із якого програма буде запускатися;

- реєстрація санкціонованого копіювання;

- протистояння вивченню певних алгоритмів роботи систем.

Під криптографічними заходами захищеності розуміється застосування спеціальних програм й пристроїв, виконання відповідних дій, що створюють сигнал, що передається незрозумілим зовсім для сторонніх людей. Криптографічні заходи захищеності роблять таку захищеність інформації, при якій у разі оброблення її будь-якими способами або перехоплення вона може бути дешифрована лише протягом часу, що необхідний їй для знищення своєї цінності. Використовуються для цього різноманітні спеціальні засоби шифрування мови, телеграфних повідомлень й документів.

При формуванні моделі застосовується низка специфічних прийомів:

- аналіз – процес перерозподілу відбитої в вигляді подій, явищ, предметів інформації на складові компоненти із наступним детальним дослідженням окремих їх властивостей. При забезпеченні такого процесу провідна роль належить підсвідомості й свідомості;

- синтез – процес об’єднання групи властивостей, що притаманні відповідному об’єкту й предмету в єдине ціле, формування моделей відомих нам процесів, явищ й об’єктів (діяльності, стану) із окремих елементів, прогнозування поведінки окремих людей, прогнозування розвитку у часі;

- порівняння – процес, що забезпечує первинне оцінювання інформації на основі співставлення її елементів із вже відомими моделями й знаходження подібностей між ними;

- узагальнення – процес ідентифікації раніше невідомих нам явищ, об’єктів із відомими в певних загальних ознаках. У прийомі узагальненні міститься як небезпечний, так і корисний компоненти. Корисний – це можливість об’єднання явищ й предметів в великі групи на базі невеликих груп основних ознак. Проте при цьому постає загроза спотворити об’єктивний стан цих явищ

й предметів внаслідок надзвичайно великого зменшення кількості незначних ознак в узагальнюючій моделі;

- абстрагування – процес розгляду явища, предмета, елемента інформації з відривом від будь-якої реальності;

- виключення – процес, в якому увага звертається на відповідні аспекти власного досвіду аналітика й виключаються при цьому інші. Це дозволяє у тих ситуаціях, що часто повторюються, знаходити швидко необхідні форми реакції, увагу концентруючи на певній відповідній частині доступного досвіду. Ця властивість надає можливість виключити знаходження в свідомості зовнішніх зайвих стимулів;

- трансформація – процес перетворення інформації, що сприймається, у відповідності до моделі, що формують. Прийом трансформації лежить в основі прогнозу, фантазії, будь-якої творчої діяльності особи.

В загальному випадку із метою забезпечити інформаційну безпеку при проектуванні інформаційної інфраструктури кожного з банків й впровадженні інформаційних банківських систем повинне бути передбачене формування відповідних систем протидії й відслідковування загроз банківської діяльності (системи інформаційної безпеки). Загальну структуру систем інформаційної безпеки кожного з банків наведено на рис. 2.4.

Рис. 2.4 Система інформаційної безпеки банку

Висновки до другого розділу

У другому розділі визначено особливості інформаційної безпеки банківської установи, проаналізовано принципи забезпечення інформаційної безпеки банку, показано формування системи інформаційної безпеки в банківському секторі України.

РОЗДІЛ 3. НАПРЯМИ УДОСКОНАЛЕННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВ

3.1 Звід правил для управління інформаційною безпекою банків (ISO/IEC 27002:2005, MOD)

Даний стандарт встановлює загальні принципи й настанови стосовно започаткування, підтримки, впровадження й удосконалення управління процесом інформаційної безпеки в організаціях. Цілі, що окреслені у даному стандарті, надають ключові настанови стосовно загальноприйнятих цілей управління процесом інформаційної безпеки.

Оцінювання ризиків безпеки

Оцінювання ризиків повинно базуватися на системному підході до кількісного визначення оцінюваного ризику (аналіз ризику) й процес порівняння кількісно оцінюваних ризиків із існуючими критеріями ризиків для встановлення їхньої значущості (визначення ризиків).

Обробка ризиків безпеки

Ще до початку обробки ризиків, організації потрібно установити певні критерії стосовно прийняття ризиків. Так, можуть бути прийняті ризики, якщо, наприклад, установлено, що ризики є невеликими або вартість обробки ризиків є для організації нерентабельною. Такі рішення мають бути задокументовані.

Стосовно кожного з ризиків, що ідентифіковані після оцінювання ризиків, слід прийняти рішення стосовно обробки ризиків. Можливі варіанти обробки ризиків охоплюють:

- застосування належного контролю для зниження ризиків;
- уникнення ризиків й не дозволяючи при цьому дії, що можуть спричинити появу ризиків;
- об’єктивне й свідоме прийняття ризиків з розумінням того, що вони чітко вписуються в критерії прийняття ризиків й політику організації;

- перенесення відповідальності за пов’язані ризики на інші сторони, передусім, постачальників чи страхувальників.

Для ризиків, стосовно яких рішенням про обробку ризиків є використання належних контролів, такі контролі мають бути впроваджені й обрані таким чином, щоб відповідати вимогам, що ідентифіковані оцінюванням ризиків. Контролі мають забезпечити зниження рівня ризиків до прийнятного, беручи до уваги:

- цілі організації;
- обмеження й вимоги міжнародного й національного законодавства і нормативів;
- функціональні обмеження й вимоги;
- необхідність балансу між ймовірними витратами, до яких можуть призвести відмова політики безпеки й інвестиціями в функціонування й впровадження контролів;
- вартість функціонування й впровадження, яка пов’язана із знижуваними ризиками, й забезпечення її пропорційності обмеженням й вимогам організації.

Контролі можуть бути вибрані з даного стандарту чи із іншого набору контролів, або можуть бути спроектовані нові контролі з метою задоволення наявних потреб в організації.

Стосовно невеликих організацій, то для них неможливим може бути розподілення усіх обов’язків й необхідними можуть бути інші методи досягнення тієї ж мети контролю.

Політика інформаційної безпеки

Сам документ стосовно політик інформаційної безпеки має бути виданий, затверджений керівництвом й доведений до відома всіх найманих працівників та необхідних зовнішніх сторін.

Настанова стосовно упровадження

Документ стосовно політик інформаційної безпеки має викласти підхід організацій стосовно управління інформаційною безпекою та встановити зобов’язання керівництва.

Документ стосовно політики має містити положення щодо:

- розуміння інформаційної безпеки, її загальної мети й галузі використання, а також важливість безпеки як механізму для уможливлення поширення певної інформації (див. вступ);
- основ установлення контролів й цілей контролів, охоплюючи структуру управління ризиками й оцінювання ризиків;
- положення про наміри й підтримку керівництвом принципів й мети інформаційної безпеки у відповідності з цілями й бізнес-стратегією;
- короткого роз’яснення критично важливих для організації принципів й стандартів безпеки, політики безпеки й вимог стосовно відповідності, включаючи:
- відповідність контрактним, законодавчим й нормативним вимогам;
- управління безперервністю бізнесу;
- вимоги до навчання, поінформованості й освіти персоналу стосовно безпеки;
- визначення спеціальних й загальних відповідальностей стосовно управління процесом інформаційної безпеки, включаючи звітування стосовно інцидентів в інформаційній безпеці;
- посилання на документацію, що може підтримувати політику, зокрема, більш детальні процедури й політики для конкретних інформаційних систем чи правила безпеки, що повинні виконувати користувачі;
- наслідки порушення політик інформаційної безпеки.

Для перегляду керівництвом вхідні дані повинні містити інформацію про:

- зворотній зв’язок від зацікавлених сторін;
- результати незалежних переглядів;
- статус коригувальних й запобіжних дій;
- результати попередніх переглядів зі сторони керівництва;

- продуктивність процесів та відповідність політиці інформаційної безпеки;
- зміни, які можуть вплинути на підхід організації до управління інформаційною безпекою, охоплюючи зміни в інфраструктурі організації, бізнес - обставинах, доступності ресурсів, контрактних, нормативних і правових умовах або в технічній інфраструктурі;
- тенденції щодо загроз та вразливостей;
- зареєстровані інциденти інформаційної безпеки;
- рекомендації, надані відповідними повноважними організаціями.

Вихідні дані перегляду з боку керівництва повинні містити будь-які рішення та дії стосовно:

- вдосконалення підходу організації до управління інформаційною безпекою та її процесами;
- вдосконалення цілей контролів та контролів;
- вдосконалення розподілу ресурсів та/або відповідальностей.

Повинна підтримуватися реєстрація переглядів з боку керівництва.

Організація інформаційної безпеки

Внутрішня організація

Керівництво повинно активно підтримувати безпеку в межах організації шляхом чіткого регулювання, підтверджених зобов'язань, чітких призначень та визнання відповідальності за інформаційну безпеку.

Настанова щодо впровадження

Керівництво повинно:

- забезпечити, щоб задачі інформаційної безпеки були визначені, відповідали вимогам організації і були інтегровані у відповідні процеси;
- сформулювати, переглядати і затверджувати політику інформаційної безпеки;
- переглядати ефективність впровадження політики інформаційної безпеки;
- забезпечити чітке регулювання та явну підтримку з боку керівництва ініціативам щодо безпеки;

- надавати ресурси, потрібні для інформаційної безпеки;
- затвердити призначення певних ролей і відповідальностей стосовно інформаційної безпеки в організації;
- започаткувати плани та програми підтримки поінформованості щодо інформаційної безпеки;
- забезпечити, щоб впровадження контролів інформаційної безпеки було скоординоване у межах організації.

Керівництво повинно визначити потреби в рекомендаціях внутрішніх та зовнішніх фахівців з інформаційної безпеки і переглядати та координувати результати рекомендацій по всій організації.

Залежно від розміру організації, такі відповідальності може нести спеціальний керівний форум або існуючий керівний орган, наприклад, рада директорів.

Розподіл відповідальностей за інформаційну безпеку

Повинні бути чітко встановлені сфери відповідальності окремих осіб, зокрема, повинно мати місце наведене нижче:

- повинні бути ідентифіковані та чітко визначені активи та процедури безпеки, пов’язані з кожною окремою системою;
- повинна бути призначена особа, відповідальна за кожний актив чи процедуру безпеки і ці відповідальності повинні бути докладно задокументовані;
- повинні бути чітко визначені й задокументовані рівні авторизації.

Процес авторизації використання засобів оброблення інформації

Настанова щодо впровадження

Для процесу авторизації повинні бути розглянуті наведені нижче настанови:

- нові засоби повинні мати належну авторизацію служби управління користувачами, яка авторизує їх цілі та використання. Авторизацію треба також отримати від керівника, відповідального за підтримку інфраструктури безпеки локальної інформаційної системи для гарантії того, що виконані всі суттєві політики безпеки та вимоги;

- там, де це необхідно, повинні бути перевірені апаратні засоби та програмне забезпечення, щоб гарантувати їх сумісність з іншими компонентами системи;
- використання персональних чи приватних засобів обробки інформації, наприклад, портативних, домашніх або кишенькових пристроїв, для обробки бізнес-інформації може спричинити нові вразливості, тому повинні бути ідентифіковані й запроваджені необхідні контролі.

Угоди щодо конфіденційності

Настанова щодо впровадження

Угоди щодо конфіденційності або нерозголошення повинні ураховувати вимоги захисту конфіденційної інформації з використанням існуючих правових норм. Для ідентифікації вимог до угод щодо конфіденційності або нерозголошення треба розглянути наведені нижче елементи:

- визначення інформації, яка повинна бути захищена (наприклад, конфіденційна інформація);
- очікувана тривалість угоди, охоплюючи випадки, коли конфіденційність повинна підтримуватися необмежено;
- необхідні дії після припинення угоди;
- відповідальності та дії сторін, що підписали угоду, для запобігання неавторизованому розголошенню інформації (типу „необхідно знати”);
- право власності на інформацію, секрети виробництва та інтелектуальна власність і як вони співвідносяться з захистом конфіденційної інформації;
- дозволене використання конфіденційної інформації і права сторони, яка підписала угоду, користуватися інформацією;
- право аудиту і моніторингу діяльності, пов’язаної з конфіденційною інформацією;
- процес сповіщення та звітування щодо неавторизованого розголошення або порушень конфіденційної інформації;
- терміни повернення або руйнування інформації у разі припинення угоди;

- очікувані дії, яких треба вжити у разі порушення угоди.

Контакти з групами фахівців з певної проблематики

Повинні підтримуватись належні контакти з групами фахівців з певної проблематики або іншими форумами фахівців з безпеки чи професійними об'єднаннями.

Настанова щодо впровадження

Членство у групах фахівців з певної проблематики або форумах повинно розглядатись як засіб для:

- вдосконалення знань щодо найкращих практик та поінформованості щодо суттєвої та найсучаснішої інформації з безпеки;
- забезпечення того, що розуміння інформаційної безпеки є сучасним та повним;
- отримання ранніх попереджень із застереженнями, повідомленнями про небезпеку, та кодів оперативного виправлення (patches), які стосуються атак і вразливостей;
- одержання доступу до рекомендацій фахівців з інформаційної безпеки;
- спільного користування та обміну інформацією щодо нових технологій, продуктів, загроз або вразливостей;
- забезпечення можливість обговорення під час роботи з інцидентами інформаційної безпеки.

Для вдосконалення співпраці та координації у питаннях безпеки можуть укладатися угоди щодо спільного використання інформації. Такі угоди повинні ідентифікувати вимоги щодо захисту чутливої інформації.

Ідентифікація ризиків, пов'язаних з зовнішніми сторонами

Ризики для інформації організації та її засобів оброблення інформації бізнес-процесів, до яких залучені зовнішні сторони, повинні бути ідентифіковані і належні контролі повинні бути впроваджені до надання доступу.

Настанова щодо впровадження

Там, де необхідно дозволити зовнішній стороні доступ до засобів оброблення інформації або інформації організації, повинна виконуватися оцінка ризику для ідентифікації будь-яких вимог до певних контролів. Ідентифікація ризиків, які стосуються доступу зовнішніх сторін, повинна брати до уваги нижченаведені питання:

- засоби оброблення інформації, доступу до яких потребує зовнішня сторона;
- вид доступу, який зовнішня сторона буде мати до інформації та засобів оброблення інформації, наприклад:

1) фізичний доступ, наприклад, до офісів, комп'ютерних кімнат, картотек;

2) логічний доступ, наприклад, до баз даних, інформаційних систем організації;

3) наявність зв'язку між мережею організації та мережею(ами) зовнішньої сторони, наприклад, постійний зв'язок, віддалений доступ;

4) чи здійснюється доступ в організації чи поза її межами;

- цінність та чутливість залученої інформації та її критичність для функціонування бізнесу;
- контролі, необхідні для захисту інформації, яку не призначено для доступу зовнішніх сторін;
- персонал зовнішньої сторони, залучений до оброблення інформації організації;
- як організація чи персонал, які авторизовані на доступ, можуть бути ідентифіковані, авторизація верифікована, і як часто це потребує повторного підтвердження;
- різні засоби та контролі, які використовуються зовнішньою стороною під час зберігання, оброблення, доведення до відома, спільного використання та обміну інформації;

- вплив відсутності доступу за потребою зовнішньої сторони, і введення чи одержання зовнішньою стороною неточної або недостовірної інформації;
- практика і процедури поводження з інцидентами інформаційної безпеки та потенційними ушкодженнями, а також терміни та умови відновлення доступу зовнішньої сторони у випадку інциденту інформаційної безпеки;
- правові та нормативні вимоги, інші контрактні зобов'язання суттєві для зовнішньої сторони, які треба взяти до уваги;
- як можуть вплинути відповідні заходи на інтереси будь-яких інших зацікавлених сторін.

Врахування безпеки в угодах з третьою стороною

Угоди з третіми сторонами щодо доступу, оброблення, передавання або управління інформацією організації або засобами оброблення інформації, або щодо до додавання продуктів чи послуг до засобів оброблення інформації повинні охоплювати усі відповідні вимоги безпеки.

Настанова щодо впровадження

Угода повинна забезпечувати відсутність непорозумінь між організацією та третьою стороною. Організації повинні задовольнити свої інтереси щодо відшкодування збитків третьою стороною.

Щоб задовольнити визначені вимоги безпеки, треба розглянути внесення до угод наведених нижче умов :

- політики інформаційної безпеки;
- контролів для забезпечення захисту активів, включаючи:

1) процедури захисту активів організації, включаючи інформацію, програмне забезпечення та апаратні засоби;

2) будь-які необхідні контролі та механізми фізичного захисту;

3) контролі для забезпечення захисту від зловмисного програмного забезпечення;

4) процедури для визначення, чи мала місце якась компрометація активів, наприклад, втрата або модифікація інформації, програмного забезпечення та апаратних засобів;

5) контролі для забезпечення повернення чи знищення інформації та активів по закінченні або в погоджений момент часу протягом дії угоди;

6) конфіденційність, цілісність, доступність та будь-які інші відповідні властивості активів;

7) обмеження щодо копіювання та розголошення інформації та використання угод щодо конфіденційності;

- навчання користувача та адміністратора щодо методів, процедур та безпеки;
- забезпечення поінформованості користувача щодо проблем та відповідальностей з інформаційної безпеки;
- умов щодо переміщення персоналу, за необхідності;
- відповідальності стосовно інсталяції та підтримки апаратних засобів та програмного забезпечення;
- чіткої структури звітування та погоджених форматів звітування;
- чіткого та визначеного процесу управління змінами;
- політики контролю доступу, яка охоплює:

1) різні причини, вимоги та переваги, які роблять доступ третіх осіб необхідним;

2) дозволені методи доступу, контроль та використання унікальних ідентифікаторів, таких як ID користувача та паролі;

3) процес авторизації доступу користувача та повноважень;

4) вимогу щодо підтримки переліку осіб, яким надано право використання доступних послуг, і які права та повноваження цих осіб стосовно такого використання;

5) положення про те, що всякий нечітко авторизований доступ є забороненим;

6) процес відкликання прав доступу або переривання зв’язку між системами;

- заходів щодо звітування, сповіщення та розслідування інцидентів інформаційної безпеки та порушень безпеки, а також порушень вимог, встановлених в угоді;
- опису продукту або послуги, які повинні надаватися, та опис інформації, яка повинна бути доступною, разом з її класифікацією щодо безпеки;
- заданого рівня послуги і неприйнятні рівні послуги;
- визначення критеріїв продуктивності, які можуть бути верифіковані, їх моніторинг та звітування;
- права здійснювати моніторинг та відміняти будь-яку діяльність, яка стосується активів організації;
- права здійснювати аудит відповідальностей, визначених в угоді, мати такі аудити, які виконуються третьою стороною, та перелічувати права аудиторів, що відповідають законодавству;
- встановлення процесу ескалації для розв'язання проблеми;
- вимоги безперервності послуги, в тому числі заходи щодо доступності та надійності відповідно до бізнес-пріоритетів організації;
- відповідних зобов'язань сторін угоди;
- відповідальностей стосовно правових питань і способу забезпечення виконання правових вимог, наприклад, законодавства щодо захисту даних, особливо беручи до уваги різні національні правові системи, якщо угода охоплює співпрацю з клієнтами в інших країнах ;
- права інтелектуальної власності (IPR), визнання авторського права і захисту будь-якої спільної роботи ;
- залучення третьої сторони як субконтрактора і контролі безпеки, які ці субконтрактори повинні запровадити;
- умов перегляду/припинення угод:

1) наявність на місці плану дій в надзвичайних ситуаціях, якщо якась із сторін бажає припинити відносини до закінчення угоди;

2) перегляд угод за умови зміни вимог безпеки організації;

3) поточне документування переліків активів, ліцензій, угод або прав,

які їх стосуються.

Перегляд журналу реєстрації призводить до розуміння загроз, на які наражається система, і способу, в який вони можуть виникнути. Приклади подій, які можуть вимагати подальшого розслідування у разі інцидентів інформаційної безпеки [22].

3.2 Аудит інформаційної безпеки банку

Види аудиту

На сьогоднішній день сама класифікація таких типів аудиту, як вважають багато експертів й аналітиків, не є усталеною. Тому й розподіл на класи у ряді випадків може бути достатньо умовним. Але тим не менше аудит у інформаційній безпеці у загальному випадку можна поділити на внутрішній й зовнішній.

Зовнішній аудит, що проводиться незалежними експертами, які мають право на це, являє собою зазвичай одноразову перевірку, що може бути ініційована акціонерами, правоохоронними органами, керівництвом підприємства і т. д. Прийнято вважати, що зовнішній аудит у інформаційній безпеці є рекомендованим (а не обов'язковим) для регулярного проведення напротязі встановленого відрізку часу. Однак для деяких підприємств й організацій, у відповідності до законодавства, він є обов'язковим (наприклад, акціонерні товариства, фінансові організації й установи і т. ін).

Внутрішній аудит в інформаційній безпеці є постійним процесом, що базується на спеціальному документі «Положення стосовно внутрішнього аудиту». Що це таке? Це, по суті, атестаційні заходи, які здійснюються в організації, у терміни, що затверджені керівництвом організацій. Проведення аудиту в інформаційній безпеці забезпечує спеціальний структурний підрозділ підприємств.

Альтернативна класифікація видів аудиту

Окрім вищеописаного розподілу на класи у загальному вигляді, можна виокремити ще декілька складових, які прийняті в міжнародній класифікації. Це:

- експертна перевірка становища захищеності інформаційних систем й інформації на основі власного досвіду експертів, що її проводять;
- аналіз становища захищеності інформаційних систем із використанням технічних засобів, що спрямований на визначення потенційних уразливостей у програмно-апаратних комплексах;
- атестація заходів й систем безпеки на предмет їхньої відповідності міжнародним стандартам (ISO 17799) й державним юридичним документам, що регулюють дану сферу діяльності.

Іноді може використовуватися й так званий комплексний вид аудиту, що вміщує в собі усі вищеперераховані види. Саме він, до речі, дає, як правило, найбільш об'єктивні оцінки.

Поставлені завдання й цілі

Будь-яка перевірка (або внутрішня, або зовнішня) починається із постановки завдань й цілей. Якщо говорити простіше, треба визначити, навіщо, як і що буде перевірятися. Саме це і визначатиме подальшу методику здійснення усього процесу.

Стосовно поставлених завдань, залежно від специфіки й структури самих організацій, установ й підприємств і їхньої діяльності, то їх може бути достатньо багато. Серед всього цього, проте, можна виділити уніфіковану мету аудиту у інформаційній безпеці:

- оцінка становища захисту інформаційних систем й інформації;
- аналіз можливих ризиків, що пов'язані з загрозами проникнення у ІС ззовні, й ймовірних методів проведення такого втручання;
- аналіз відповідності рівнів безпеки інформаційних систем діючим юридичним (нормативно-правовим) актам й стандартам;
- локалізація дірок у системі безпеки;

- видача й розробка рекомендацій, що передбачають вирішення наявних проблем, а також вдосконалення наявних засобів захищеності й запровадження нових розробок.

Засоби та методика проведення аудиту

Зараз декілька слів стосовно того, як здійснюється перевірка й які етапи й засоби вона включає у себе.

Проведення аудиту в інформаційній безпеці складається з декількох головних етапів:

- ініціація процедури перевірки (підготовка аудитором плану перевірки й його узгодження із керівництвом, чітке визначення обов'язків й прав аудитора, рішення питання стосовно меж проведення дослідження, покладання на співробітників організації зобов'язань допомоги й своєчасного надання необхідної інформації);
- консолідація вихідних даних (розподіл засобів забезпечення безпеки, структура систем безпеки, рівні функціонування систем безпеки, визначення взаємодії й каналів зв'язку ІС із іншими структурами, аналіз методів надання й одержання інформації, визначення протоколів, ієрархія користувачів в комп'ютерних мережах тощо);
- проведення часткової або комплексної перевірки;
- аналіз одержаних даних (аналіз будь-яких типів ризиків й відповідність стандартам);
- надання рекомендацій стосовно усунення можливих проблем;
- формування звітної документації.

Оцінювання результатів аудиту й рекомендації стосовно усунення проблем

На базі проведеного аналізу експерти роблять висновок стосовно стану захисту й видають рекомендації стосовно усунення можливих чи наявних проблем, модернізації систем безпеки і т. д. Рекомендації при цьому повинні бути не тільки об'єктивними, але і чітко прив'язаними до реалій специфіки підприємств. Іншими словами, поради стосовно апгрейду програмного забезпечення й конфігурації комп'ютерів не приймаються. Так у рівній мірі

відноситься це й до порад стосовно звільнення ненадійних робітників, установлення нових систем для спостереження без конкретного зазначення їхнього призначення доцільності й місця установки.

Аудит інформаційної безпеки: приклад

Нарешті, розглянемо найпростіший приклад ситуації, яка вже траплялася. Багатьом, до речі, вона може здатися дуже знайомою.

Так, наприклад, якийсь співробітник компанії, що займається закупівлями в США, встановив на комп'ютер месенджер ICQ (ім'я та назва фірми не називається по зрозумілих міркувань). Переговори велися саме за допомогою цієї програми. Але «аська» є досить вразливою в плані безпеки. Сам співробітник при реєстрації номер на той момент або не мав адреси електронної пошти, або просто не захотів його давати. Замість цього він вказав щось схоже на e-mail, причому навіть з неіснуючим доменом.

Як показав аудит інформаційної безпеки, він зареєстрував точно такий же домен і створив би в ньому інший реєстраційний термінал, після чого міг відіслати повідомлення в компанію Mirabilis, яка володіє сервісом ICQ, з проханням відновлення пароля через його втрати (що і було зроблено). Оскільки сервер одержувача не був поштовим, на ньому був включений редирект – перенаправлення на існуючу пошту зловмисника.

Як результат, він отримує доступ до листування з вказаним номером ICQ і повідомляє постачальника про зміну адреси одержувача товару в певній країні. Таким чином, вантаж відправляється невідомо куди. І це найбезпечніший

приклад. Так, дрібне хуліганство. А що говорити про більш серйозних хакерів, які здатні куди більш.

Ось коротко і все, що стосується аудиту безпеки ІС. Звичайно, тут порушені далеко не всі його аспекти. Причина полягає тільки в тому, що на постановку задач та методи його проведення впливає дуже багато факторів, тому підхід у кожному конкретному випадку строго індивідуальний. До того ж методи і засоби аудиту інформаційної безпеки можуть бути різними для різних ІС. Проте, думається, загальні принципи таких перевірок для багатьох стануть зрозумілими хоча б на початковому рівні [23].

3.3 Методичні рекомендації щодо впровадження та функціонування системи забезпечення інформаційної безпеки банку та методики оцінки ризиків відповідно до стандартів НБУ

Запровадження в вітчизняних банках стандартів стосовно управління процесом інформаційної безпеки дозволить:

- оцінювати й постійно відслідковувати ризики із урахуванням мети й цілей бізнесу;
- оптимізувати вартість підтримання й побудови систем інформаційної безпеки;
- ефективно визначати найбільш критичні ризики й знижувати ймовірність їхньої реалізації;
- ефективно впроваджувати, тестувати й розробляти плани відновлення бізнесу;
- розробляти ефективну політику стосовно інформаційної безпеки й забезпечити якісне її виконання;
- забезпечувати розуміння питань стосовно інформаційної безпеки усіма працівниками банку й керівництвом;
- забезпечувати підвищення ринкової привабливості й репутації банків;
- знижувати ризики рейдерських й інших атак, що шкідливі для банку.

Класифікація інформації

В усіх банках можна виокремити наступні категорії інформації із обмеженим доступом:

- комерційна таємниця;
- банківська таємниця;
- персональні дані;
- конфіденційна інформація іншого характеру.

Аналіз ризиків

Стосовно ризику інформаційної безпеки, то ним вважається можливість того, що зазначена загроза, що впливаючи на уразливості групи ресурсів або ресурсу, може нанести шкоду банкові.

Управління процесом інформаційних ризиків повинен включати:

- ідентифікацію й аналіз ризиків;
- інформування особи, що відповідальна за прийняття рішення, й акціонерів банків стосовно ймовірностей та впливів цих ризиків (наслідки й ймовірність ризиків повинні бути зрозумілими);
- оцінювання ризиків із точки зору ймовірності їх появи й їхнього впливу на бізнес;
- установлення пріоритетів виконання певних дій стосовно зниження ризиків;
- установлення пріоритетів й порядку оброблення ризиків;
- регулярний перегляд й ефективний моніторинг процесу управління ризиками й самих ризиків;
- інформування персоналу й керівництва стосовно ризиків й дій стосовно управління ними;
- участь керівництва у процесі ухвалення рішень стосовно управління ризиками та його інформованість стосовно стану справ щодо управління ризиками.

Ідентифікація загроз й вразливостей

Потенційно загрози можуть нанести збитки ресурсам СЗІБ, а саме інформації, обладнанню, процесам, програмно-технічним комплексам, персоналу, клієнтам, бізнес-процесам (банківським продуктам) і, відповідно, й банку. Так загрози можуть мати людські й природні джерела й можуть бути випадковими або навмисними. Мають бути ідентифіковані як і навмисні, так і випадкові джерела загроз. Загрози також можуть бути ідентифіковані за типами (наприклад, фізичне пошкодження, неавторизовані дії, технічні пошкодження і т. ін.) або в загальному вигляді.

Уразливості, що можуть бути загрозами використані з метою впливу на бізнес-процеси/ресурси СЗІБ/банківські продукти, повинні бути також ретельно ідентифіковані та розглянуті.

Уразливості можуть бути ідентифіковані у таких сферах:

- банк в цілому;
- процедури й процеси;
- системи управління;
- фізичне середовище;
- персонал;
- конфігурація обладнання, програмно-технічних комплексів;
- телекомунікаційне обладнання або програмне забезпечення;
- залежність від зовнішніх організацій/установ.

Документація

У процесі підготовки до запровадження СЗІБ мають бути сформовані відповідні документи, список яких надається в додатку 5. При наявності таких документів в банках вони мають бути оновлені й переглянуті в разі потреби у відповідності з вимогами щодо оформлення документів, що наведені далі.

В загальному комплект документів, що повинен бути наявний на момент запровадження СЗІБ і що відповідає стандарту ISO 27001 як правило має чотирьохрівневу структуру, зокрема:

- адміністративні документи;
- документи нижнього рівня;

- документи середнього рівня;
- документи верхнього рівня.

Адміністративні документи

Адміністративні документи є обов'язковою начальною точкою підготовки до впровадження СЗІБ.

Ці документи включають:

- 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 СЗІБ;
- наказ про призначення керівника проекту впровадження та функціонування СЗІБ;
- положення про службу захисту інформації (підрозділ інформаційної безпеки);
- положення про службу безпеки (охорона, пропускний та внутрішньобанківський режим тощо);
- посадові інструкції відповідальних за впровадження та функціонування СЗІБ осіб;
- організаційна структура банку.

Впровадження та функціонування СЗІБ

За результатами діяльності, яка описана у попередніх розділах, створюється політика управління інформаційною безпекою, де визначаються основні види діяльності щодо впровадження та функціонування СЗІБ з посиланнями на всі документи нижчого рівня (окремі політики, процедури, методики, інструкції). У цій політиці управління інформаційною безпекою

повинні бути також визначені процедури та строки виконання специфічних для функціонування СЗІБ видів діяльності, а саме:

- моніторинг функціонування СЗІБ;
- вимірювання ефективності СЗІБ;
- внутрішній аудит СЗІБ;
- навчання та тренінг персоналу;
- управління інцидентами інформаційної безпеки;
- перегляд СЗІБ керівництвом банку;
- корегуючі та запобіжні дії.

Функціонування СЗІБ повинно постійно супроводжуватися підвищенням ефективності СЗІБ шляхом використання політики інформаційної безпеки, цілей інформаційної безпеки, результатів аудитів, аналізу подій, що підлягають моніторингу, коригувальних і запобіжних дій та перегляду з боку керівництва.

Висновки до третього розділу

У третьому розділі проаналізовано звід правил для управління інформаційною безпекою банків (ISO/IEC 27002:2005, MOD), визначено аудит інформаційної безпеки банку та надано методичні рекомендації щодо впровадження системи забезпечення інформаційної безпеки банку та методики оцінки ризиків відповідно до стандартів НБУ.

ВИСНОВКИ

Головними складовими інформаційної безпеки є: доступність, конфіденційність й цілісність. Доступність - це можливість протягом прийнятного часу одержати потрібну інформаційну послугу. Конфіденційність - це захищеність інформації від несанкціонованого доступу до неї. Під цілісністю розуміється несуперечливість й актуальність інформації, захищеність її від несанкціонованої зміни й руйнування.

У відповідності до Закону України “Про засади національної безпеки в Україні” до загроз національній українській безпеці й національним українським інтересам у інформаційній галузі відноситься наступне: прояви обмежити свободу слова й доступ людей до інформації; поширення шляхом засобів масової інформації культів жорстокості, порнографії й насильства; комп’ютерний тероризм й комп’ютерна злочинність; розголошення інформації, що складає державну й іншу, що передбачена законодавчо, таємницю, а також інформації конфіденційного характеру, що належить державі чи спрямована на реалізацію потреб й національних українських інтересів держави й суспільства; намагання маніпуляцій суспільною свідомістю, передусім, шляхом поширення упередженої, недостовірної або неповної інформації.

Стосовно систем забезпечення української інформаційної безпеки, то засадами для функціонування й формування систем забезпечення української інформаційної безпеки є:

- діяльність й формування оптимальної структури систем інформаційної української безпеки, організація функціонування цих систем в цілому, аналіз функціонування їхніх окремих елементів;
- комплексне визначення терміну інформаційна безпека та складових її елементів, концептуальне й світоглядне закріплення у доктрині, концепції, планах, програмах й інших таких документах;

- створення ясного механізму, ціллю якого б була координація діяльності елементів систем забезпечення української інформаційної безпеки на кожному рівні державного управління;

- формування одного методологічного підходу, а також прийняття й вироблення одного цілісної й узгодженої законодавчої бази стосовно питань інформаційної української безпеки;

- забезпечення й підготовка найкращими професійними фахівцями всіх складових елементів підсистем інформаційної безпеки.

Забезпечити інформаційну безпеку банківських установ – це нагальна і актуальна проблема їхнього розвитку й функціонування, адже вона несе в собі потенціали ефективного використання і збереження інформаційних, фінансових й матеріальних ресурсів банків, формування умов для реалізації банками їхніх стратегічних інтересів, а також нейтралізації та своєчасного виявлення потенційних й реальних загроз.

Основними небезпеками, загрозами й ризиками інформаційній безпеці банків є:

– порушення (втрата) конфіденційності ресурсів й інформації, тобто розкриття змісту інформаційних ресурсів несанкціонованим користувачем;

– порушення (втрата) цілісності ресурсів й інформації через впливи як штучного, так і природного характеру;

– порушення (втрата) або неякісний доступ до ресурсів й інформації зі сторони користувачів, можливості доступів до інформації зловмисників;

– недостатньо неякісна спостережуваність власників або/та користувачів за ресурсами й інформацією.

Серед об’єктів інформаційної безпеки банків є:

– інформаційні ресурси (файли, банки й бази даних тощо);

– обладнання автоматизованих систем (фізичні ресурси);

– програмне забезпечення (прикладне, системне, інші допомагаючі програми);

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

Безпека банків є одним із основних елементів менеджменту, що має комплексний та багатофункціональний характер.

Серед основних принципів забезпечення інформаційної безпеки систем банків є:

1. Всебічний й постійний аналіз інформаційних систем із метою виявити уразливості існуючих інформаційних активів підприємств й банків.

2.Своєчасне виявлення проблем, які потенційно здатні впливати на інформаційну безпеку підприємств й банків, корегування моделей порушника й загроз.

3.Впровадження й розробка заходів захищеності, що є адекватні характеру з'ясованих загроз, із урахуванням видатків на їхню реалізацію й сумісності таких заходів із діючими банківськими технологічними процесами. Заходи при цьому, які приймаються, щоб забезпечити інформаційну безпеку, не повинні ускладнити досягнення статутної мети підприємств й банків, а також підвищити трудомісткість технологічних процесів оброблювання інформації й створити додаткові складнощі для клієнтів.

4. Розподіл й персоніфікація відповідальності й ролей між користувачами інформаційних систем підприємств чи банків, виходячи з принципів одноосібної й персональної відповідальності за проведені операції.

5. Контроль ефективності здійснених заходів захищеності.

6. Принцип (чотирьох очей), що полягає в тому, що надкритичні дії й операції підтверджуються або здійснюються мінімум двома з уповноважених осіб.

7. Знання підприємствами або банками своїх персоналу і клієнтів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про інформацію» від 02.10.1992 №2657-XII.
2. Закон України «Про телекомунікації» від 18.11.2003 №1280-IV.
3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 №80\94-ВР.
4. ISO/IEC 27001:20013 [електронний ресурс]// Міжнародний стандарт з інформаційної безпеки – режим доступу : https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en
5. НБУ: СОУ Н НБУ 65.1 СУІБ 1.0:2010 «Методи захисту в банківській діяльності Система управління інформаційною безпекою. Вимоги» (ISO / IES 27001:2005, MOD).
6. Настанова з впровадження системи управління інформаційною безпекою; ISO/IEC 27005:2008. Інформаційні технології – Методика безпеки – Управління ризиками інформаційної безпеки (на основі стандарту BS 7799-3:2006); ISO/IEC 27006:2007.
7. UA-REFERAT.COM [електронний ресурс]// Основи інформаційної безпеки – режим доступу: http://ua-referat.com/%D0%9E%D1%81%D0%
8. Теоретико-методологічні засади забезпечення інформаційної безпеки людини, суспільства, держави [електронний ресурс]// Сучасні загрози інформаційній безпеці України – режим доступу: http://www.nbuv.gov.ua/old_jrn/soc_gum/iblsd/2011_2/_private/4somsou.pdf
9. Державний стандарт України [електронний ресурс] // Захист інформації. Технічний захист інформації – режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38934&cat_id=38836 .
10. Золотар О.О, Трубін І.О., Класифікація загроз інформаційної безпеки [електронний ресурс] – режим доступу : http://ndi-fp.asta.edu.ua/files/doc/publications/trubin/Zolotar_Trubin_klas_zagroz_.pdf

11. Навчальні матеріали онлайн [Електронний ресурс]// Методи забезпечення інформаційної безпеки – режим доступу: http://pidruchniki.com/16330826/politologiya/metodi_zabezpechennya_informatsiynoyi_bezpeki
12. Світлична В.Ю. Забезпечення інформаційної безпеки банківських установ / В.Ю. Світлична // Крымский экономический вестник: Научный журнал. №1 (08) лютий 2014. Частина ІІ. – Сімферополь, 2014. – С.172-175.
13. Інформаційна безпека банку [електронний ресурс]//режим доступу: http://elib.lutsk-ntu.com.ua/book/fof/bs/2011/11-15/page15.html
14. Свереда Н.І., Буковинська державна академія [електронний ресурс]// Інформаційна безпека банків в сучасних умовах – режим доступу: http://www.rusnauka.com/2_KAND_2011/Informatica/77828.doc.htm
15. Борисова А.М., Загрози інформаційній безпеці у банківських установах[електронний ресурс]// - режим доступу: http://essuir.sumdu.edu.ua/bitstream/123456789/34067/1/Borysova_banking%20establishment.pdf
16. Зубок М.І. Організаційно-правові основи безпеки банківської діяльності в Україні: навч. посіб. / М.І. Зубок, Л. . Ніколаєва. – 2-ге вид., доп. – К.: Істина, 2010. – 88 с.
17. Степаненко О.П., Формування інформаційної безпеки в банківському секторі України.
18. Ярочкин В.И. Безопасность банковских систем / В. И. Ярочкин. – М. : Ось-89, 2014. – 416 с.
19. Галузевий стандарт України // Інформаційні технології та методи захисту// Система управління інформаційною безпекою - ГСТУ СУІБ 1.0/ISO/IEC 27001:2010
20. Навчальні матеріали онлайн [Електроний ресурс] // Методи і засоби захисту в інформаційних системах – режим доступу :

http://pidruchniki.com/17680410/informatika/metodi_zasobi_zahistu_informatsiyi_informatsiynih_sistemah

21. ННІБ [Електроний ресурс] // Нормативно – Правове регулювання Захисту інформації та ISO 27 серії – режим доступу : http://izi.at.ua/publ/it_novosti/nashi_studenty/normativno_pravove_reguljuvnnja_zakhistu_informaciji_ta_iso_27_seriji/4-1-0-8
22.. Інформаційні технології . Методи захисту [електронний ресурс] // Звід правил для управління інформаційною безпекою (ISO/IEC 27002: 2005, MOD) – режим доступу : http://s-byte.com/useful/27002.pdf
23. Аудит інформаційної безпеки [електронний ресурс]// Аудит інформаційної безпеки банку – режим доступу : http://hair2014.ru/audyt-informatsijnoyi-bezpeky-tsili-metody-i-zasoby-pryklad-audyt-informatsijnoyi-bezpeky-banku/
24. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України// режим доступу : https://bank.gov.ua/doccatalog/document;jsessionid=CFBC8B2C438BD3EA2EC848B721D77179?id=72235