МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації

На рецензію	До захисту
Завідувач кафедри УІКБ	Завідувач кафедри УІКБ
Доктор економічних наук, доцент	Доктор економічних наук, доцент
_____ С.В. Легомінова	_____ С.В. Легомінова
«___»_____20__ р.	«___»_____20__ р.

ДИПЛОМНА РОБОТА
на тему:

ШЛЯХИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИСТЕМИ УПРАВЛІННЯ ЗАХИСТОМ ПЕРСОНАЛЬНИХ ДАНИХ КЛІЄНТІВ БАНКУ

СТУДЕНТ: Новоселецький Дмитро Геннадійович _____
(підпис)

КЕРІВНИК: к.т.н. Рабчун Ігор Дмитрович _____
(підпис)

НОРМКОНТРОЛЕР: _____ _____
(підпис)

Київ-2021

МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації
Кафедра Управління Інформаційною та Кібернетичною Безпекою

Освітньо-кваліфікаційний рівень – магістр
Галузь знань – «12 Інформаційні технології»
Спеціальність – «125 Кібербезпека»
Спеціалізація – «Управляння інформаційною безпекою»

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
д.е.н., доцент _____С.В.Легомінова
(підпис)
“___” _____ 20__ року

ЗАВДАННЯ

на магістерську атестаційну роботу студенту

студенту **Новоселецькому Дмитру Геннадійовичу**

1. **Тема роботи – «Шляхи підвищення ефективності системи управління захистом персональних даних клієнтів банку»,** затверджена наказом по університету від «13» жовтня 2020 р. №230

2. **Термін здачі** студентом закінченої дипломної роботи 25 грудня 2020 р.

3. **Об’єкт дослідження:** система управління захистом персональних даних клієнтів банку.

4. **Предмет дослідження:** підвищення ефективності системи управління захистом персональних даних клієнтів банку.

5. **Мета дослідження:** з’ясувати стан вітчизняного та зарубіжного законодавства у сфері захисту персональних даних, розгляд існуючої системи захисту персональних даних та внесення змін і пропозицій щодо удосконалення побудови цієї системи захисту на правовому, організаційному та технічному рівнях

6. **Перелік питань, які мають бути розроблені:**

6.1 Стан вітчизняного та зарубіжного законодавства у сфері захисту персональних даних

6.2 Розглянути існуючу систему захисту персональних даних

6.3 Розробити пропозиції щодо удосконалення системи захисту на правовому, організаційному та технічному рівнях

7. **Дата видачі завдання:** 26.10.2020

Календарний графік

№ з/п	Назва етапів магістерської атестаційної роботи	Термін виконання етапів	Відмітка про виконання
1.	Визначення об’єкту, предмету, мети та завдань дослідження	27.10.2020 р	
2.	Підбір науково-технічної літератури	29.10.2020 р	
3.	Аналіз та систематизація матеріалу. Вступ.	05.11.2020 р	
4.	Аналіз нормативних документів з питань управління захистом персональних даних клієнтів банку	13.11.2020 р	
5.	Оцінка ефективності системи управління захистом персональних даних клієнтів банку: стан та напрямки розвитку.	01.12.2020 р	
6.	Розробка та обгрунтування рекомендацій щодо підвищення підвищення ефективності системи управління захистом персональних даних клієнтів банку	15.12.2020 р	
7.	Формулювання висновків за результатами проведеного дослідження.	20.12.2020 р	
8.	Попередній захист на кафедрі	25.12.2020 р	
9.	Отримання відгука та рецензії на роботу	26.12.2020 р	
10.	Оформлення презентації	28.12.2020 р	
11.	Захист в ДЕК	20.01.2021 р	

Керівник _____ Рабчун Ігор Дмитрович
(підпис) (прізвище, ім’я, ініціали)

Завдання приймав
для виконання _____ Новоселецький Дмитро Геннадійович
(підпис) (прізвище, ім’я, ініціали)

РЕФЕРАТ

Магістерська атестаційна робота присвячена дослідженню питань захисту персональних даних клієнтів банку. Робота складається зі вступу, трьох розділів, що містять 6 рисунків, 9 таблиць, висновки та перелік посилань, що містить 41 найменування. Загальний обсяг роботи становить 100 аркушів, а також перелік умовних скорочень та список використаних джерел.

Мета магістерської атестаційної роботи полягає у з'ясуванні стану вітчизняного та зарубіжного законодавства у сфері захисту персональних даних, розгляду існуючої системи захисту персональних даних і внесення змін і пропозицій щодо удосконалення побудови цієї системи захисту на правовому, організаційному та технічному рівнях.

Обєкт дослідження – система управління захистом персональних даних клієнтів банку.

Предмет дослідження – підвищення ефективності системи управління захистом персональних даних клієнтів банку.

Методологічною базою дослідження є положення різних концепцій управління інформаційною безпекою та праці провідних вітчизняних і зарубіжних учених у забезпеченні безпеки діяльності банків.

Для цього у роботі використовуються загальнонаукові методи дослідження: статистичних порівнянь, узагальнення, статистичні методи, системний підхід.

Галузь застосування. Матеріали роботи можуть бути використані при впровадженні системи управління захистом персональних даних клієнтів банку.

Ключові слова: ПЕРСОНАЛЬНІ ДАНІ, СИСТЕМА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ, СТАНДАРТИ, БАНК, КЛІЄНТИ БАНКУ, СФЕРА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ, ІНФОРМАЦІЯ.

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ВРУ – Верховна Рада України

ДССЗЗІ – Державна служба спеціального зв’язку та захисту інформації України

ЄС – Європейський Союз

ІБ – інформаційна безпека

ІСПДн – інформаційна система персональних даних

ІС – інформаційна система

ІТС – інформаційно-телекомунікаційна система

КС – комп'ютерна система

КСЗІ –комплексна система захисту інформації

НБУ – Національний банк України

ОЕСР – Організація з економічного співробітництва і розвитку

ПДн – персональні дані

ПКЗД – пристрій криптографічного захисту даних

СБ – служба безпеки

СЗПДн – система захисту персональних даних

СУІБ – система управління інформаційною безпекою

СУПДн – система управління персональними даними

ТЗІ – технічний захист інформації

ВСТУП

В сучасних умовах інформаційного суспільства, інформація є найбільш цінним і дорогим ресурсом, а проблеми ІБ – найбільш складними і практично значущими. ІБ є однією із складових частин безпеки банку, яка формує модель захищеності підприємства.

Чільне місце в захисті приділяється підтриманню на належному рівні, оптимізації та безперервному покращенні СУПДн клієнтів банку. Банківська інформація, в тому числі ПДн клієнтів банку, є основним об'єктом оперування, тому вона вимагає належного захисту на законодавчому, технологічному та управлінському рівнях.

Будь-який український банк у своїй діяльності керується законодавчими актами України [1, 2, 6], нормативними актами НБУ, законами України, постановами Верховної Ради та Уряду України, Статутом та іншими нормативними документами банку. Особливу увагу банк повинен приділяти захисту ПДн. Для надійного захисту сьогодні вже замало витрат в сфері захисту на використання передових технологій захисту в банку. Потрібно безперервно переймати, розробляти і впроваджувати передові європейські методи і засоби захисту, котрі добре зарекомендували себе. Також це стосується законів, стандартів та нормативних актів.

Захист інформаційних ресурсів банку загалом, та ПДн зокрема, є одним з ключових завдань в умовах підвищення рівня внутрішніх і зовнішніх загроз ІБ, що можуть безпосередньо вплинути на його фінансову діяльність і стійкість на ринку. Щоб зберегти бізнес, розвиватися і бути конкурентоспроможним, підприємствам необхідно створити ефективну СУІБ.

У сучасному світі інформація стає стратегічним ресурсом, одним з основних багатств економічно розвиненої держави. Тому виникла необхідність захисту цієї інформації.

Механізм захисту ПДн клієнтів банку недостатньо досконалий і потребує суттєвого доопрацювання. Сам процес роботи банків з ПДн має бути

врегульованим не тільки шляхом прийняття відповідних процедурних документів в самому банку, але на державному рівні шляхом прийняття відповідного спільного документу НБУ та омбудсменом та ВРУ. Також вирішення даного питання по захисту ПДн обов’язково повинно включати в себе розробку відповідної політики безпеки банку щодо захисту ПДн та побудову власної системи захисту, яка буде спиратись на європейський досвід по захисту ПДн [24]. Мова йде про створення не вузькоспеціалізованої системи захисту, а цілісної СУПДн, яка могла б оперативно реагувати на випадки несанкціонованого доступу до них.

Розділ 1
НОРМАТИВНІ ДОКУМЕНТИ З ПИТАНЬ УПРАВЛІННЯ ЗАХИСТОМ ПЕРСОНАЛЬНИХ ДАНИХ КЛІЄНТІВ БАНКУ

1.1. Вітчизняні нормативно-правові документи в сфері захисту персональних даних

Побудова в Україні демократичної європейської правової держави, найвищою цінністю в якій визнається людина, її особисте життя, честь, гідність, недоторканність і безпека та підтримання ефективного функціонування державних інститутів, пов'язана із необхідністю вдосконалення захисту людини та її інтересів у сфері ПДн.

Мета захисту – припинення правопорушення та відновлення бажаних для людини, суспільства та держави прав і свобод, встановлених державним нормативно-правовим актом чи договором. Це потребує вжиття засобів державного управління, тобто застосування організаційно-правових заходів упорядкування суспільних відносин щодо реалізації задекларованих прав людини.

У XX сторіччі з виникненням комп'ютера розпочалися процеси проникнення в усі сфери діяльності людини, суспільства і держави інформаційно-комп'ютерних технологій та телекомунікаційних мереж. Ці процеси мають два аспекти.

З одного боку, нові технології та засоби комунікації дозволяють «зменшити» час та «скорочувати» відстані, отримувати економію живої та матеріалізованої праці, політичні, технологічні та інші переваги, як у плані досягнення інтересів окремої особи, так і в масштабах груп людей, країни, регіону, світової спільноти.

З іншого боку, загострюється проблема неправомірних дій різних суб'єктів, які використовують засоби Інтернет-середовища. Активність у формуванні баз даних, обробка та поширення відомостей про осіб без їх відома

призвели до виникнення глобальної за своїми масштабами у часі та просторі проблеми ІБ людини, суспільства і держави щодо захисту ПДн.

Тож виникла необхідність керування діяльності банків на державному рівні. Якщо говорити в цілому про організацію виробництва в банківській сфері, то тут існують певні особливості, котрі полягають в тому, що функції регулювання та банківського впливу у різних країнах світу виконує центральний банк держави або міністерство фінансів чи незалежне агентство. Центральний банк є основою фінансово-кредитної системи, чинним законодавством на нього покладається обов’язок стежити за станом і стабільністю фінансового сегмента економіки. В Україні відповідальність за банківський нагляд несе НБУ.

Потрібно звернути увагу на те, що право на захист ПДн у більшості розвинутих країн вже досить давно є одним з основоположних принципів правової держави. Захист ПДн трактується як невід'ємна частина права людини на захист особистого життя, закріпленого в таких актах як [12, 19].

Незважаючи на формальне закріплення певних принципів у відповідних законах, захист ПДн до недавнього часу був не чітким. В Україні набрали чинності ряд спеціальних актів, що регламентують порядок управління захистом ПДн. До цих нормативно-правових актів належать: [1, 2, 3, 4, 5, 7,8, 9, 13, 17, 18, 20].

Тепер потрібно більш детально розглянути основні закон і нормативні акти, що діють в Україні. Згідно із [20], ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особи без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Право на особисте життя та його таємницю закріплено у [7]: «Фізична особа має право на особисте життя. Фізична особа сама визначає своє особисте життя і можливість ознайомлення з ним інших осіб. Фізична особа має право на

збереження у таємниці обставин свого особистого життя. Обставини особистого життя фізичної особи можуть бути розголошені іншими особами лише за умови, що вони містять ознаки правопорушення, що підтверджено рішенням суду, а також за її згодою».

Закон України «Про захист персональних даних» визначає функціональні межі предмету правового упорядкування суспільних інформаційних відносин у зв'язку із захистом ПДн.

Розділи Закону охоплюють основні, принципово важливі напрямки діяльності щодо захисту ПДн при їх обробці, яка передбачає збирання, упорядкування, реєстрацію, накопичення, зберігання, поширення, використання, зміну, поновлення та знищення ПДн.

Необхідно навести основні терміни у сфері захисту ПДн. Відповідно до [1, ст. 2]:

База ПДн – іменована сукупність упорядкованих ПДн в електронній формі та/або у формі картотек ПДн;

Володілець ПДн – фізична або юридична особа, я, яка визначає мету обробки ПДн, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом;

Обробка ПДн – будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення ПДн, у тому числі з використанням інформаційних (автоматизованих) систем;

ПДн – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Основна мета обробки банком персональних даних - це:

надання банком фінансових послуг та провадження іншої діяльності відповідно до статуту банку та законодавства України;

виконання умов договорів, що були/будуть укладені банком, реалізації та захисту прав сторін за укладеними договорами;

забезпечення якості банківського обслуговування та безпеки в діяльності банку;

виконання вимог законодавства України, внутрішніх документів банку, колективного договору, рішень органів державної влади та органів нагляду за діяльністю банку, судових рішень, рішень органів управління банку;

з метою реалізації інших повноважень, функцій та обов'язків Банку, що не суперечать законодавству України.

Зокрема, банк здійснює обробку ПДн фізичних осіб для реалізації трудових, соціальних відносин у сфері найму, обліку та управління персоналом, адміністративно-правових відносин та виконання вимог у сфері бухгалтерського обліку, оплати праці, оподаткування, зайнятості населення та військових обов'язків, для інформування про послуги банку та його партнерів тощо.

Обробка ПДн здійснюється банком за згодою фізичних осіб, а також без такої згоди у випадках, визначених [1, ст.11].

До переліку ПДн належить:

прізвище, ім'я, по батькові; реєстраційний номер облікової картки платника податків (ідентифікаційний номер);

фактичне місце проживання та за державною реєстрацією, умови проживання;

освіта, професія, спеціальність, стаж роботи та інформація про місце роботи та посаду;

особисті відомості про вік, сімейний, родинний стан, родичів;

дані та копії документів, виданих на ім'я фізичної особи або від її імені;

фінансовий стан, доходи, види нарахувань і утримань;

адреси електронної пошти, номерів телефонів та інші електронні ідентифікаційні дані;

записи голосу, зображення (фото та відео);

кредитна історія та будь-яка інформація про стан виконання фізичною особою обов’язків за договорами, що укладені з банком, та іншими правочинами;

інформацію про дії фізичної особи та їх результати, що мали місце при виконанні укладених із банком договорів;

іншу інформацію, що стала відома банку в зв‘язку із реалізацією правовідносин із фізичною особою, при виконанні вимог законодавства України та внутрішніх документів банку.

Розглянемо галузевий стандарт [17]. Даний документ створений для надання моделі розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення СУІБ. Він містить вимоги, які відповідають чинному законодавству. Основна мета розробки цього стандарту є надання змоги банку узгодити свою СУІБ з відповідними вимогами системи управління або інтегрувати її в них.

Він наголошує, що прийняття СУІБ повинне бути стратегічним рішенням для організації. На проектування та впровадження СУІБ організації впливають потреби та цілі організації, вимоги безпеки, застосовувані процеси, розмір і структура організації. Передбачається, що впровадження СУІБ буде масштабуватися відповідно до потреб організації.

Головною перевагою цього стандарту є те, що в ньому використовується модель ПВПД «Плануй-Виконуй-Перевіряй-Дій» («PIan-Do-Check-Act», яку застосовують для структуризації всіх процесів СУІБ. Алгоритм послідовності дії цієї моделі наведений на рисунку 1.1.

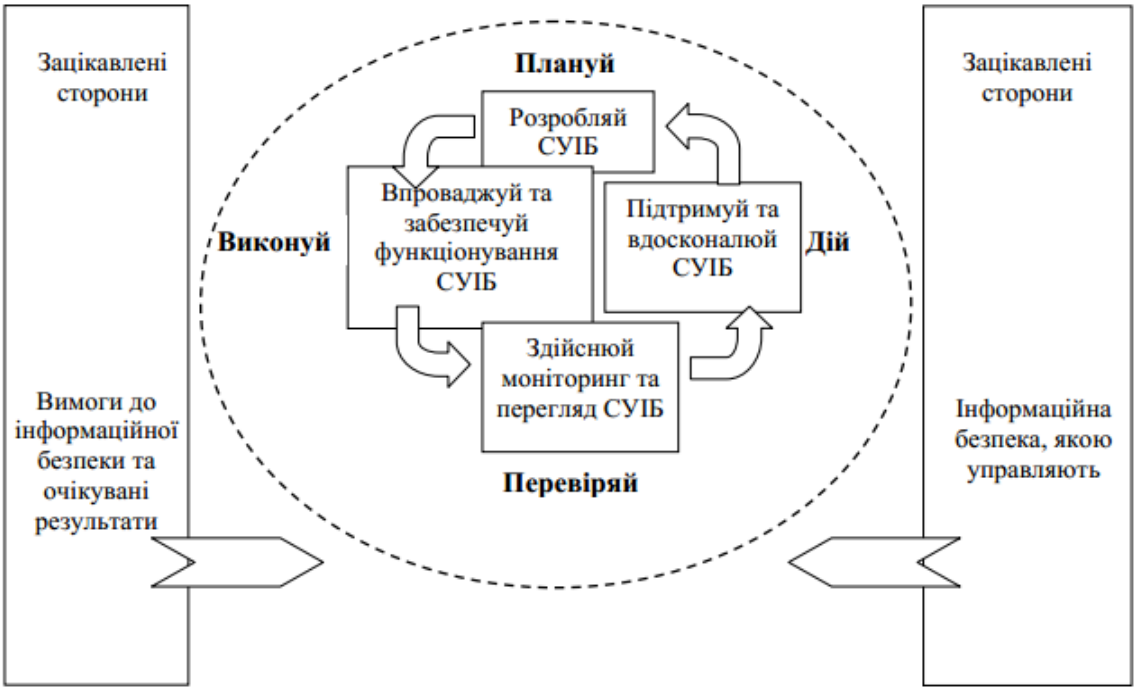

Рис. 1.1. Модель ПВПД, яка застосована до процесів СУІБ

Також в цьому стандарті на ці чотири етапи «ПВДП» існує таблиця, котра пояснює їхню функцію. Ця таблиця зображена на рис. 1.2.:

Плануй (розробляй СУІБ)	Розробити політику СУІБ, цілі, процеси та процедури, суттєві для управління ризиком та вдосконалення інформаційної безпеки для отримання результатів, які відповідають загальним політикам та цілям організації.
Виконуй (впроваджуй та забезпечуй функціонування СУІБ)	Впровадити та забезпечити функціонування політики інформаційної безпеки, заходів безпеки, процесів та процедур СУІБ.
Перевіряй (здійснюй моніторинг та перегляд СУІБ)	Оцінювати і, за можливості, вимірювати продуктивність процесів згідно з політикою, цілями СУІБ і практичним досвідом та звітувати про результати керівництву для перегляду.
Дій (підтримуй та вдосконалюй СУІБ)	Вживати коригувальні та запобіжні дії на підставі результатів внутрішнього аудиту і перегляду СУІБ з боку керівництва або іншої важливої інформації для досягнення постійного вдосконалення СУІБ.

Рис. 1.2. Етапи ПВПД та характеристика їх дій

До плюсів цього стандарту також належить те, що цей документ узгоджено із стандартами [22, 23] з метою підтримки послідовного та комплексного впровадження і функціонування разом з іншими пов’язаними стандартами управління.

Впровадження в банках України стандартів з управління інформаційною безпекою [17,18] дозволить:

знизити і оптимізувати вартість побудови та підтримки системи ІБ;

постійно відстежувати і оцінювати ризики з урахуванням специфіки банківського бізнесу;

ефективно виявляти найбільш критичні ризики і уникати їх реалізації;

забезпечити розуміння питань ІБ керівництвом банку і всіма працівниками банку;

підвищити репутацію та інвестиційну привабливість банківських установ;

забезпечити захист від рейдерських атак, НСД з ІС, витоку конфіденційної інформації що становить банківську таємницю;

підвищити захищеність клієнтів банківських установ від шахрайства.

Проблему відповідальності за порушення законодавства про захист ПДн вирішує [2], яким внесено зміни до Кодексу України про адміністративні порушення. Особливо потрібно створити відповідні умови роботи з ПДн в банку. На виконання вимог [1] та з метою недопущення правопорушень у сфері захисту ПДн на підприємстві необхідно створити СУПДн, яка об’єднає організаційні та технічні заходи щодо створення умов роботи з ПДн.

Наприклад, в будь-якому українському банку створюється КСЗІ, яка буде забезпечувати захист ПДн в інформаційній (автоматизованій) системі від незаконної обробки, а також від незаконного доступу до них здійснюється відповідно до [6], а також за допомогою інших нормативно-законодавчих документів у сфері ТЗІ. Під комплексністю захисту слід розуміти використання організаційних, правових та технічних заходів та засобів для максимального захисту інформації від внутрішніх та зовнішніх деструктивних впливів.

Контроль за додержанням законодавства про захист ПДн у межах повноважень, передбачених законодавством України, здійснюють: уповноважений ВРУ з прав людини (омбудсмен) і суди.

До основних обов’язків омбудсмена належать [1]:

розглядання скарг й пропозицій осіб;

проводення перевірки володільців ПДн;

отримання доступу до будь-якої інформації (документів) володільців або розпорядників ПДн, які необхідні для здійснення контролю;

затверджування нормативно-правові акти у сфері захисту ПДн у випадках, передбачених цим законом.

Також омбудсмен видає приписи щодо усунення чи запобігання порушенням, надає рекомендації та пропозиції, у тому числі стосовно вдосконалення законодавства, та вносить пропозицій щодо формування державної політики та її реалізації у сфері захисту ПДн, контролює за додержанням вимог законодавства про захист ПДн, здійснює міжнародно-правове співробітництво у сфері захисту ПДн.

Якщо говорити про стан вітчизняного законодавства у сфері захисту ПДн, то тут можна виділити кілька основних недоліки у цій сфері. Серед основних недоліків вітчизняного законодавства слід виокремити такі: «всеохопленість» понять ПДн та база ПДн; відсутність чіткого правового закріплення механізму взаємодії суб’єкта ПДн і володільця ПДн щодо їх використання, обробки та знищення; онбуцмен отримав досить широкі повноваження, хоча на законодавчому рівні не встановлено ні порядок проведення, ні механізм проведення перевірок; нечіткість визначення відповідальності за порушення законодавства у сфері захисту ПДн.

Також можна навести приклади типових порушень. Для законодавства у сфері захисту ПДн та ІБ характерні наступні види типових порушень:

власники баз ПДн здійснюють обробку ПДн без повідомлення уповноваженого органу з захисту прав суб'єктів ПДн;

обробка ПДн здійснюється без попередньої згоди суб’єкта ПДн;

ПДн співробітників перевірених організацій передавалися третій особі без згоди працівників і без укладання відповідного договору, який передбачає обов'язок щодо забезпечення конфіденційності та безпеки ПДн при їх обробці.

Не прийняті необхідні організаційні та технічні заходи для захисту ПДн від неправомірного або випадкового доступу до них.

До позитивних явищ належать те, що Кабінет Міністрів додатково наділив Уповноваженого ВРУ з прав людини повноваженнями здійснювати контроль за дотриманням законодавства у сфері захисту ПДн. Зокрема, онбуцмена наділили повноваженнями з проведення планових та позапланових перевірок власників та розпорядників баз ПДн; направлення подання для вживання ними заходів щодо усунення виявлених порушень законодавства; надання рекомендації у сфері захисту ПДн. Щороку Уповноважений ВРУ з прав людини готуватиме та оприлюднюватиме щорічну доповідь про стан дотримання законодавства про захист ПДн у державі. Також в Україні розроблені і використовуються галузеві стандарти НБУ, які основуються на таких міжнародних стандартах як [21-23].

1.2. Зарубіжні нормативно-правові документи в сфері захисту персональних даних

Закони про захист ПДн в європейських країнах почали приймати у 1970-х роках. Головною передумовою їх появи було виникнення автоматизованих баз даних, розвиток телекомунікацій та потреба у забезпеченні приватного життя людини відповідно до принципів [19].

Більшість зарубіжних законів у сфері захисту ПДн мають типову назву закон про захист даних. Під захистом даних розуміють будь-які правові, організаційні, технічні (технологічні, криптографічні, програмні) засоби щодо захисту інформації персонального змісту. Для комплексного захисту даних на міжнародному рівні використовується термін «безпека даних».

Історично відомими є дотримання двох принципів при укладанні національних правових систем захисту ПДн, які передбачають:

створення всеохоплюючого закону про захист приватного життя, який спрямований на упорядкування суспільних інформаційних відносин, пов'язаних з визначеними даними. Цей підхід веде до необхідності коригування положень закону при появі нових загроз;

створення спеціальних законів для кожного типу зазіхань на приватне життя або для кожної сфери, яка є потенційним джерелом загрози та порушень (наприклад, для засобів масової інформації, банків, телекомунікацій та ін.). У даному випадку, при виникненні нових загроз, такий підхід призводить до безсистемності, дублювання та суперечливості окремих норм права.

У практичному застосуванні обидва підходи виявили свою низку ефективність.

На даний час набутий досвід враховується законодавцями і при створенні національних правових систем застосовують змішаний підхід, який полягає у створенні базового закону про захист ПДн, а вже на його основі розробляються галузеві нормативно-правові акти. При виникненні нових загроз та видів порушень прав особи на її ПДн система захисту залишається незмінною, а до галузевої нормативно-правової бази вносяться необхідні доповнення та зміни.

При цьому, створення зазначених національних базових законів обов'язково ґрунтується на принципах захисту ПДн, що були розроблені різними міжнародними організаціями, які представляють політико-економічні союзи та співтовариства держав, зокрема, Організацію з економічного співробітництва і розвитку, Раду Європи, Євросоюз, Організацію американських держав, країни Шенгенської угоди, Міжнародну торговельну палату.

У середині 1970-х рр. стало зрозумілим, що національні системи правового захисту даних, з причин наявних особливостей національного менталітету і розходжень законодавчих систем (як за формою, так і за змістом), не можуть забезпечити принцип екстериторіальності ПДн. Це стримувало

вирішення багатьох питань розвитку міжнародного співробітництва. Саме тому потреба в створенні міжнародної системи правового регулювання обробки і передачі даних ставала всі більш нагальною.

Для вирішення проблеми у 1978 р. в Організації з економічного співробітництва і розвитку була заснована експертна група, із завданням розробити набір базових принципів захисту приватного життя і індивідуальних свобод (тобто – «прайвеси») у зв'язку з обробкою ПДн і в зв'язку з транскордонними потоками даних. Прайвеси - (англ. privacy - таємниця, усамітнення, приватне життя) - особлива правова категорія в англо-американській правовій системі, що означає таємницю і недоторканність приватного життя, інтимну сферу людини. Термін «privacy» не має аналогів в українській мові. Він може означати в одних випадках приватне життя, в інших - право на приватне життя, в третіх - право на захист недоторканності приватного життя і т.д. Ці принципи повинні були послужити підґрунтям для гармонізації відповідних національних законів.

Розробка таких принципів і досягнення консенсусу держав-членів ОЕСР виявилася непростою задачею, оскільки досить неоднорідний її склад визначив не менш неоднорідний набір національних підходів до правового захисту ПДн. Так, наприклад, деякі національні закони захищали дані стосовно тільки фізичних осіб. Інші країни – вважали необхідним захищати юридичних осіб також, як і фізичних. Треті країни дотримувалися захисту ПДн, які обробляються тільки автоматично, у той час як інші поширювали його також на ручні і друковані дані. Частина країн вважала за необхідне забезпечити захист «прайвесів» взагалі і ПДн, зокрема. Серед держав-членів ОЕСР були прихильники всіх трьох можливих підходів до побудови системи правового захисту ПДн: генерального, секторного (галузевого) і змішаного.

Генеральний полягає у прагненні до створення єдиного і всеосяжного закону про захист сфери приватного життя і був пов'язаний зі спробами теоретичного обґрунтування загального і абсолютного права на невтручання в приватне життя.

Він складається з таких основних елементів:

принцип достовірності ПДн;

права суб'єкта даних у зв'язку з обробкою і використанням даних про нього;

встановлені законом правила доступу до чужих ПДн, їх розкриття та передачі;

вилучення з правового регулювання даних в інтересах державної та громадської безпеки, у зв'язку з розслідуванням злочинів;

встановлені законом заходи правового регулювання збору, зберігання, обробки, передачі та використання ПДн, наприклад ліцензування передачі ПДн за межі національної території;

вимоги до організаційно-технічних заходів щодо забезпечення безпеки даних при їх зборі, обробці, використанні, передачі і збереженні ;

статті, які встановлюють покарання за порушення принципів захисту даних та інших положень закону про захист даних.

Також необхідно зазначити, що в деяких національних системах захисту даних системоутворююче законодавче ядро складається не з одного, а з двох взаємодоповнюючих законів - закону типу Data Protection Act (Закон про захист даних) і закону типу Information Freedom Act (Закон про свободу інформації), які нерідко навіть розробляються та приймаються одночасно. В інших системах принцип свободи доступу до інформації безпосередньо закладається в положеннях закону типу Data Protection Act.

Секторний (або галузевої) - полягає у створенні спеціалізованих законів для кожного типу посягань на сферу приватного життя, або для кожної галузі або сектора людської діяльності, що є потенційним джерелом загроз для права людини на невтручання в його приватне життя (наприклад, для пошти та засобів зв'язку, для бюро кредитної інформації , для засобів масової інформації та рекламної сфери, для приватних детективів, для комп'ютерних банків даних).

Галузеві закони рідко розробляються спеціально для конкретного виду загроз сфері приватного життя. Найчастіше відбувається так, що додаткові

положення про захист ПДн включаються у вже існуючі або розроблювані закони, що регламентують всі аспекти діяльності в тій чи іншій галузі по мірі накопичення прецедентної бази посягань на права суб'єктів ПДн в конкретній галузі.

Варто відзначити, що основна гідність такого нежорсткій ієрархічної системи «базовий закон - галузеві закони» складається по суті в тому, що при появі нових видів неправомірних посягань на ПДн немає необхідності переробляти всю систему захисту. Досить внести зміну до відповідного галузевого закон або доповнити його новим галузевим законоположенням.

Як вже зазначалося вище у чистому вигляді і той, і інший підходи виявилися непродуктивними. Секторний (галузевий) підхід, при якому нові галузеві закони приймалися в міру накопичення прецедентної бази, що вказувала на нове джерело загроз для сфери приватного життя, приводив до безсистемності, дублювання і суперечливості законоположень. Прикладом може слугувати законодавство США в галузі захисту права громадян на недоторканність приватного життя. Застосування генерального підходу призвело до створення «всеосяжних і громіздких» законів про захист сфери приватного життя, які застарівали при появі кожного нового типу загроз для права на невтручання в приватне життя.

Отож, цей досвід був врахований при створенні національних СЗПДн. У переважній більшості країн сучасні національні системи правового регулювання обробки та використання ПДн застосовують так званий змішаний принцип, який об'єднує певні аспекти генерального і галузевого підходів. Національне законодавство у сфері захисту даних, як правило, складається:

з базового або, як їх ще називають, системоутворюючого закону типу Data Protection Act (генеральний підхід);

комплексу секторних (галузевих) законів, що забезпечують захист ПДн в галузях людської діяльності, які створюють потенційну загрозу для права суб'єкта ПДн на невтручання в його приватне життя.

Активним регулюючим компонентом сучасних систем захисту ПДн визначений національний орган (або система органів) щодо захисту даних. І останнім компонентом таких систем будуть нестатутні (корпоративні) засоби захисту, котрі ще часто називаються «засобами саморегулювання».

Повертаючись до експертної групи, потрібно сказати, що за підсумками дворічної роботи, включаючи процес узгодження принципів із усіма державами-членами, Рада ОЕСР прийняла Настанови «Про базові принципи захисту недоторканності приватного життя і транскордонних потоків ПДн». Вони складаються з п'яти частин:

перша – визначає сферу дії базових принципів;

друга – встановлює вісім базових принципів захисту «прайвесів» у зв'язку з обробкою

ПДн на національному рівні;

третя – присвячена принципам міжнародного застосування, тобто взаємодії між державами-членами ОЕСР;

четверта – визначає заходи для здійснення на практиці вищезгаданих принципів і, зокрема, встановлює, що вони повинні застосовуватися в «недискримінаційній манері»;

п'ята – присвячена організації співробітництва держав-членів ОЕСР (за допомогою обміну інформації і запобігання несумісних національних процедур для захисту ПДн).

Положення базових принципів розроблені з метою:

досягнення державами-членами ОЕСР мінімальних стандартів захисту «прайвесів» у зв'язку з обробкою ПДн;

зменшення нормативно-правових розходжень між відповідними нормами національного законодавства різних країн;

гарантії того, що при захисті ПДн на національному рівні будуть прийматися до уваги інтереси інших країн, зокрема, не допускатися неналежне втручання при передачі ПДн між країнами;

усунення причин, що могли б спонукати країни обмежити або заборонити транскордонні потоки ПДн через можливі ризики, асоційовані з такими потоками.

Як встановлено в преамбулі Настанов Ради ОЕСР, предметом турботи є дотримання двох важливих положень демократичного світу: захист приватного життя і індивідуальних свобод, з одного боку, і сприяння розвитку вільних потоків ПДн, з іншого боку. Приймаючи певні обмеження для вільних транскордонних потоків ПДн, ОЕСР вважає необхідним все ж зменшити необхідність у таких обмеженнях.

До основних принципів захисту недоторканності приватного життя і міжнародного обміну ПДн Рада ОЕСР відносить:

обмеження обсягу ПДн, що збираються;

якість ПДн;

конкретизації цілей збору ПДн;

обмеження на використання ПДн;

забезпечення безпеки ПДн;

відкритість політики і практики по відношенню до ПДн;

індивідуальна участь (права індивідуума на свої ПДн);

відповідальності (обов'язок розпорядника ПДн).

Дотримання принципів на національному рівні передбачає наступні обов'язки для держав-членів ОЕСР, якими передбачено:

прийняти належні національні закони;

заохочувати і підтримувати саморегулювання шляхом прийняття кодексів поведінки/поводження або інших правил;

забезпечити наявність розумних механізмів реалізації індивідуальних прав;

застосувати необхідні санкції й інші засоби захисту ПДн на випадок не виконання заходів, що передбачені зазначеними принципами;

забезпечити недискримінаційне ставлення до суб'єктів даних.

Стосовно обміну ПДн і законним його обмеженням державами-членами ОЕСР передбачено:

враховувати можливі наслідки, – використання ПДн в межах країни і їх реекспорт можуть мати певні наслідки й для інших країн;

приймати розумні і належні заходи для забезпечення того, щоб міжнародний обмін ПДн, у тому числі їх транзит через територію кожної держави-члена ОЕСР, був безперервним і безпечним;

утримуватися від запровадження обмежень на обмін ПДн в межах країни й з іншою державою-членом ОЕСР, за винятком випадків, коли остання ще не почала дотримуватися базових принципів, а також під загрозою того, що реекспорт таких даних може привести до порушення діючих у першій країні внутрішніх законів про недоторканність приватного життя.

Держава-член ОЕСР може також вводити обмеження стосовно тих категорій ПДн, відносно яких її внутрішніми законами про недоторканність приватного життя передбачені конкретні правила, у зв'язку з характером таких даних, у випадку якщо інша держава-член ОЕСР не забезпечує їх еквівалентного захисту.

Проблема корпоративного «прайвесу» відповідно до базових принципів стосовно даних зводилася до питання: чи поширювати задекларовані принципи захисту ПДн на інформацію, що стосується юридичних осіб. Підсумковий текст базових принципів ОЕСР відображає ту точку зору, що недоторканість особи є, в багатьох аспектах, особливою приватною сферою індивідуума, яка не повинна трактуватися таким чином, як і недоторканість будь-якої групи фізичних осіб або корпоративної безпеки чи конфіденційності. Потреби у захисті вказаних категорій зовсім різні.

Деякі члени експертної групи вважали, що повинна бути передбачена можливість поширення базових принципів і на юридичних осіб (корпорації, асоціації і т.п.). Однак ця пропозиція не знайшла консенсусу. Тому сфера дії базових принципів обмежена даними, які стосуються індивідуумів, а на відповідну частину держав-членів ОЕСР залишена завдання прийняття рішення

щодо їх власної політики стосовно «приватної сфери» діяльності корпорацій, груп, партій і інших подібних організацій.

Що стосується другої проблеми, те експертна група вважає, що обмеження базових принципів тільки сферою автоматизованої обробки ПДн було б істотним недоліком цієї ініціативи ОЕСР. Слід почати хоча б з того, що в термінах визначень дуже важко провести розмежування між автоматизованою і неавтоматизованою обробкою ПДн.

Існують «змішані» системи обробки ПДн і існують такі стадії в обробці даних, що можуть привести до автоматизованої їх обробки, а можуть і не привести. І ці труднощі мають тенденцію до подальшого ускладнення завдяки розвитку технологій.

Із європейських законів слід виокремити найважливіші, зокрема такий як [8, 9].

В кінці 70-х роках XX століття суперечність між активним впровадженням засобів автоматизованої обробки даних та їх поширенням у телекомунікаційних мережах, зловживання при використанні ПДн, потреба у впорядкуванні експортно-імпортних операцій призвели до необхідності розробки міжнародно-правового акту, який мав забезпечити упорядкування суспільних інформаційних відносин у сфері захисту ПДн. Комітетом Ради Європи з питань захисту даних були сформульовані принципи захисту від неправомірного збирання, обробки, зберігання та поширення ПДн. Ці принципи 28 січня 1981 року отримали закріплення у першій і єдиній на сьогодні міжнародній угоді – [8] (відома як Конвенція № 108 згідно порядку у серії Європейських договорів). З того часу захист ПДн виокремився у самостійний вид діяльності.

Згідно з [8] держави, які підписали цей документ, зобов'язуються керуватися її положеннями при розгляді питань, пов'язаних із захистом ПДн, що підлягають чи не підлягають автоматизованій обробці, як у суспільному, так і приватному секторах. Держава-член Конвенції № 108 Ради Європи має право визначати види ПДн, які підлягають захисту (стаття 3 Конвенції).

Кожна держава-член [8] коригує національне законодавство у частині втілення її основних принципів та поставленої мети забезпечення на території держави-члена поваги до прав та основних свобод кожної особи незалежно від її громадянства або місця проживання (стаття 4).

До захисту ПДн висуваються певні вимоги. Їх отримання та обробка мають здійснюватися законним шляхом. Вони повинні зберігатися та використовуватися у визначених та законних цілях, бути точними та поновлюваними, допускати ідентифікацію фізичної особи.

ПДн, що свідчать про расову приналежність, політичні, релігійні чи інші переконання, а також дані, що стосуються здоров'я або статевого життя, не можуть піддаватися автоматизованій обробці, якщо внутрішнє законодавство країни не забезпечує відповідних гарантій. Це правило застосовується також до ПДн, що стосуються засудження у кримінальному порядку. Засоби та заходи, що застосовують до таких даних, повинні передбачати безпеку ПДн від випадкового та несанкціонованого доступу, знищення, модифікації, блокування, розповсюдження та випадкової втрати (статті 5 – 7).

Виходячи з інтересів держави [8] допускає обмеження у правах фізичних осіб, якщо це стосується державної чи суспільної безпеки, фінансової стабільності, боротьби зі злочинністю, захисту прав та основних свобод інших осіб (стаття 9).

Транскордонні потоки даних мають здійснюватися за умов забезпечення захисту ПДн. Допускається обмеження цієї вимоги у разі, коли національне законодавство передбачає особливий порядок упорядкування суспільних інформаційних відносин та визначення окремих видів ПДн у зв'язку із специфічністю деяких відомостей, крім випадків, коли законодавство іншої держави-члена має аналогічний ступінь захисту (стаття 12).

Для захисту ПДн [8] зобов'язує кожну державу-члена призначити один або більше Уповноважених органів нагляду та направити відповідне повідомлення Генеральному секретарю Ради Європи. Завдання інституту

Уповноваженого передбачають створення належного організаційно-правового регулювання діяльності щодо захисту ПДн у країні (стаття 13).

Десятиріччя, що минули з часу прийняття [8] показали, що інститут Уповноваженого із питань захисту ПДн не лише зберігся, а й дістав поширення у всіх західноєвропейських країнах. Нині Уповноважені органи із питань захисту ПДн діють більше ніж у двадцяти країнах Європи. Їх діяльність свідчить, що вони є ефективним засобом, здатним забезпечити баланс інтересів людини, суспільства і держави.

Також хотіла звернути особливу увагу на новий закон - британський стандарт [24], який став першим у світі стандартом для СУПДн. Оскільки питання захисту ПДн є досить актуальним у всьому світі, в ньому описано СУПДн і визначаються дії відносно ПДн. Тобто ПДн повинні:

оброблятися чесно і законно;

бути не надлишковими і відповідати цілям;

бути точними і своєчасно оновлюватись;

повинна забезпечуватися відповідна безпека;

не повинні передаватися за межі ЄС без адекватного захисту.

Основним недоліком цього стандарту є те, що він не передбачає процедуру оцінки застосування вимог на основі аналізу ризиків, і тому його вимоги є жорстко регламентовані. До плюсів належить те, що цей стандарт може використовуватися організаціями будь-яких розмірів, сфери діяльності та форми власності для створення системи управління (менеджменту), котра включає в себе процедури в таких областях як навчання та підвищення обізнаності, оцінка ризику, спільне використання даних, збереження і знищення даних, мінімізує розкриття даних третіми сторонами.

Вкінці потрібно зазначити, що економічний аспект ПДн проступає в тому, що зі становленням і функціонуванням внутрішнього ринку, який передбачає рух інформаційних ресурсів щодо товарів, капіталів і послуг, виникає необхідність руху ПДн за допомогою інформаційно-комп'ютерних технологій та телекомунікаційних мереж та необхідність у захисті їх споживчої і мінової

вартості і, тим самим, у захисті прав людини та свобод щодо її економічних інтересів. Інформація в усьому світі визнається товаром. Ринкові відносини передбачають не безоплатну передачу інформації-товару, а взаємовигідний економічний обмін в умовах вільної конкуренції. Конкретні ПДн ототожнюють відповідну інформацію, яка може складати економічний інтерес і може бути товаром, хочемо ми того чи ні, наприклад, якщо вкладена праця по акумулюванню відомостей у базах даних чи картотеках, або вкладена творча праця щодо розміщення ПДн на інтернет-сайті. Але цей товар не має юридичного визнання щодо права власності на майно і не підпадає під дію норм інституту інтелектуальної власності тому, що ПДн не є річчю і не є результатом творчості. Зважаючи на те, що інтереси будь-яких суб'єктів і конкретної людини можуть не збігатися, а її ПДн можуть використовуватися для задоволення потреб економічної, фінансової, комерційної тощо діяльності, то ПДн повинні мати організаційні, технологічні і правові засоби захисту від несанкціонованого їх використання. Це все більш стає зрозумілим за умов розвитку зовнішньоекономічних зв'язків, економічної інтеграції, розширення і поглиблення процесів інформатизації, розвитку телекомунікаційних мереж, зростання активності при формуванні різних банків інформаційних ресурсів і баз ПДн (політичних, економічних, технологічних, екологічних, медичних, освітянських, культурних, інформаційних, виробничих, правоохоронних і ін.).

Ці процеси випливають із функціонування внутрішнього ринку, а також зростання транскордонних інформаційних потоків між суб'єктами економічної, політичної, правової та ін. діяльності різних держав.

Зазначені тенденції дозволяють зробити важливі попередні висновки.

Перший: фізична особа об'єктивно має право на свої ПДн, що має природно-конституційний зміст і повинно бути закріплено юридично.

Другий: в умовах активного розвитку процесів інформатизації, захист ПДн може і повинен бути забезпечений уже не тільки засобами організаційного і техніко-технологічного змісту, але і правовими засобами.

Висновки до розділу 1

Розглянувши нормативні документи з питань управління захистом ПДн клієнтів банку можна зробити наступні висновки. Нові інформаційні технології, органічно вбудовуючись в ІС економічних об'єктів і підвищуючи ефективність і якість їх роботи, однак породили проблеми забезпечення ІБ. Виникли мало вивчені інформаційні загрози, реалізація яких може призводити до непередбачуваних і навіть катастрофічних наслідків, зводячи нанівець всі зусилля з підвищення ефективності управління економічним об'єктом. Щорічний збиток від таких зловживань в банківській сфері тільки в США становить від 100 млн. до 7.5 млрд. доларів. Витік тільки 20 відсотків комерційної інформації в 60 випадках зі 100 призводить до банкрутства фірм і банків.

Тож, якщо проаналізувати появу і розвиток європейських законів про захист ПДн, то потрібно зазначити, що головною причиною появи цих законів було виникнення автоматизованих баз даних, розвиток телекомунікацій та потреба у забезпеченні приватного життя людини відповідно до принципів [19].

Зокрема [8] є по собі міжнародно-правовим актом, який забезпечував упорядкування суспільних інформаційних відносин у сфері захисту ПДн. В ній регламентовані принципи захисту від неправомірного збирання, обробки, зберігання та поширення ПДн.

Щодо [9], то він передусім конкретизує вимоги Ради Європи до держав-членів Конвенції стосовно призначення національних органів нагляду і забезпечення транскордонних потоків даних. Протокол відзначає, що орган нагляду повинен мати повноваження щодо розслідування і втручання в необхідних випадках, а також мати право брати участь у судових засіданнях або оповіщати судові органи про порушення національного законодавства.

Інший нормативно-правовий акт, такий як [10] конкретизує європейські принципи та загальні умови обробки ПДн, умови правової допомоги, відповідальності та санкцій, порядок передачі даних до третіх країн, обумовлює

необхідність укладання кодексу поведінки при обробці ПДн, а також регламентує організаційні питання, що пов'язані з правами та обов'язками контрольного (наглядового) органу та консультативної групи у питаннях захисту ПДн.

А вже [11] зазначає, що у телекомунікаційному секторі Європейського Співтовариства запроваджуються нові передові цифрові технології та нові телекомунікаційні послуги, які зумовлюють певні вимоги до захисту ПДн користувача. Цей закон передбачає захист ПДн як фізичних осіб, так й захист законних інтересів юридичних осіб. Також ця [11] містить рекомендації, що спрямовані на гармонізацію положень держав-членів, необхідну для забезпечення адекватного рівня захисту ПДн у телекомунікаційному секторі та забезпечення їх вільного обігу.

Необхідно також розглянути міжнародний стандарт [25].

Згідно з цим стандартом, СУІБ - це «частина загальної системи управління організації, що заснована на оцінці бізнес ризиків, яка створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід та вдосконалення ІБ». Серед основних його цілей можна виділити: забезпечення безпеки найважливішої корпоративної інформації; захист основних активів і критичних бізнес-процесів організації; мінімізація ризиків ІБ при веденні операційної діяльності організації; забезпечення безперервності основної діяльності організації; підвищення загального рівня управління організації.

Також цей стандарт встановлює рекомендації з управління ІБ особам, відповідальним за планування, реалізацію або підтримку рішень безпеки в організації. Він призначений для забезпечення загальних основ для розробки стандартів безпеки та вибору практичних заходів з управління безпекою в організації, а також в інтересах забезпечення довіри в ділових відносинах між організаціями. Рекомендації цього стандарту слід вибирати і використовувати відповідно до чинного законодавства.

Останній закон - британський стандарт [24], який став першим у світі стандартом для СУПДн. Оскільки питання захисту ПДн є досить актуальним у

всьому світі, в ньому описано СУПДн і визначаються дії відносно ПДн. Основним недоліком цього стандарту є те, що він не передбачає процедуру оцінки застосування вимог на основі аналізу ризиків, і тому його вимоги є жорстко регламентовані.

До його переваг належить те, що цей стандарт може використовуватися організаціями будь-яких розмірів, сфери діяльності та форми власності для створення системи управління, котра включає в себе процедури в таких областях як навчання та підвищення обізнаності, оцінка ризику, спільне використання даних, збереження і знищення даних, мінімізує розкриття даних третіми сторонами.

Тобто можна зробити висновок, що за останні 25 років у більшості європейських країн прийняті базові закони про захист ПДн, створюються передумови розвитку їх вільного обміну і гармонізації національних законодавств із законодавством ЄС.

Однак незважаючи на розходження правових систем, в основу всіх законів про захист ПДн покладені однакові основоположні принципи, і ці принципи залишаються незмінними дотепер, навіть якщо саме законодавство в деяких країнах обновилося.

Зазначене не можна пояснити запозиченням досвіду хоча б тому, що деякі закони були прийняті майже одночасно. Всі вони мають однакову структуру, однакову мету і відрізняються лише у деталях. Захист ПДн передбачає обов’язкову реєстрацію баз даних і ліцензування діяльності щодо ПДн відповідними Уповноваженими органами. Відмова від реєстрації чи ліцензування розглядається як порушення національного законодавства.

Наостанок потрібно сказати, що право на захист ПДн у більшості розвинутих країн вже досить давно є одним з основоположних принципів правової держави. Захист ПДн трактується як невід'ємна частина права людини на захист особистого життя, закріпленого в таких актах як [12, 19].

Розділ 2
ОЦІНКА ЕФЕКТИВНОСТІ СИСТЕМИ УПРАВЛІННЯ ЗАХИСТОМ ПЕРСОНАЛЬНИХ ДАНИХ КЛІЄНТІВ БАНКУ: СТАН ТА НАПРЯМКИ РОЗВИТКУ

2.1.Основні види загроз ПДн в банківській сфері та їх характеристика

Перед тим, як визначити сучасний стан та напрямок розвитку СЗПДн потрібно детально проаналізувати основні види загроз ПДн в банківській сфері, визначити їх основні властивості та характеристики.

Отож, визначимо основні види загроз у банківській сфері при проведенні основних банківських операцій. Під поняттям загрози розуміється потенційно можливі або реальні дії зловмисників чи конкурентів, здатні нанести банку матеріальної або моральної шкоди. До неї також відносять недобросовісну конкуренцію і промислове шпигунство. В таблиці 2.1. наведено приклади основних способів і засобів здійснення злочинів та самих злочинців в банківській сфері.

Розрізняємо зовнішні та внутрішні загрози.

У свою чергу, як перші, так і другі за направленістю і характером впливу на банки можуть бути економічними, фізичними та інтелектуальними.

Наведемо приклади економічних, фізичних та інтелектуальних загроз банківській безпеці.

Економічні загрози можуть реалізовуватись у формі корупції, шахрайства, недобросовісної конкуренції, використання банками неефективних технологій банківського виробництва. Реалізація таких загроз веде до заподіяння збитків банкам або упущення ними вигоди.

Основними причинами виникнення економічних загроз можуть бути: недостатня адаптація банківської системи до постійно змінюваних умов ринку; загальна неплатоспроможність суб’єктів господарювання; зростаюча злочинність; споживацький менталітет значної кількості громадян; низький

рівень трудової дисципліни та відповідальності працівників банківських установ; недостатнє правове врегулювання банківської діяльності; низький професійний рівень частини керівного складу і працівників банку.

Таблиця 2.1

Типові способи, засоби та категорії осіб, що здійснюють злочини у банківській сфері

Вид операцій	Основні способи здійснення злочинів	Засоби здійснення злочинів	Особи, які здійснюють злочини
Депозитні операції	Неправомірне проникнення в КС банку. Підробка документів	Депозитні сертифікати. Комп'ютерні віруси. Помилкові комп'ютерні команди	В основному співробітники банку
Кредитні операції	Незаконне одержання кредиту Невиплата відсотків за кредитом Навмисне неповернення кредиту	Надання позичальником підроблених документів про кредитоспроможність або документів, що містять недостовірні дані. Фальсифікація надання застави під кредиті. Навмисне банкрутство	Особи, які не є співробітниками банку. Співробітники банку у змові з третіми особами
Розрахункові операції	Підробка документів. Внесення шахрайських змін у документи. Розкрадання документів. Неправомірне проникнення в КС банку та в електронні системи банківських рахунків.	Розрахунково-платіжні банківські документи. Пластикові картки. Комп'ютерні віруси. Помилкові комп'ютерні команди.	Співробітники банку. Особи, які не є співробітниками банку.

Фізичні загрози реалізуються у формі крадіжок, пограбувань майна та коштів банків, поломок, виведення із ладу обладнання банків, неефективної його експлуатації. Унаслідок реалізації таких загроз завдаються збитки банкам, пов’язані з втратою своєї власності та необхідністю нести додаткові витрати на відновлення засобів виробництва та інших матеріальних засобів.

Основними причинами фізичних загроз є неефективна кадрова політика банку, низька професійна підготовка банківських фахівців, недостатній рівень охорони установ банків, низький контроль стану роботи працівників банків.

Інтелектуальні загрози проявляються як розголошення або неправомірне використання банківської інформації, дискредитація банку на ринку банківських послуг, різного роду соціальні конфлікти навколо банківських установ або в них самих. Наслідками реалізації таких загроз можуть бути збитки банків, погіршення їхнього іміджу, соціальна чи психологічна напруженість навколо установ банків або в їхніх колективах. Причинами таких загроз, як правило, виступають загострення конкуренції на регіональних ринках банківських послуг, неефективна кадрова політика банків, порушення принципу гласності результатів банківської діяльності.

Із цих проблем виокремимо проблему захисту інформації в Інтернеті. Невпинне зростання користувачів Інтернет в останні роки спричинило появу в мережі багатьох негативних явищ. Покупки товарів з чужими кредитними картками, крадіжки інтелектуальної власності в Internet набули величезного розмаху і нікого вже не дивують.

Основною проблемою безпеки електронної комерції в Internet з часу її виникнення була проблема передавання закритої інформації (номерів кредитних карток, сум платежів тощо) через відкриту мережу. У таблиці 2.2. подано ймовірні загрози безпеці інформації, яка передається в мережі, разом з рішеннями, що дають змогу організувати й значно підвищити захищеність даних, у тому числі й у ситуаціях, не пов’язаних безпосередньо з електронною

комерцією (наприклад, під час відправлення конфіденційної інформації електронною поштою).

Таблиця 2.2

Імовірні загрози безпеці інформації в мережі й вирішення проблем захисту

Різновид загрози	Рішення	Дія	Технологія
Дані навмисно перехоплюються, читаються або змінюються	Шифрування	Кодування даних, яке перешкоджає їх читанню або викривленню	Симетричне або асиметричне шифрування
Користувачі ідентифікують себе неправильно (з шахрайською метою)	Автентифікація	Перевірка справжності відправника, одержувача і повідомлення	Цифрові підписи
Користувач отримує НСД з однієї мережі до іншої	Брандмауер	Фільтрація трафіка, який іде до мережі або на сервер	Брандмауер, віртуальні приватні мережі

Ці проблеми вирішується шифруванням даних, використанням брандмауерів та цифрових підписів. Щодо захисту на основі шифрування, то немає такої системи шифрування, що ідеально підходить для всіх ситуацій. У таблиці 2.3. проілюстровані переваги і недоліки кожного типу шифрування.

Таблиця 2.3

Порівняння методів шифрування

Тип шифрування	Переваги	Недоліки
Шифрування з симетричним ключем	Швидкість; Легко реалізувати апаратно.	Обидва ключа однакові; Важко поширювати ключі; Не підтримує цифрові підписи
Шифрування з відкритим ключем	Використовувати два різних ключі; Відносно просто поширювати ключі; Забезпечує цілісність і неможливість відмови від авторства (за рахунок цифрового підпису)	Працює повільно; Вимагає великих обчислювальних потужностей

Відомо, що алгоритми захисту інформації (насамперед шифрування) можна реалізувати як програмним, так і апаратним методом. Розглянемо апаратні шифратори: чому вони вважаються більш надійними і забезпечують кращий захист.

Апаратний шифратор з вигляду і, по суті, являє собою звичайну комп’ютерну апаратуру, найчастіше це плата розширення, що вставляється в роз’єм системної плати ПК. Виробники апаратних шифраторів зазвичай намагаються оснастити їх різними додатковими можливостями, серед яких:

Генерація випадкових чисел. Це потрібно, насамперед, для отримання криптографічних ключів.

Контроль входу на комп’ютер. При включенні ПК пристрій вимагає від користувача ввести персональну інформації (наприклад, вставити дискету з ключами). Робота буде дозволена тільки після того, як пристрій пізнає пред’явлені ключі доступу і визнає їх зареєстрованими. В іншому випадку доведеться розбирати системний блок і виймати звідти шифратор , щоб завантажитися (проте, як відомо, інформація на ПК теж може бути зашифрована).

Контроль цілісності файлів операційної системи. Це не дозволить зловмиснику у вашу відсутність змінити будь-які дані. Шифратор зберігає в

собі список всіх важливих файлів із заздалегідь розрахованими для кожного контрольними сумами, і якщо при наступному завантаженні не збігається еталонна сума хоча б одного з них, комп’ютер буде блокований.

Плата з усіма перерахованими можливостями називається пристроєм криптографічного захисту даних - ПКЗД.

Шифратор котрий виконує контроль входу на ПК і перевіряє цілісність операційної системи, називається також електронним замком. Зрозуміло, що електронному замку не обійтися без програмного забезпечення - необхідна утиліта, за допомогою якої формуються ключі для користувачів і ведеться їх список для розпізнання свій/чужий. Потрібна програма для вибору важливих файлів і розрахунку їх контрольних сум. Ці програми зазвичай доступні тільки адміністратору з безпеки, який повинен попередньо налаштувати всі ПКЗД для користувачів, а в разі виникнення проблем розбиратися в їх причинах.

Тепер розмежуємо всі дії, що призвели до порушення ІБ. В основному вони поділяються на такі складові:

НСД до інформації;

розголошення інформації;

витік інформації.

Несанкціонований доступ (НСД). Це найбільш поширений вид інформаційних загроз. НСД – це доступ до інформації в порушення посадових повноважень співробітника, доступ до закритої для публічного доступу інформації з боку осіб, які не мають дозволу на доступ до цієї інформації. Також НСД в окремих випадках називають отримання доступу до інформації особою, яка має право на доступ до цієї інформації в обсязі, що перевищує необхідний для виконання службових обов'язків.

За характером, вплив НСД є активним впливом, що використовує помилки системи. НСД звертається безпосередньо до необхідного набору даних, або впливає на інформацію про санкціонованому доступі з метою легалізації НСД. НСД може бути підданий будь-який об’єкт системи. НСД

може бути здійснений як стандартними, так і спеціально розробленими програмними засобами до об'єктів.

Є досить примітивні шляху НСД:

розкрадання носіїв інформації та документальних відходів;

ініціативне співробітництво;

схилення до співпраці з боку зломщика;

випитування;

підслуховування;

спостереження

інші шляхи.

Будь-які способи витоку конфіденційної інформації можуть привести до значного матеріального і морального збитку як для організації, де функціонує ІС, так і для її користувачів.

Менеджерам слід пам'ятати, що досить велика частина причин і умов, що створюють передумови і можливість неправомірного оволодіння конфіденційною інформацією, виникає через елементарні недопрацювання керівників організацій та їх співробітників. Наприклад, до причин і умов, що створює передумови для витоку комерційних секретів, можуть належати:

недостатнє знання працівниками організації правил захисту конфіденційної інформації і нерозуміння необхідності їх ретельного дотримання;

використання неатестованих технічних засобів обробки конфіденційної інформації;

слабкий контроль за дотриманням правил захисту інформації правовими, організаційними та технічними заходами.

Методики НСД зводиться до двох різновидів:

«Злам» зсередини: злочинець має фізичний доступ до терміналу, з якого доступна інформація, котра його цікавить. Він може певний час працювати на ньому без стороннього контролю.

«Злам» ззовні: злочинець не має безпосереднього доступу до комп’ютерної системи, але має можливість будь-яким способом (зазвичай за допомогою віддаленого доступу через мережі) проникнути в захищену систему для впровадження спеціальних програм, маніпуляцій з оброблюваною інформацією або інформацією, що зберігається в цій системі, чи здійснення інших протизаконних дій.

Розголошення інформації. На відміну від необережності, навмисне розголошення інформації передбачає, що метою дій співробітників було саме розголошення інформації, що є конфіденційною. Причому співробітників могли завербувати агенти промислового шпигунства або ж вони самі ініціативно вирішили зрадити організацію, на яку працювали (в цих випадках вони вже самі можуть шукати контактів з представниками конкуруючих фірм чи інших осіб, зацікавлених в отриманні певної інформації).

Для того щоб виявити або попередити такі дії, потрібно визначитися, чому ж саме працівники пішли на них. Кожна людина є індивідуальною, в кожного своє життя та свої проблеми, через які він приймає ті чи інші рішення. Тож кожна ситуація має свої нюанси, але є декілька розповсюджених причин для розголошення інформації співробітниками. До них відносяться:

помста;

матеріальна або інша вигода;

самореалізація.

Саме з цих причин персонал банку найчастіше зраджує його інтереси. Багато в чому тут також є прорахунки керівництва. Саме це найчастіше є тим, через що вербують співробітників. Невдоволені працівники краще йдуть на контакт з промисловими шпигунами, бо не відчувають патріотизму до цієї фірми, мріють поквитатися з кимось із колег чи з керівництвом, або прагнуть покращити своє матеріальне становище. Таким особам пропонують те, чого в них немає і не буде на даній фірмі: або значні матеріальні виплати, або ж пропонування роботи, де їх працю оцінять, де їх будуть поважати, або ж інші речі, що відповідають потребам цих співробітників.

Розголошення комерційних секретів, мабуть, найбільш розповсюджена дія власника інформації, що призводить до неправомірного оволодіння конфіденційною інформацією за мінімальних витратах зусиль з боку зловмисника. Для цього він користується в основному легальними шляхами і мінімальним набором технічних засобів. Реалізується розголошення формальними і неформальними каналами поширення інформації.

До формальних каналів поширення інформації належать:

ділові зустрічі, наради, переговори та інші форми спілкування;

обмін офіційними діловими, науковими і технічними документами засобами передачі офіційної інформації (пошта, телефон, телеграф, факс тощо).

Неформальними каналами поширення інформації є:

особисте спілкування (зустрічі, переписка, телефонні переговори тощо);

виставки, семінари, конференції, з'їзди та інші масові заходи;

засоби масової інформації (преса, інтерв'ю, радіо, телебачення тощо).

Як правило, причиною розголошення конфіденційної інформації є:

слабке знання (або незнання) вимог захисту конфіденційної інформації;

помилковість дій персоналу через низьку виробничу кваліфікацію;

відсутність системи контролю за оформленням документів, підготовкою виступів, реклами і публікацій;

злісне, навмисне невиконання вимог захисту комерційної таємниці.

Тому співробітник, який отримав доступ до конфіденційної інформації, повинен в обов'язковій формі підписати індивідуальне письмове зобов'язання про її нерозголошення.

Витік конфіденційної інформації - це безконтрольний вихід конфіденційної інформації за межі підприємства або кола осіб, яким вона була довірена по службі або стала відома в процесі роботи. Цей витік може бути наслідком:

розголошення конфіденційної інформації;

перехоплення інформації з різних, головним чином технічних, каналів витоку інформації;

НСД до конфіденційної інформації різними способами.

І наостанок хотіла звернути увагу на підбір паролів персоналом організації. Потрібно дуже уважно відноситися до вибору персоналом паролів. Існує велика ймовірність взлому пароля, якщо його вибрати загалоновідомим, наприклад ім’я, фамілія, номер паспорту і т.д., адже зловмисники можуть використовувати так званий метод «інтелектуального перебору» паролів.

Метод «інтелектуального перебору» заснований на підборі передбачуваного пароля, виходячи з заздалегідь визначених тематичних груп його приналежності. Результати експериментів, представлені фахівцями у таблиці 2.4.:

Таблиця 2.4

Статистичні дані методу «інтелектуального перебору» паролів

Тематичні групи паролів	Частота вибору пароля людиною, %	Розкриття пароля, %
Імена, прізвища	21,2	54,5
Інтереси (хобі, спорт, музика)	9,5	29
Дати народження, знаки зодіаку свої і близьких; їх комбінація з першою групою	10,8	54,5
Адреса проживання, місце народження	4,7	55
Номери телефонів	3,5	66
Послідовність клавіш ПК, повтор символу	16,1	72,3
Номери документів (паспорт, пропуск, посвідчення і т.д.)	3,5	100
Інші	30,7	5,7

Дана статистика розкриття паролів повинна стати застереженням «любителям» установки тематичних паролів - вони є ненадійними, тому що дуже легко розкриваються.

Тому, щоб вирішити висвітлені вище проблеми захисту ПДн потрібно розробити надійну послідовність впровадження СЗПДн.

Почати впровадження СУІБ в організації необхідно з вивчення стандарту керівним складом та фахівцями в галузі ІБ. Потім необхідно провести інвентаризацію ресурсів та оцінку рівня зрілості організації в області ІБ організації, після чого слід приступати до розробки плану впровадження СЗПДн. Належну увагу потрібно приділити підвищенню кваліфікації та перепідготовці фахівців в області ІБ. Далі розробляються нормативні документи, що реалізують практичні правила управління ІБ, і відбувається введення їх у дію. Організація приступає до практичної реалізації правил управління ІБ організації. Після чого, політику ІБ і інструкції щодо забезпечення ІБ доводять до відома всіх службовців організації.

2.2. Система захисту персональних даних в банку, її склад та вимоги до неї

Треба сказати, що найголовніше в функціонуванні СЗПДн є надійний безперебійний захист від всіх впливів навколишнього та внутрішнього середовища, котрі несуть в собі загрозу для надійної роботи даної системи. Тому для мінімізації ризиків потрібно провести достовірну оцінку системи управління захистом ПДн клієнтів банку.

Для об’єктивної оцінки системи управління захистом ПДн клієнтів банку потрібно детально проаналізувати основні загрози, способи їх вирішення та розробку послідовності дій при побудові і впровадженню СУІБ.

Насамперед необхідно визначити, що являє собою банківська безпека та яка її основна мета.

Банківська безпека — це стан стійкої життєдіяльності, за якого забезпечуються реалізація основних інтересів, пріоритетних цілей банків, захист від зовнішніх і внутрішніх дестабілізуючих факторів незалежно від умов їх функціонування. Основним критерієм ефективності безпеки банківської діяльності є стабільність фінансового і економічного стану банку.

Передусім метою безпеки банківської діяльності є усунення можливостей завдання банку збитків або упущення ним вигоди, забезпечення його ефективної діяльності та якісної реалізації операцій і угод.

Банк, котрий хоче уберегти себе від протиправних посягань зі сторони злочинців повинен створити спеціальну СБ у себе на підприємстві. СБ формується на основі аналізу, оцінки та прогнозування діяльності організації в частині вирішення завдань забезпечення її безпеки.

СБ - система штатних органів управління та підрозділів, призначених для забезпечення безпеки організації. Правовою основою формування СБ є рішення керівництва про створення СБ, оформлене відповідним наказом чи розпорядженням, або рішенням вищестоящої організації, до складу якої входить дана організація.

СБ підприємства підпорядковується керівнику служби безпеки, який знаходиться в підпорядкуванні керівника організації. Штатна структура і чисельність СБ визначається реальними потребами організації. Мета даної служби - визначення конкретного завдання безпеки банківської діяльності.

До завдань служби безпеки в банківській діяльності відносять [39]:

Захист законних інтересів банку та його працівників.

Профілактика та попередження правопорушень і злочинних посягань на власність і персонал банку.

Своєчасне виявлення реальних і потенційних загроз банку, проведення заходів щодо їх нейтралізації.

Оперативне реагування елементів структури банку на загрози, що виникають, та негативні тенденції розвитку зовнішньої і внутрішньої обстановки.

Виявлення внутрішніх і зовнішніх причин та умов, які можуть сприяти заподіянню банку, його працівникам, клієнтам і акціонерам матеріальної та іншої шкоди, перешкоджати їх нормальній діяльності.

Виявлення та формування причин і умов, сприятливих для реалізації банком своїх основних інтересів.

Виховання та навчання персоналу з питань безпеки.

Послаблення шкідливих наслідків від акцій конкурентів або злочинців, спрямованих на підрив безпеки банку.

Збереження й ефективне використанні фінансових, матеріальних та інформаційних ресурсів банку.

Тепер перейдемо до етапів побудови системи захисту інформації. Кожну систему захисту слід розробляти індивідуально, враховуючи такі особливості:

Організаційну структуру організації;

Обсяг і характер інформаційних потоків (всередині об'єкта в цілому, всередині відділів, між відділами, зовнішніх);

Кількість і характер виконуваних операцій: аналітичних і повсякденних;

Кількість і функціональні обов'язки персоналу;

Кількість і характер клієнтів;

Графік добового навантаження.

Захист обов’язково повинен розроблятися для кожної системи індивідуально, але відповідно до загальних правил. Тобто має бути визначена послідовність впровадження СЗПДн.

До послідовності впровадження СЗПДн належать такі складові [29, стор. 14]:

Вивчення стандартів керівним складом і фахівцями в галузі ІБ.

Інвентаризація ресурсів.

Визначення рівня зрілості організації в області ІБ.

Розробка плану впровадження СЗПДн.

Підвищення кваліфікації та перепідготовка фахівців в ІБ.

Розробка нормативних документів з практичним правилам управління ІБ і введення їх у дію.

Практична реалізація правил управління ІБ.

Ознайомлення персоналу з політикою ІБ та інструкціями щодо забезпечення ІБ.

Типовою компанією, яка впроваджує СЗПДн, як правило, є та, яка або сама має великі обсяги інформації, або змушена керувати нею за дорученням своїх клієнтів. Але є й такі організації, де питанням захисту інформації приділяється зовсім мало уваги, а в деяких зведені нанівець. Тому необхідно визначити до якого рівня зрілості в галузі захисту інформації вона відноситься (таблиця 2.5.).

Етапи розвитку та існування підприємства класифікують залежно від того, як воно обробляє і використовує інформацію в процесі своєї діяльності [6]. Застосування сертифікованих засобів захисту інформації включає апаратні, програмні, програмно-апаратні засоби захисту. Рівні зрілості організації розрізняються наявністю в повному обсязі, не в повному обсязі або відсутністю нормативних документів, які регламентують забезпечення ІБ, відповідальності персоналу, що працює з такого роду інформацією і так далі.

Таблиця 2.5

Рівні зрілості організації в галузі захисту інформації та їх характеристики

Рівень зрілості	Характеристики		
	Засоби захисту	Відповідальний за захист персонал	Регламентація
1)Хаос (Спонтанні інформаційні зв'язки)	Відсутні	Відсутні	Відсутні
2)Фрагментарний захист	Використовуються фрагментарно	Призначені відповідальні за захист	Є окремі документи, що регламентують захист
3)Системний захист	Використовуються засоби захисту, об'єднані в систему	Сформовано служба захисту інформації	Діяльність по захисті регламентована нормативними документами
4)Керований захист	Функціонує КСЗІ	Персонал, відповідальний за захист інформації має спеціальну підготовку (освіта, перепідготовка)	Впроваджено СУІБ організації на основі [25]
5)Управління якістю ІБ (Оптимізуються)	Функціонує КСЗІ	Персонал відповідальний за захист інформації має спеціальну підготовку (освіта, перепідготовка)	Впроваджені: СУІБ на основі [25]; система менеджменту якості інформаційної безпеки на основі [21-23]

Компанія, що знаходиться на самому високому рівні розвитку, всі системи являють собою єдиний інтегрований комплекс, забезпечує ефективне управління та обробку інформації на всіх етапах її роботи.

Найвищий етап розвитку є ідеалом, який доступний лише лідерам, тому в сучасних умовах підприємство (і це особливо важливо для українських компаній) має прагнути забезпечити умови для функціонування на четвертому рівні.

Також потрібно зазначити, що для максимального захисту системи ПДн слід використовувати і виконувати такі принципи ІБ:

Принцип законності. Складається в проходженні чинним законодавством в галузі забезпечення ІБ.

Принцип неможливості створення ідеальної системи захисту. Випливає з принципу невизначеності та обмеженості ресурсів та коштів.

Принципи мінімального ризику і мінімального збитку. Випливають з неможливості створення ідеальної системи захисту. Відповідно до нього необхідно враховувати конкретні умови існування об'єкта захисту для будь-якого моменту часу.

Принцип «захисту всіх від усіх». Передбачає організацію захисних заходів проти всіх форм загроз об'єктам захисту, що є наслідком принципу невизначеності.

Принципи персональної відповідальності. Передбачає персональну відповідальність кожного співробітника підприємства, установи та організації за дотримання режиму безпеки в рамках своїх повноважень, функціональних обов'язків і діючих інструкцій.

Принцип обмеження повноважень. Передбачає обмеження повноважень суб'єкта на ознайомлення з інформацією, до якої не потрібно доступу для нормального виконання ним своїх функціональних обов'язків, а також введення заборони доступу до об'єктів і зон, перебування в яких не вимагається за родом діяльності.

Принцип взаємодії та співпраці. У внутрішньому прояві передбачає культивування довірчих відносин між співробітниками, що відповідають за безпеку (в тому числі інформаційну), і персоналом. У зовнішньому прояві - це

налагодження співпраці з усіма зацікавленими організаціями та особами (наприклад, правоохоронними органами, охоронними фірмами).

Принцип комплексності та індивідуальності. Передбачає неможливість забезпечення безпеки об'єкта захисту якимсь одним заходом чи методом, а лише сукупністю комплексних і взаємопов'язаних заходів, що реалізуються з індивідуальною прив’язкою до конкретних умов.

Принцип послідовних етапів безпеки. Передбачає якомога раніше оповіщати про посягання на безпеку того чи іншого об'єкта захисту чи іншу несприятливу дію з метою збільшення ймовірності того, що завчасний сигнал тривоги засобів захисту забезпечить співробітникам, відповідальним за безпеку, можливість вчасно визначити причину тривоги і організувати ефективні заходи з протидії.

Зазначені вище принципи ІБ реалізуються за допомогою наступних основних засобів: апаратних, програмних, апаратно-програмних, криптографічних, організаційних та законодавчих. Нижче наведені пояснення до кожного з засобів.

Апаратні засоби захисту - це електронні, електромеханічні та інші пристрої, безпосередньо вбудовані в блоки автоматизованої ІС або оформлені у вигляді самостійних пристроїв і сполучаються з цими блоками. Вони призначені для внутрішнього захисту структурних елементів засобів і систем обчислювальної техніки: терміналів, процесорів, периферійного обладнання, ліній зв'язку і т.д.

Програмні засоби захисту призначені для виконання логічних і інтелектуальних функцій захисту і включаються або до складу програмного забезпечення автоматизованої ІС, або до складу засобів, комплексів і систем апаратури контролю.

Програмні засоби захисту інформації є найбільш поширеним видом захисту, володіючи такими позитивними властивостями: універсальністю, гнучкістю, простотою реалізації, можливістю зміни і розвитку. Дана обставина

робить їх одночасно і найбільш вразливими елементами захисту ІС підприємства.

Апаратно-програмні засоби захисту – це засоби, в яких програмні (мікропрограмні) і апаратні частини повністю взаємопов'язані і нероздільні.

Криптографічні засоби – це засоби захисту за допомогою яких здійснюється перетворення інформації (шифрування).

Організаційні засоби – це організаційно-технічні та організаційно-правові заходи, котрі регламентують поведінку персоналу.

Законодавчі засоби - це правові акти країни, які регламентують правила використання, обробки та передачі інформації обмеженого доступу і які встановлюють міри відповідальності за порушення цих правил.

Комплексність захисту повинна використовувати організаційні, технічні та правові заходи і засоби. Тож вся СЗПДн в банку обов’язково повинна складатися з трьох основних складових (рис. 2.1.), котрі взаємодіють між собою:

організаційного захисту;

технічного захисту;

правового захисту.

Рис. 2.1. Основні складові системи захисту персональних даних в банку

Організаційні заходи та засоби захисту:

Розподіл відповідальності.

Постійна підтримка (періодичний перегляд системи управління захистом інформації).

Періодичний перегляд методів контролю безпеки.

Перевірка благонадійності персоналу.

Оцінка ризиків.

Навчання в галузі безпеки інформації.

Розподіл обов'язків.

Реєстрація та видалення облікових записів в ІС.

Підтримка в актуальному стані плану захисту підприємства.

Знищення залишкових даних.

Контроль цілісності даних і програм.

Зміна паролів.

Обмеження на використання мережевих сервісів, служб, мережевих протоколів , сценаріїв.

Розробка документів (регламентують питання організації забезпечення безпеки ПДн: порядок роботи з криптографічними засобами захисту інформації, положення з організації та проведення робіт із забезпечення безпеки ПДн при їх обробці в ІСПДн, вимоги щодо забезпечення безпеки ПДн при обробці в ІСПДн, порядок надання доступу до ПДн.)

Підготовка персоналу (забезпечення доступу відповідальним особам до ПДн, оброблюваних в ІС, для виконання посадових обов'язків).

Також сюди входить створення служби безпеки на підприємстві, котра виконує всі організаційні заходи захисту.

Отож, які організаційні заходи щодо забезпечення безпеки ПДн треба зробити, і що треба зробити в першу чергу, а що можна зробити пізніше?

При забезпеченні безпеки ПДн на початку розробки насамперед необхідно розробити документи, що регламентують захист ПДн в організації: положення про обробку ПДн, регламенти, керівництво користувачам і

адміністраторам ІСПДн, акт класифікації ІСПДн, перелік застосовуваних засобів захисту інформації і т.д.

Розробити форму і порядок письмової згоди суб'єктів ПДн на обробку своїх ПДн, визначити строки зберігання ПДн, розробити план заходів щодо захисту ПДн (і виконати ці заходи):

обмеження доступу до ПДн;

визначення кола осіб, допущеного до обробки ПДн, контроль обробки ПДн;

встановлення персональної відповідальності за порушення правил обробки ПДн;

організація доступу в приміщення, де здійснюється обробка ПДн.

ПДн на паперових носіях зберігаються в робочий і неробочий час у металевих шафах, що закриваються. Співробітникам банку заборонено при виході з приміщення залишати будь-які документи, що містять ПДн, на робочому столі або залишати незамікненими пристрої замикаються (дотримання «політики чистих столів»). Під час роботи з документами, що містять відомості про ПДн, допускається зберігання таких документів протягом робочого дня в особистих сейфах, проте зробити так, щоб повністю виключтити відкритий доступ до них. На робочому столі співробітника винен завжди знаходитися тільки той массив документів, що містять ПДн, з яким зараз він працює. Інші документи, справи, що містять ПДн, протягом робочої години повінні перебуваті в особистих пристроях, що закриваються. Зберігання ПДн має здійснюватіся у формі, що дозволяє ідентіфікуваті клієнта і не довше ніж цього вімагають цілі обробки ПДн.

Зберігання конфіденційних документів вимагає особливого режиму, так як інформація, що міститься в даних документах, є об'єктом захисту. Спеціальний режим [40] зберігання конфіденційних документів передбачає обов'язкове дотримання наступних правил:

1. Приміщення, де зберігаються конфіденційні документи, не повинно знаходитися на першому або останньому поверхах будівлі, тому що дані поверхи потенційно найбільш доступні для проникнення.

2. Вхід в приміщення дозволяється тільки особам, які мають доступ до роботи з документами.

3. Прибирання, ремонт приміщень в яких перебувають обладнання і технічних засоби, пов'язаних із залученням осіб, що не мають доступу до документів, що там зберігаються, повинні проходити тільки в присутності співробітників служби захисту інформації.

4. Вхідні двері приміщень повинні бути оббиті металом і обладнані надійними замками.

5. По закінчення робочого дня двері не тільки закриваються, а й опечатуються печаткою служби захисту інформації. Друк проставляється на тонкий шар пластиліну таким чином, щоб відбиток не можливо було зняти і відновити.

6. Перед відкриттям дверей на початку робочого дня перевіряється збереження відбитка печатки і цілісність запорів. При виявленні спроб проникнення в приміщення необхідно негайно поставити до відома службу безпеки і доповісти першому керівнику. До прийняття рішення першим керівником приміщення не відкриваються і забезпечуються фізичною охороною .

7. Для запобігання несанкціонованого входу в приміщення протягом робочого дня на дверях встановлюються електромеханічні або електронні замки.

8. Вхідні двері, вікна, сейфи, шафи, стелажі слід оснастити охоронною сигналізацією.

Організаційно-адміністративні заходи передбачають:

мінімізацію витоку інформації через персонал (організація заходів щодо підбору і розстановки кадрів, створення сприятливого клімату в колективі і т. д.);

організацію спеціального діловодства та документообігу для конфіденційної інформації, що встановлюють порядок підготовки, використання, зберігання, знищення та обліку документованої інформації на будь-яких видах носіїв;

виділення спеціальних захищених приміщень для розміщення засобів обчислювальної техніки і зв'язку, а також зберігання носіїв інформації;

виділення спеціальних засобів комп'ютерної техніки для обробки конфіденційної інформації;

організацію зберігання конфіденційної інформації на промаркованих відчужуваних носіях у спеціально відведених для цієї мети місцях;

використання в роботі сертифікованих технічних і програмних засобів, встановлених в атестованих приміщеннях;

встановлення заборони на використання відкритих каналів зв'язку для передачі конфіденційної інформації;

контроль дотримання вимог щодо захисту конфіденційної інформації.

Система організаційних заходів, спрямованих на максимальне запобігання витоку інформації через персонал включає:

оцінка у претендентів на вакантні посади при підборі кадрів таких особистісних якостей, як порядність, надійність, чесність і т. д.;

обмеження кола осіб, що допускаються до конфіденційної інформації;

перевірка надійності співробітників, що допускаються до конфіденційної інформації, письмове оформлення допуску;

розвиток і підтримку у працівників компанії корпоративного духу, створення внутрішньої середовища, що сприяє прояву у співробітників почуття приналежності до своєї організації, позитивного ставлення людини до організації в цілому (лояльність);

проведення інструктажу працівників, що беруть участь у заходах, які безпосередньо належать до одного з можливих каналів витоку інформації.

Всі особи, що приймаються на роботу, проходять інструктаж і знайомляться з пам’яткою про збереження службової або комерційної таємниці.

Пам’ятка розробляється системою безпеки з урахуванням специфіки організації.

Співробітник, який отримав доступ до конфіденційної інформації, підписує індивідуальне письмове зобов’язання про її нерозголошення. Зобов'язання складається в одному примірнику і зберігатися в особовій справі співробітника не менше 5 років після його звільнення. При звільненні з організації співробітником дається підписка. Функції відібрання зобов’язання і підписок покладаються на кадровий апарат організації.

Службовець організації, підписуючи подібного роду документ, повинен чітко уявляти, що конкретно з конфіденційної інформації є таємницею організації. У тому числі з цієї причини необхідно, щоб вся конфіденційна інформація була відособлена від решти відомостей, а документи, що її містять, носили відповідний гриф.

Використання зобов'язань про збереження конфіденційної інформації дозволяє забезпечити її юридичний захист, до якої має (або мав) доступ персонал організації.

Всі керівники, співробітники і технічний персонал повинні бути охоплені регулярної підготовкою з питань забезпечення ІБ. При цьому має бути два види навчання: початкове і систематичне.

З співробітниками, що звільняються проводяться бесіди, спрямовані на запобігання розголошенню конфіденційної інформації. Ці зобов'язання, як правило, підкріплюються відповідною підпискою.

Організацією конфіденційного діловодства є:

Документування інформації;

Облік документів та організація документообігу;

Забезпечення надійного зберігання документів;

Перевірка наявності, своєчасності та правильності їх виконання;

Своєчасне знищення документів.

Технічні заходи та засоби захисту [32]**:**

1. Програмні засоби ОС

Засоби блокування модифікації та несанкціонованого доступу.

Програмні засоби адміністрування (розмежування повноважень, реєстрації та контролю).

Програмні засоби ідентифікації і аутентифікації.

Програмні засоби резервного копіювання.

2. Криптографічні засоби

Абонентського шифрування

Пакетного шифрування

Шифрування паролів

Стеганографії

ЕЦП

VPN - технології

3. Інші засоби захисту

Засоби тестування мереж і програм

Засоби виявлення атак

Міжмережеві екрани

Засоби виявлення шкідливих програм

Засоби тестування

Програми для відновлення інформації.

Правові заходи та засоби захисту [Творча розробка].

Полягає в спиранні на документацію, починаючи з міжнародних стандартів, державних, галузевих законів закінчуючи розробкою внутрішньої документації для забезпечення безперервності та покращення СЗПДн.

До цієї документації відносять:

Повідомлення про обробку ПДн.

Положення про порядок обробки ПДн.

Положення про підрозділ, що здійснює функції з організації захисту ПДн.

Наказ про призначення відповідальних осіб для роботи з ПДн.

Посадові регламенти осіб, які здійснюють обробку ПДн.

Журнали (реєстри, книги) містять ПДн, які необхідні для одноразового пропуску суб'єкта ПДн на територію, на якій знаходиться оператор, або в інших аналогічних цілях.

Тепер потрібно розглянути СЗПДн в банку. Якщо перейти до складу, то як правило, система захисту включає в себе такі основні підсистеми [35]:

Підсистему антивірусного захисту, призначену для виявлення і блокування шкідливого коду;

Розмежування доступу, що забезпечує захист від НСД до ПДн. Як правило, дана підсистема виконує функції реєстрації та обліку, а також контролю цілісності;

Криптографічного захисту, призначену для забезпечення конфіденційності ПДн у процесі їх передачі по каналах зв'язку;

Міжмережевого екранування, яка встановлюється в точці з’єднання з Інтернетом або між ІС різних класів. Підсистема призначена для фільтрації потенційно небезпечних пакетів даних, що проходять через міжмережевий екран;

Виявлення вторгнень, призначену для виявлення і блокування мережевих атак в ІС;

Аналізу вразливостей, що забезпечує виявлення наявних вразливостей в програмному, апаратному та телекомунікаційному забезпеченні ІС, що обробляє ПДн.

Основні вимоги до КСЗІ [36]:

розробка на основі положень і вимог існуючих законів, стандартів і нормативно-методичних документів щодо забезпечення ІБ;

використання комплексу програмно-технічних засобів і організаційних заходів для її захисту;

надійність, продуктивність, конфігурованість;

економічна доцільність (оскільки вартість засобів захисту не повинна бути вище можливого збитку від втрати інформації);

можливість вдосконалення;

забезпечення розмежування доступу до конфіденційної інформації з відволіканням порушника на неправдиву інформацію (забезпечення не тільки пасивного, але й активного захисту);

забезпечення проведення обліку та розслідування випадків порушення безпеки інформації в системі;

можливість оцінки ефективності її застосування.

Отож, КСЗІ в стандартному вигляді є такою.

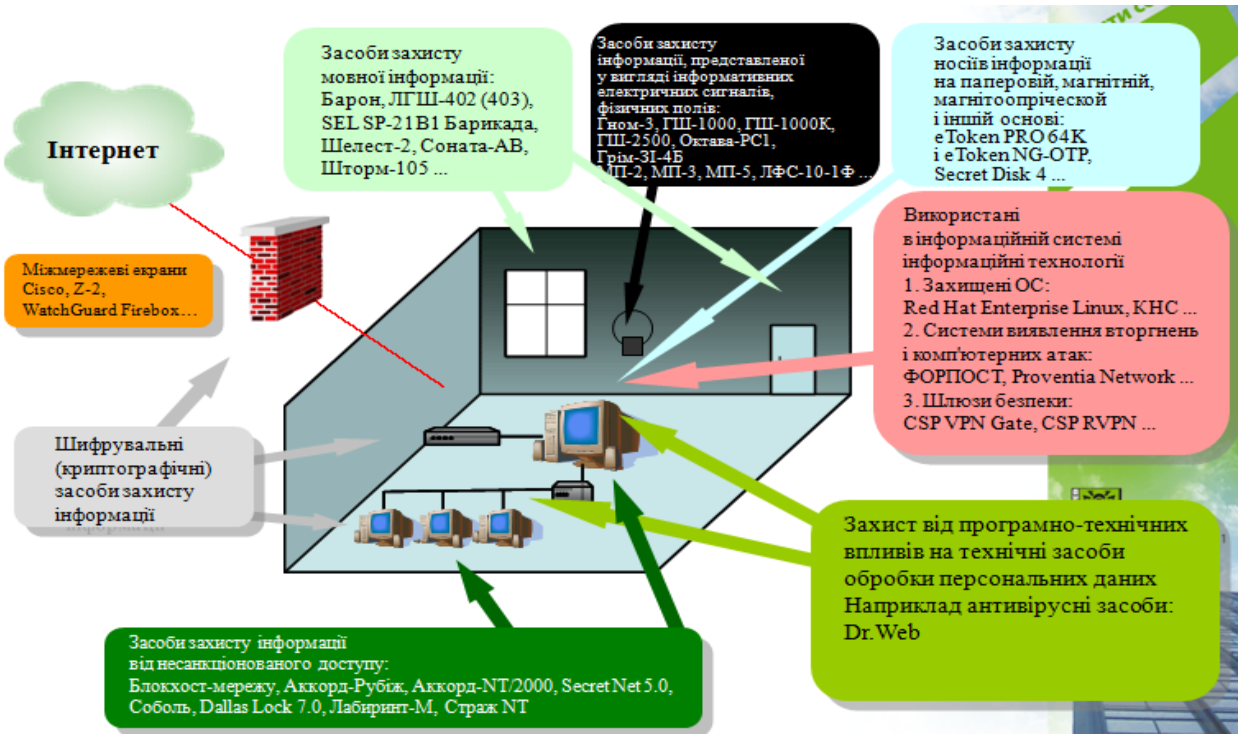

Рис.2.2. Склад КСЗІ на підприємстві

Також потрібно виділити основні інструменти захисту ПДн. Передусім захист ПДн можна забезпечити тільки в тій ІС, де зловмисник не може втрутитися в роботу її базових елементів - мережевих пристроїв, операційних систем і т.д. І обов’язково потрібно застосовувати комплексність захисту.

До комплексу захисту належать: антивіруси, міжмережеві екрани, системи запобігання вторгнень, сканери вразливостей, контроль над пристроями, DLP–системи, шифрування; управління правами доступу.

Антивіруси. Захист від вірусів є одним із засобів запобігання витоків конфіденційної інформації, в тому числі і ПДн, - віруси, черв’яки і інші шкідливі програми часто займаються крадіжкою інформації та організують приховані канали витоку. Сучасні антивірусні рішення включають в себе не тільки сигнатурну захист, але і більш сучасні засоби, такі як поведінковий аналіз програм, екрани рівня додатків, контроль цілісності критичних для операційної системи даних і інші методи захисту робочих місць і серверів.

Міжмережеві екрани. Корпоративна мережа цілком повинна бути захищена не тільки від масових атак за допомогою вірусів, але і від цілеспрямованих мережевих атак. Для цього достатньо поставити систему блокування невикористовуваних мережевих протоколів і сервісів, що і робить міжмережевий екран. Часто до функціональності міжмережевих екранів додають і засоби організації віртуальних приватних мереж - VPN.

У деяких антивірусних рішеннях класу Internet Security (наприклад, «Лабораторії Касперського», Symantec, Eset, McAfee і Trend Micro) вже вбудовані персональні міжмережеві екрани, що фіксують атаки з мережних протоколах і спроби мережевих черв'яків проникнути на захищену машину.

Системи запобігання вторгнень. Системи запобігання вторгнень (Intrusion Prevention System, IPS) встановлюються в розрив мережі і служать для виявлення в трафіку ознак нападу. На відміну від шлюзових антивірусів, IPS аналізують не тільки вміст IP-пакетів, але і використовувані протоколи і коректність їх використання. Спектр атак, від яких можуть захистити системи запобігання вторгнень, дещо ширше, ніж у шлюзових антивірусів . Системи IPS виробляють як компанії, що спеціалізуються на мережевому захисті, такі як Check Point і McAfee (продукт Network Security Platform), так і виробники мережевого устаткування - Juniper і Cisco.

Сканери вразливостей. До загальних засобів захисту відносяться також сканери вразливостей, які перевіряють ІБ на наявність різних «проломів» в операційних системах та програмному забезпеченні. Як правило, це окремі програми або пристрої,які тестують систему шляхом посилання спеціальних

запитів, що імітують атаку на протокол або додаток. Найбільш популярними продуктами цього класу є MaxPatrol, сімейство продуктів IBM ISS, Symantec і McAfee (Vulnerability Manager). Втім, зараз з'являються пасивні сканери, які просто контролюють мережевий трафік і виявляють в ній наявність тих чи інших ознак уразливості. Такі сканери тільки з'явилися і ще не завоювали досить великої частки ринку. Сканери вразливостей можна використовувати для проведення внутрішнього аудиту захисту.

Згадані засоби захисту є загальними для всієї мережі і не пов'язані безпосередньо з захистом власне ПДн, проте їх присутність має бути обов’язковою, так як вже сама їх наявність говорить про виконання мінімальних вимог захисту, що саме по собі є правилом хорошого тону.

Контроль над пристроями. Нерідко витік даних відбувається через знімні носії інформації і несанкціоновані канали зв'язку: флеш-пам’ять, USB-диски, Bluetooth або Wi-Fi, тому контроль за використанням USB-портів і іншого периферійного обладнання також є одним із способів контролю витоків . На ринку є кілька рішень цього класу, наприклад від компаній SmartLine і SecureIT.

DLP-системи. (DLP - Data Loss Prevention). Системи захисту від витоків дозволяють за допомогою спеціальних алгоритмів виділити з потоку даних конфіденційні і заблокувати їх несанкціоновану передачу. У DLP-системах передбачені механізми контролю різноманітних каналів передачі інформації: електронної пошти, миттєвих повідомлень, Web- пошти, друку на принтері, збереження на знімному диску та ін. Причому модулі DLP блокують витік тільки конфіденційних даних, оскільки мають вбудовані механізми для визначення того, наскільки та чи інша інформація є секретною.

У цьому випадку використовується три технології: за ключовими словами і регулярними виразами, за відбитками еталонних конфіденційних документів або по мітках секретності. Продукти різних виробників донедавна використовували один з цих методів, проте останнім часом ведуться розробки комплексного механізму контролю конфіденційності, який використовував би кілька перерахованих методів.

Шифрування. Захист даних від витоків так чи інакше використовує механізми шифрування. Слід зазначити, що шифрувати потрібно не тільки самі бази ПДн, але і їх передачу по мережі, а також резервні копії баз даних. Можна використовувати механізми шифрування, вбудовані в бази даних, однак для їх законного застосування потрібно інтегрувати в них українські алгоритми шифрування. Отож, для захисту ПДн можна шифрувати цілі розділи файлової системи, які використовуються для зберігання данних. Шифрування використовується і при передачі ПДн по мережі в розподіленій системі. З цією метою можна застосовувати пропоновані різними розробниками продукти класу VPN, які, як правило, базуються на шифруванні, проте подібні системи повинні бути сертифіковані і тісно інтегровані з базами даних, в яких зберігаються ПДн.

Всі ці заходи запобігають витоку в тому числі і ПДн, хоча їх можна використовувати і для захисту іншого критичної для компанії інформації, проте слід пам'ятати, що для найкращого захисту потрібно користуватися сертифікованими засобами захисту.

Управління правами доступу. У великій ІС головною проблемою для адміністратора є правильна організація доступу співробітників до різних ресурсів - від коректного налаштування прав доступу часто залежить збереження конфіденційних і ПДн, тому система управління правами доступу повинна бути включена в систему захисту великої ІС. Така система зазвичай дозволяє ввести рольове управління правами доступу і контролює дотримання цих прав. Система також блокує спроби змінити права доступу без дозволу адміністратора безпеки, що забезпечує захист від локальних адміністраторів. Типовими представниками цього сімейства продуктів є Oracle IAM і IBM Tivoli Access Manager . Слід зазначити , що методика захисту ПДн передбачає управління правами доступу в системах будь-яких розмірів, що обробляють таку інформацію.

Далі потрібно сказати про розробку політики безпеки інформації в ІТС. Розробка політики безпеки інформації в ІТС обов'язково виконується на основі [14], та включає в себе такі основні пункти:

1. Вивчення об'єкта, на якому створюється КСЗІ, проведення науково-дослідних робіт.

На цьому етапі розробник КСЗІ проводить детальне вивчення об'єкта, на якому створюється КСЗІ, уточнює моделі загроз, потенційного порушника та результати аналізу можливості керування ризиками, які виконані на попередніх етапах, а також виконує у разі необхідності додаткові науково-дослідні роботи, пов'язані з пошуком шляхів реалізації завдання на створення КСЗІ, оформлює і затверджує звіти з науково-дослідної роботи, що виконувалися.

2. Вибір варіанту КСЗІ

У загальному випадку за результатами робіт попереднього етапу готуються альтернативні варіанти концепції створення КСЗІ і планів їх реалізації, здійснюється оцінка переваг і недоліків кожного варіанту, вибір найбільш оптимального варіанту. Концепція оформлюється у вигляді звіту.

3. Оформлення політики безпеки

3.1. На цьому етапі здійснюється:

вибір основних рішень з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, рекомендацій і т.п., які регламентують використання захищених технологій обробки інформації в ІТС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій;

документальне оформлення політики безпеки інформації.

3.2. Політика безпеки може розроблятись для ІТС в цілому або, якщо мають місце особливості функціонування окремих компонентів КСЗІ, для окремої компоненти, для окремої функціональної задачі, для окремої технології обробки інформації тощо.

3.3. Політика безпеки розробляється згідно з положеннями [13], та рекомендаціями [15].

2.3. Вітчизняний досвід у сфері захисту персональних даних

При оцінці та аналізі чинників підвищення ефективності системи управління захистом ПДн, перш за все потрібно проаналізувати кроки, які реалізує банк для захисту ПДн за як в Україні, так і за її межами.

Що стосується сучасного стану СЗПДн в Україні, то ситуація тут склалася наступним чином. Банк, за законом, при обробці ПДн зобов'язаний приймати необхідні організаційні та технічні заходи або забезпечувати їх прийняття для захисту ПДн від неправомірного або випадкового доступу до них, знищення, зміни, блокування, копіювання, надання, розповсюдження ПДн, а також від інших неправомірних дій відносно ПДн. Всі ці роботи можуть виконуватись на замовлення різних банків. Компанія, котра має досвід побудови комплексної СЗПДн відповідно до вимог законодавства, а також подальший супровід і гарантію на виконані роботи, може з легкістю вирішити дане завдання.

У процес створення КСЗІ залучаються такі сторони:

організація, для якої здійснюється побудова КСЗІ (Замовник);

організація, що здійснює заходи з побудови КСЗІ (Виконавець);

Державна служба спеціального зв’язку та захисту інформації України (Контролюючий орган);

організація, що здійснює державну експертизу КСЗІ (Організатор експертизи).

Об'єктом захисту КСЗІ є інформація, в будь-якому її вигляді і формі подання. Матеріальними носіями інформації є сигнали. По своїй фізичній природі інформаційні сигнали можна розділити на такі види: електричні, електромагнітні, акустичні, а також їх комбінації.

Сигнали можуть бути представлені у формі електромагнітних, механічних та інших видах коливань, причому інформація, яка підлягає захисту, міститься в їх змінних параметрах. Залежно від природи, інформаційні сигнали поширюються в певних фізичних середовищах. Середовища можуть бути газовими, рідинними і твердими. Наприклад, повітряний простір,

конструкції будівель, з'єднувальні лінії і струмопровідні елементи, грунт та інші.

Необхідність побудови КСЗІ визначається вимогами нормативних документів чи бажанням власника інформаційних ресурсів.

Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах»:

інформація, яка є власністю держави, або інформація з обмеженим доступом повинна бути захищена шляхом побудови КСЗІ, з отриманням «Атестата відповідності», який видається ДССЗЗІ;

інша інформація може бути захищена за допомогою КСЗІ за бажанням її власника.

Після прийняття Замовником рішення про створення КСЗІ між Замовником та Виконавцем підписується договір про створення КСЗІ, в якому мають бути описані порядок і терміни виконання, а також вартість робіт.

В результаті виконання даних робіт реалізується повний комплекс організаційно-технічних заходів щодо забезпечення захисту всієї конфіденційної інформації організації замовника послуг, в тому числі ПДн.

При створенні комплексної СЗПДн фахівцями фірми, яка виконує замовлення будуть проведені наступні етапи робіт [38]:

Проведення обстеження та отримання первинних даних необхідних для розробки системи захисту.

Оцінка ризиків і загроз для інформації, розробка моделі загроз і моделі порушника.

Проектування системи захисту, розробка технічного завдання, плану захисту та інших нормативно-технічних і організаційних документів.

Закупівля та впровадження засобів захисту, конфігурація наявних механізмів безпеки, проведення дослідної експлуатації.

Проведення експертних випробувань.

Підтримка та супровід створеної системи.

Під час створення комплексної СЗПДн, компанії, котрі її створюють надають консультаційні послуги з реєстрації баз ПДн, розробку внутрішніх інструкцій, положень і регламентів, а також навчальний семінар для співробітників компанії про порядок обробки та захисту ПДн. Під час проведення робіт зі створення системи захисту фірма, яка виконує замовлення обов'язково повинна врахувати як українські нормативні документи в галузі технічного та криптографічного захисту інформації, так і міжнародні та національні стандарти в галузі ІБ.

Основними результатами розробки та впровадження СЗПДн, в організації замовника, будуть:

Забезпечення захисту інформації з обмеженим доступом, у тому числі ПДн та іншої конфіденційної інформації організації.

Забезпечення повної відповідності вимогам законодавства і контролюючих органів.

Захист від навмисної або випадкової витоку інформації з обмеженим доступом.

Захист від сучасних інформаційних загроз.

Удосконалення технологій обробки інформації.

Особливою потребою для захисту ПДн в банку є кодування даних з метою унеможливлювання його прочитання зловмисниками. Кодування інформації - це подання повідомлень в конкретному виді за допомогою деякої послідовності знаків. Правило відображення одного набору знаків в інший називається кодом. Спосіб представлення інформації за допомогою двох символів - 0 і 1 називають двійковий код.

Для поліпшення якості передачі дискретних повідомлень в лініях зв'язку, зокрема, в локальних обчислювальних мережах, використовуються різні способи перетворення двійкових сигналів (методи кодування). В результаті чого сигнал стає менш вразливий до таких ефектів погіршення якості передачі, як шум, перешкоди і завмирання.

При передачі дискретної інформації в лініях зв'язку до сигналів передачі пред'являються певні вимоги:

1. Збільшення відношення сигнал/шум;

2. Підвищення швидкості передачі даних;

3. Забезпечення низької вартості реалізації , тобто процес кодування і декодування повинен бути досить простим , що дозволить зменшити вартість обладнання.

При передачі даних в лінії зв'язку використовують дворівневі і багаторівневі канальні коди. Самий найпростіший дворівневий код - це код NRZ (Non Return to Zero - без повернення до нуля), що представляє собою звичайний цифровий сигнал, має два стани (+1, -1), які безпосередньо відображають значення бітів.

Найпростіший трирівневий код - це код RZ (Return to Zero - з поверненням до нуля) або, як його ще називають, біполярний імпульсний код, що забезпечує повернення до нульового рівня після значущого рівня сигналу в першій половині переданого біта інформації.

Також великою популярністю користується манчестерський код. Манчестерський код (або код Манчестер–II) - це код, який самосинхронізується. Манчестерське кодування широко використовується для передачі інформації, як по електричним, так і по оптоволоконним кабелях. Найбільшого поширення манчестерський код отримав в локальних обчислювальних мережах. Зокрема, він застосовується в технологіях Ethernet і Token Ring.

Є ще питання, які можуть виникнути в процесі побудови захисту КС. Тому в процесі побудови надійного захисту в КС необхідно спиратися на [13], який визначає методологічні основи (концепцію) вирішення завдань захисту інформації в КС.

Основними завданнями засобів захисту є ізоляція об'єктів КС всередині сфери керування, перевірка всіх запитів доступу до об'єктів і реєстрація запитів і результатів їх перевірки і/або виконання. З одного боку, будь-яка елементарна

функція будь-якої з послуг, що реалізуються засобами захисту, може бути віднесена до функцій ізоляції, перевірки або реєстрації. З іншого боку, будь-яка з функцій, що реалізуються засобами захисту, може бути віднесена до функцій забезпечення конфіденційності, цілісності і доступності інформації або керованості КС і спостереженості дій користувачів.

2.4. Зарубіжний досвід у сфері захисту персональних даних

При проведенні аналізу нормативної бази, зокрема [16] у сфері захисту банківських даних, можна зробити висновок, що при розробці своїх законів та стандартів інші держави спираються на існуючі європейські та міжнародні стандарти, при цьому детально аналізуючи результати ефективності впровадження їх за кордоном. Так, у зв'язку зі специфікою банківської діяльності обробка ПДн в ІС банку нерозривно пов'язана з захистом банківською таємницею. Усі працівники банку зобов’язані зберігати таємницю про операції, рахунки і вклади, інших ПДн його клієнтів і кореспондентів, а також про інші відомості, встановлених банком, якщо це не суперечить чинному законодавству. Винні у порушенні встановлених банком вимог, несуть відповідальність. Відповідальність за дотримання режиму захисту ПДн стосовно ПДн, що знаходяться у співробітників на персональних комп'ютерах і в документарній формі, несуть дані співробітники.

Вибір і реалізація методів і способів захисту інформації в ІС банку здійснюється відповідно до рекомендацій регуляторів у галузі захисту інформації з урахуванням визначених банком загроз безпеки ПДн (моделі загроз) і залежно від класу ІС.

У Європі питаннями захисту ПДн всерйоз почали займатися з 1980 р., коли ОЕСР випустила рекомендації щодо захисту конфіденційності особистості та транскордонному обміні ПДн. На сьогоднішній день, європейське право в галузі захисту ПДн пройшло довгий шлях становлення та модернізації. У результаті вийшов цілком прагматичний підхід: європейське право захищає ті

об’єкти і суб'єкти, яким ця захист необхідна, і рівно настільки, наскільки цей захист економічно виправдана. Така концепція виявилася вкрай ефективною: заходи щодо захисту систем обробки ПДн не здаються надмірними і, що найголовніше, є вельми дієвими. Згідно з соціологічними дослідженнями, 80 % європейських операторів та суб'єктів ПДн вважають себе захищеними. Великобританія є одним з лідерів у цій галузі і 2 липня 2009 року випустила першу редакцію [24]. Цей документ став першим в світі стандартом з СУПДн і дозволяє отримати уявлення про організацію захисту ПДн.

Висновки до розділу 2

За результатами виконання другого розділу можна зробити наступні висновки.

При детальному аналізі основних видів загроз ПДн в банківській сфері, ми визначити:

за направленістю і характером впливу на банки загрози можуть бути економічними, фізичними та інтелектуальними;

дії, що призвели до порушення ІБ поділяються на НСД, розголошення і витік інформації.

Найголовніше в функціонуванні СЗПДн є надійний безперебійний захист від всіх впливів навколишнього та внутрішнього середовища, котрі несуть в собі загрозу для надійної роботи даної системи. Тому потрібно, щоб в організацій була своя служба безпеки.

Щодо комплексності захисту, то треба обов’язково використовувати організаційні, технічні та правові заходи і засоби. При побудові КСЗІ використовують такі основні підсистеми:

підсистема антивірусного захисту;

розмежування доступу, що забезпечує захист від НСД до ПДн;

криптографічний захист;

міжмережеве екранування;

виявлення вторгнень, яка призначена для виявлення і блокування мережевих атак в ІС;

аналіз вразливостей.

Треба сказати, що кожен проект по захисту ПДн є по-своєму унікальним, оскільки завжди враховує особливості бізнес-процесів організацій, а також тих ІС, за допомогою яких вони реалізовані. Крім цього, своя специфіка також є у банків та операторів зв'язку, оскільки для захисту інформації в цих організаціях можна застосовувати відповідні галузеві стандарти.

При проведенні аналізу нормативної бази РФ, зокрема [16] у сфері захисту банківських даних, можна зробити висновок, що Росія при розробці своїх законів та стандартів тісно спирається на існуючі європейські та міжнародні стандарти, при цьому детально аналізуючи результати ефективності впровадження їх за кордоном. В Росії у зв'язку зі специфікою банківської діяльності обробка ПДн в ІС банку нерозривно пов'язана з захистом банківською таємницею.

У Європі питаннями захисту ПДн всерйоз почали займатися з 1980 р., коли ОЕСР випустила рекомендації щодо захисту конфіденційності особистості та транскордонному обміні ПДн. І зараз згідно з соціологічними дослідженнями, 80 % європейських операторів та суб'єктів ПДн вважають себе захищеними. Великобританія є одним з лідерів у цій галузі і 2 липня 2009 року випустила першу редакцію [24]. Цей документ став першим в світі стандартом з СУПДн і дозволяє отримати уявлення про організацію захисту ПДн.

Реалізація вимог українського законодавства щодо захисту ПДн є необхідною, але недостатньою умовою для забезпечення високого рівня реальної захищеності системи. Необхідно розуміти, що навіть атестована система захисту може бути потенційно зламана, якщо в рамках проекту був використаний формальний підхід, що передбачає реалізацію виключно тих вимог, які викладені в нормативних документах регуляторів.

Тому система захисту інформації повинна постійно супроводжуватися і вдосконалюватися в рамках процесної моделі управління ІБ. Це передбачає

адміністрування засобів захисту інформації, актуалізацію документів, що регламентують питання захисту, проведення періодичного аудиту захищеності і т.д.

Реальна захищеність системи захисту інформації ПДн можлива тільки при комплексному підході, який враховував би не тільки вимоги українського законодавства, а й рекомендації міжнародних стандартів.

Розділ 3
РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИСТЕМИ УПРАВЛІННЯ ЗАХИСТОМ ПЕРСОНАЛЬНИХ ДАНИХ КЛІЄНТІВ БАНКУ

3.1. Рекомендації щодо удосконалення системи управління захистом персональних даних клієнтів банку

При розробці рекомендацій щодо підвищення ефективності СЗПДн клієнтів банку бажано було б розробити свою послідовність, завдяки якій можна буде крок за кроком впроваджувати СЗПДн. Адже саме створення і надійне функціонування СЗПДн полягає не в купівлі і впровадженні передових технологій, а в послідовній побудові цієї системи, котра буде спиратися на діючі міжнародні, державні і галузеві нормативні акти.

Потрібно наголосити, що для будь-якої компанії дуже важливо гроші на захист інформації вкладати обґрунтовано. У ІБ відомий принцип розумної достатності, який свідчить про таке: «створення 100 % надійної системи захисту інформації неможливо в принципі, в будь-яких випадках залишається ненульова можливість реалізації якої загрози або вразливості». Будь-яка система захисту інформації може бути зламана, це питання тільки часу і витрачених зловмисником коштів.

Зараз в Україні діє [1], який повністю повторює вимоги [24] до захисту ПДн. Якщо всі ці умови дотримані, то можна приступити до створення СЗПДн на підприємстві.

Створення такої системи дозволило б реально і адекватно захистити ПДн на підприємстві або в організації шляхом створення:

юридично обґрунтованою внутрішньої документації, яка дозволяє розмежувати відповідальність між посадовими особами та виконавцями, які безпосередньо використовують ПДн в повсякденній діяльності;

процесів обробки, зберігання, передачі та знищення ПДн на підприємстві і в ІС зокрема;

дієвих заходів захисту ПДн відповідно до ризиків на конкретному підприємстві (або в ІС).

Пропонована нами модель системи захисту (і обробки) ПДн дозволить :

задовольнити вимоги [1];

реалізувати процеси обробки та обміну ПДн з урахуванням особливостей бізнес-процесів конкретної компанії;

розрахувати і впровадити достатні та адекватні ризикам заходи щодо захисту ПДн.

Етапи впровадження СЗПДн [Творча розробка]:

1) Інвентаризація та підготовчі дій до впровадження СЗПДн

Вивчення стандартів (міжнародних, державних, галузевих) фахівцями ІБ;

Проведення інвентаризації всіх ПДн (Саме цей крок допоможе чітко структурувати всі ПДн, які обробляються у компанії. Результати інвентаризації повинні бути оформлені документально і описувати повний перелік ПДн, оброблюваних в організації, а також перелік підрозділів і співробітників, допущених до обробки таких даних.);

Інвентаризація баз ПДн (Потрібне документальне описання і фіксування кожної бази, в якій обробляються ПДн. При цьому потрібно обов'язково описувати весь життєвий цикл ПДн: як вони з’являються в базах, як зберігаються, для чого використовуються і як видаляються).

2) Визначення поточного стану СЗПДн

Визначення рівня зрілості організації в області ІБ (основна мета якого полягає у визначенні реального стану організації для подальшого розвитку і підвищення до п’ятого рівня);

Підвищення кваліфікації та перепідготовка фахівців в ІБ;

Підготовка звіту, щодо подальшого напрямку розвитку СЗПДн в організації.

3) Визначення заходів захисту ПДн

Розробка регламентної документації.

Проектування майбутньої СЗПДн (Цей крок є дуже важливий.)

Для захисту ПДн повинні бути використані тільки сертифіковані засоби захисту інформації. В більшості випадків використовуються:

Засоби захисту від несанкціонованого доступу;

Засоби антивірусного захисту;

Засоби міжмережевої екранування.

Рідше потрібні:

Системи виявлення/запобігання вторгнень;

Системи контролю захищеності;

Засоби криптографічного захисту.

4) Впровадження СЗПДн

Впровадження технічних засобів захисту інформації (Цей етап передбачає переведення у промислову експлуатацію систему. Саме на даному етапі проводиться закупівля і установка засобів захисту інформації, а також розробка експлуатаційної документації.);

Ознайомлення персоналу з політикою ІБ та інструкціями щодо забезпечення ІБ.

Атестація системи (якщо потрібно).

Реєстрація баз у Держреєстрі.

Отож, створення СЗПДн на підприємстві слід починати з підготовки внутрішньої нормативно-правової бази та ідентифікації баз ПДн та самих ПДн. Метою побудови СЗПДн є запобігання або зниження шкоди через втрати внаслідок реалізації загроз ПДн та іншій цінній інформації банку, що захищається. Завдання СЗПДн полягають у своєчасному виявленні, усуненні загроз ПДн та створенні механізму та умов оперативного реагування на загрози безпеки в різних ситуаціях їх прояву.

Фундаментом для майбутньої системи буде політика обробки ПДн на підприємстві. Цей етап є вкрай важливим, адже правильно створена політика буде гарантувати, що майбутня система буде відповідати вимогам закону, ПДн

в ній будуть відповідати всім необхідним вимогам, а також підтримувати цілі організації в області обробки ПДн.

Оскільки жодна система не може обійтися без управління, то на цьому етапі потрібно розподілити ролі і відповідальність. Тому один з представників менеджменту компанії призначається відповідальним за СЗПДн. Його основні обов'язки: затвердження нормативних документів (політик, інструкцій) на рівні правління, розробка та реалізація їх положень, управління безпекою та ризиками відносно ПДн, виділення необхідної кількості ресурсів. Відповідальними за функціонування СЗПДн визначають посадових осіб, які найбільш часто використовують ПДн за родом діяльності. У їх обов'язки, як правило, входить:

моніторинг інцидентів, пов'язаних з усією системою;

юридичні аспекти (законність обробки і зберігання ПДн, контроль змін в законодавстві та впровадження відповідних змін в систему);

розробка та аналіз ефективності нормативних документів, що регламентують роботу з ПДн на підприємстві;

проведення навчання, тренінгів для персоналу та інших заходів з безпеки ПДн.

До підбору відповідальних необхідно підходити з особливою ретельністю, адже збереження ПДн більшою мірою лягає на їхні плечі.

Після побудови системи захисту керівництво компанії і відповідальні за обробку ПДн повинні зареєструвати бази ПДн підприємства у Державному Реєстрі баз ПДн, як того вимагає законодавство України [26].

Коли система вже створена і функціонує, виникає питання її підтримки. Тому ми рекомендуємо проводити два види аудиту СЗПДн. Перший - це звичайний аудит, його головними цілями є визначення відповідності реальних процесів нормативним документам і вимогам законодавства. Другий вид аудиту - це аудит з боку правління компанії. Він проводиться з певними інтервалами часу або при значних змінах (у системі, бізнес-процесах або законодавстві). Він базується на звітах зовнішніх або внутрішніх аудиторів,

звітах про перегляд процедур, виявлених ризиках або при серйозних інциденти пов'язаних з системою. Метою такого аудиту є потенційні зміни в системі (політиці, процедурах, технологіях) для задоволення вимог закону та готовності до можливих інспекціям з боку Уповноваженого ВРУ з прав людини.

Зараз існують ряд підходів, що дозволяють забезпечити захист ПДн відповідно до пред'явлених вимог за ціною розумних витрат.

При проектуванні нових систем потрібно застосовувати програмне забезпечення з вбудованими сертифікованими засобами захисту, що пройшло сертифікацію за вимогами безпеки інформації. Це дозволить надалі заощадити на закупівлі засобів захисту та навчанні персоналу.

Також слід визначитися з тим, хто буде забезпечувати безпеку ПДн. Для великих організацій, що мають власну службу безпеки і набір необхідних ліцензій, кращим буде самостійна побудова та супроводження системи захисту інформації. У той же час, для більшості дрібних і середніх компаній оптимальним варіантом є укладення договору зі сторонніми спеціалізованими організаціями на розробку та впровадження системи захисту і подальший аутсорсинг забезпечення ІБ. Такий підхід дозволяє як скоротити витрати на навчання та утримання штатного персоналу, так і перекласти більшість ризиків, пов'язаних з безпекою інформації.

Якщо розглядати захист ПДн з боку застосування програмно-технічних засобів захисту, то тут можна виділити спеціалізовані системи моніторингу подій ІБ.

Одним із прикладів подібних систем є продукт ArcSight ESM. ArcSight ESM - це провідна платформа на ринку для моніторингу корпоративних загроз і ризиків безпеки, яка займає одну з лідируючих позицій в даній області.

Цей продукт стане в нагоді:

службі інформаційного контролю та аудиту (коли необхідно отримати задовільну оцінку аудиту);

службі ІБ (коли необхідно визначити хто хоче отримати доступ до інформації, і чи є у цієї особи відповідні повноваження);

службі IT (коли інфраструктура повинна відповідати вимогам затвердженої політики і ми повинні швидко реагувати на нові загрози).

Рішення ArcSight ESM надає широкий спектр функцій, які забезпечують швидкий і зручний доступ до необхідної інформації.

Сьогодні також є ще одна дуже цікава послуга в галузі захисту інформації - тест на проникнення. Тест на проникнення (penetration test або скорочено pentest) - це практичний спосіб показати, наскільки захищена компанія від зазіхань на її конфіденційні дані і інших загроз для інформації. Даний метод симулює набір «хакерських» атак, цілі яких - проникнення у внутрішню інфраструктуру мережі компанії, крадіжка та / або модифікація конфіденційних даних, порушення роботи критичних бізнес процесів компанії. Кожен банк може перевірити свою систему безпеки на надійність і, виходячи з результатів цієї перевірки, вживати необхідних заходів. Ця послуга являє собою імітацію послідовності дій зломщика щодо здійснення несанкціонованого проникнення в ІС замовника.

Також ми вирішили показати майбутні напрямки розвитку захисту СУПДн на прикладі інтернет-банкінгу. Багато хто зараз вважають, що використання інтернет-банкінгу на сьогодні є достатньо надійним і безпечним засобом обслуговування клієнтів.

Наприклад, крім здешевлення транзакцій інтернет-банкінг дозволяє:

залучити нових клієнтів. Тепер це можуть бути жителі інших областей, віддалених на тисячі кілометрів від найближчого відділення банку;

утримати старих клієнтів. Переїжджаючи на нове місце , клієнт відривається від старого банку, якщо він управляє рахунком по телефону або модему. Завдяки інтернету створюється враження, що нічого не сталося - банк залишився на місці, тому переважна більшість клієнтів залишаються зі своїм старим банком і після переїзду;

заохочувати найбільш вигідних клієнтів. Якщо клієнт керує рахунком по інтернету, всі його дії можна зафіксувати, встановити карту його переваг і відповідно до цього будувати індивідуальну політику банку.

Оскільки інтернет-банкінг вигідний, то створюються нові банки, що працюють тільки в інтернеті, не мають ні власних будівель, ні філій, ні банкоматів. Такі банки можуть запропонувати своїм клієнтам більш вигідні, ніж у звичайних банках, умови, наприклад , менші відсотки по кредиту або вищі виплати за депозитними вкладами. Однак чим простіше доступ до інтернету, тим складніше забезпечити її ІБ, так що користувач може навіть і не дізнатися, що у нього були скопійовані логін і пароль.

Отож, платою за користування Internet є загальне зниження ІБ. Зараз безпека даних є однією з головних проблем в інтернеті. З'являються відомості про те, як комп'ютерні злодії, що використовують усе більш витончені прийоми, проникають у чужі бази даних або отримують доступ в архівів комерційних даних.

У банківській сфері проблема безпеки інформації ускладнюється двома факторами:

по-перше, майже всі цінності, з якими має справу банк (крім готівки), існують лише у вигляді тієї чи іншої інформації.

по-друге, банк не може існувати без зв'язків із зовнішнім світом: без клієнтів і т.п.

Отже, існують наступні шляхи вирішення даної проблеми.

При роботі в мережі інтернет на перше місце виходить міжмережевий екран або брандмауер. Брандмауер – невід'ємна частина системи захисту, без якої неможлива розробка її політики. Брандмауер дозволяє значно знизити число ефективних зовнішніх атак на корпоративну мережу або персональний комп'ютер, НСД до мережі організації з боку віддалених і передавальних серверів, включених в мережу інтернет, знизити ймовірність збору та моніторингу мережевої інформації в інтересах третіх осіб, блокувати доступ непотрібної і шкідливої інформації в систему;

Використання VPN технології, алгоритмів криптозахисту (електронного підпису, стиснення з паролем, шифрування), дозволяє знизити втрати від несанкціонованого програмно-апаратного доступу до інформації, що

знаходиться в каналі зв'язку інтернет, збирання і моніторинг інформації в інтересах третіх осіб;

Дублювання каналу інтернет і стиснення інформації дозволяє підвищити надійність системи в разі відмови, перевантаження каналу зв’язку і в разі стихійних лих;

Використання антивірусних засобів, не без підстав, вважається необхідною умовою при підключенні до інтернет, дозволяє значно знизити втрати інформації в результаті зараження шкідливими програмами;

Використання автоматизованих засобів перевірки мережі на можливі вразливості в системі захисту та аудиту безпеки корпоративних серверів дозволяє встановити джерела загроз і значно знизити ймовірність ефективних атак на корпоративну мережу або персональний комп’ютер;

Використання маршрутизаторів і надійних постачальників мережевих послуг, дозволяють скоротити потік непотрібної і шкідливої інформації в систему.

Ну і на кінець необхідно звернути увагу банку на особливо гостру проблему підбору висококваліфікованих кадрів. Слід наголосити, що ключовим фактором, у забезпеченні ІБ підприємства є його персонал, основними заходами при роботі з яким є:

проведення аналітичних процедур при прийомі і звільненні; навчання і інструктаж практичним діям по захисту інформації;

контроль за виконанням вимог по захисту інформації, стимулювання відповідального відношення до збереження інформації та ін.

Часто банки нехтують самим головним – безпекою і стабільністю через економію коштів чи некомпетентність. Все це може вилитися в великі проблеми пов’язані з витоком важливої інформації банку конкурентам або злочинцям, котрі мають на меті підірвати довіру клієнтів до даного банку. Щоб такого не трапилося, потрібно ставити жорсткі вимоги до підбору персоналу, який працює з ПДн, розголошення яких може завдати непоправної шкоди банку та

відповідально ставитися до підбору засобів і заходів захисту ПДн клієнтів банку.

Не менш важливим є питання економічного обґрунтування витрат на захист інформації. Адже чим вище рівень захищеності інформації, тим за інших рівних умов, буде нижче розмір можливих збитків, але тим вищою буде вартість захисту. Оптимальний розміром витрат на захист буде такий, при якому забезпечується рівень захищеності, що дорівнює мінімуму загальних витрат. Вартість збитків визначається двома параметрами: ймовірністю реалізації різних загроз інформації; вартістю (важливістю) інформації, захищеність якої може бути порушена під впливом різних загроз.

ІБ банку на практиці включає сукупність напрямів, методів, засобів і заходів, що знижують вразливість інформації і перешкоджають несанкціонованому доступу до інформації, її розголошенню або витоку. Як вже зазначалося вище, елементами цієї системи є: правовий, організаційний, технічний захист інформації, а основною її характеристикою - комплексність. Структура системи, склад і зміст елементів, їх взаємозв’язок залежать від об'єму і цінності інформації, що захищається, характеру можливих загроз безпеки інформації, необхідної надійності захисту і вартості системи.

Тому для успішного вирішення цього завдання банкам потрібно завжди бути в курсі останніх новинок захисту (як технічних, так і законодавчих) своїх даних і ПДн своїх клієнтів, оскільки останнім часом атаки на банки для заволодіння базами даних стають все більш небезпечними.

3.2. Економічне обґрунтування вибраних методів покращення захисту персональних даних клієнтів банку

Тепер економічно обґрунтуємо декілька наших пропозицій щодо підвищення ефективності функціонування КСЗІ. Одною із основних проблем при створенні КСЗІ є прийняття рішення щодо того, кому краще довірити впровадження захисту ПДн. Тут потрібно зазначити, що роботи по захисту ПДн

є досить численні і потребують багато сил, знань і часу на їх виконання. Саме тому багато консалтингові компанії пропонують свою допомогу в даному питанні.

На даний час є три підходи до проведення робіт по захисту ПДн [творча розробка]:

1. Всі роботи проводяться організацією самостійно. Цей варіант потребує наявності навчених і сертифікованих фахівців в області захисту ПДн та отримання ліцензій. Потрібно також взяти до уваги, що якщо подібний проект ми впроваджуємо вперше, це означає, що нам доведеться зіткнутися з недосконалістю і протиріччям законодавства у сфері захисту ПДн та ІБ, ознайомитися з масою регламентуючих документів різних відомств.

Навіть вивчивши ці документи та нормативно-правові акти, відсутність досвіду проектування і впровадження подібних систем ускладнює завдання вибору всіх елементів рішення складових системи захисту інформації. Це справедливо як в частині вибору технічних засобів, так і в частині підготовки СЗПДн до атестації. При цьому існує ризик неправильно оцінити і класифікувати загрози безпеки, неправильно вибрати клас захисту тощо, що, в свою чергу, може привести або до завищення вартості системи захисту, або до виявлення порушень з боку регуляторів, які вимагатимуть їх усунення та підвищення класу захисту. Серйозна переробка проекту може виявитися істотно дорожче побудови системи «з нуля». Середньому та малому бізнесу цей варіант не прийнятний. А от великим компаніям цей варіант найбільш доцільний через наявність сертифікованих фахівців в області захисту ПДн.

2. Всі роботи виконує стороння організація. Даний підхід є дуже витратним для організації, але дозволяє в необхідні терміни привести систему захисту в належний вигляд. Основне завдання як замовника - правильно вибрати партнера-виконавця.

Критерії вибору [37]:

Позитивний досвід в області побудови систем ІБ.

Наявність ліцензій на здійснення діяльності щодо захисту ПДн та забезпечення ІБ.

Наявність досвідчених кваліфікованих фахівців, яких необхідно залучати для участі в проекті.

Адекватність параметрів комерційної пропозиції (ціни, терміни та інше).

Правовий супровід кваліфікованих юристів з досвідом роботи в галузі ІБ та взаємодії з силовими структурами.

3. Експертний консалтинг. При цьому підході всі роботи проводяться фахівцями організації котра його замовила, а фахівець сторонньої організації здійснює лише управління проектом і проводить експертизу розроблених документів.

Далі зробимо порівняння цих підходів. Припустимо, ми володіємо малою організацією. Вартість побудови КСЗІ показана в таблиці 3.1.

Таблиця 3.1

Підходи до проведення робіт по захисту ПДн та їхня вартість

Підходи до проведення робіт по захисту ПДн	Загальна вартість робіт з урахуванням побудови КСЗІ
Всі роботи проводяться організацією самостійно.	18000000 - 22000000 грн.
Всі роботи виконує стороння організація.	1000000 грн
Експертний консалтинг.	6500000 грн.

Тепер проаналізую в таблиці 3.2. кожен з підходів до проведення робіт по захисту ПДн з розміром організації.

Отож, як ми можемо бачити, найкращим варіантом для малої та середньої організації буде вибір експертного консалтингу, оскільки це знижує фінансове навантаження на організацію, котра замовила дані послуги, а також дозволяє її фахівцям отримати необхідних досвід в області побудови надійного комплексного захисту.

Таблиця 3.2

Характеристика зіставлення підходів до проведення робіт по захисту ПДн з розмірами організації.

Підходи до проведення робіт по захисту ПДн	Розмір організації		
	Малий	Середній	Великий
Всі роботи проводяться організацією самостійно.	Не є вигідним. Надзвичайно витратний через відсутність навчених фахівців в області захисту ПДн	Не є вигідним. Надзвичайно витратний через відсутність навчених фахівців в області захисту ПДн.	Є вигідним. Найбільш доцільний через наявність навчених і сертифікованих фахівців в області захисту ПДн.
Всі роботи виконує стороння організація.	Дуже витратний для організації. Але дозволяє в необхідні терміни привести систему захисту в належний вигляд. Основне завдання замовника - правильно вибрати виконавця.	Дуже витратний для організації. Але дозволяє в необхідні терміни привести систему захисту в належний вигляд. Основне завдання замовника - правильно вибрати виконавця.	Не є вигідним. Витратний для організації. Може мати місце витік інформації від організації-виконавця, котра будувала КСЗІ.
Експертний консалтинг.	Є дуже вигідним. Малі витрати з боку організації, отримання досвіду працівниками організації.	Є дуже вигідним. Малі витрати з боку організації, отримання досвіду працівниками організації.	Є плюси і мінуси. Малі витрати з боку організації. Отримання нового досвіду в побудові КСЗІ. Може мати місце витік інформації від фахівця сторонньої організації, котрий здійснює управління проектом і проводить експертизу розроблених документів.

На мій погляд, це найбільш потрібний на ринку вид надання послуг. Але поки лише невелика кількість компаній на ринку банківської безпеки готові надавати висококваліфіковані консалтингові послуги. Щодо великих організацій, то для них найбільш вигідним є побудова КСЗІ власними силами через наявність навчених і сертифікованих фахівців в області захисту ПДн. Також вибір такого підходу мінімізує витік інформації про деталі складових цієї КСЗІ.

Тепер проведу економічну оцінку доцільності застосування заходів захисту. Величина вигоди може мати як позитивне, так і негативне значення. У першому випадку це означає, що використання системи захисту приносить нам очевидний виграш, а в другому - лише додаткові витрати на забезпечення власної безпеки.

Далі розглянемо засоби захисту інформації досліджуваного нами банку. Склад КСЗІ досліджуваного банку зображено на рисунку 3.1.

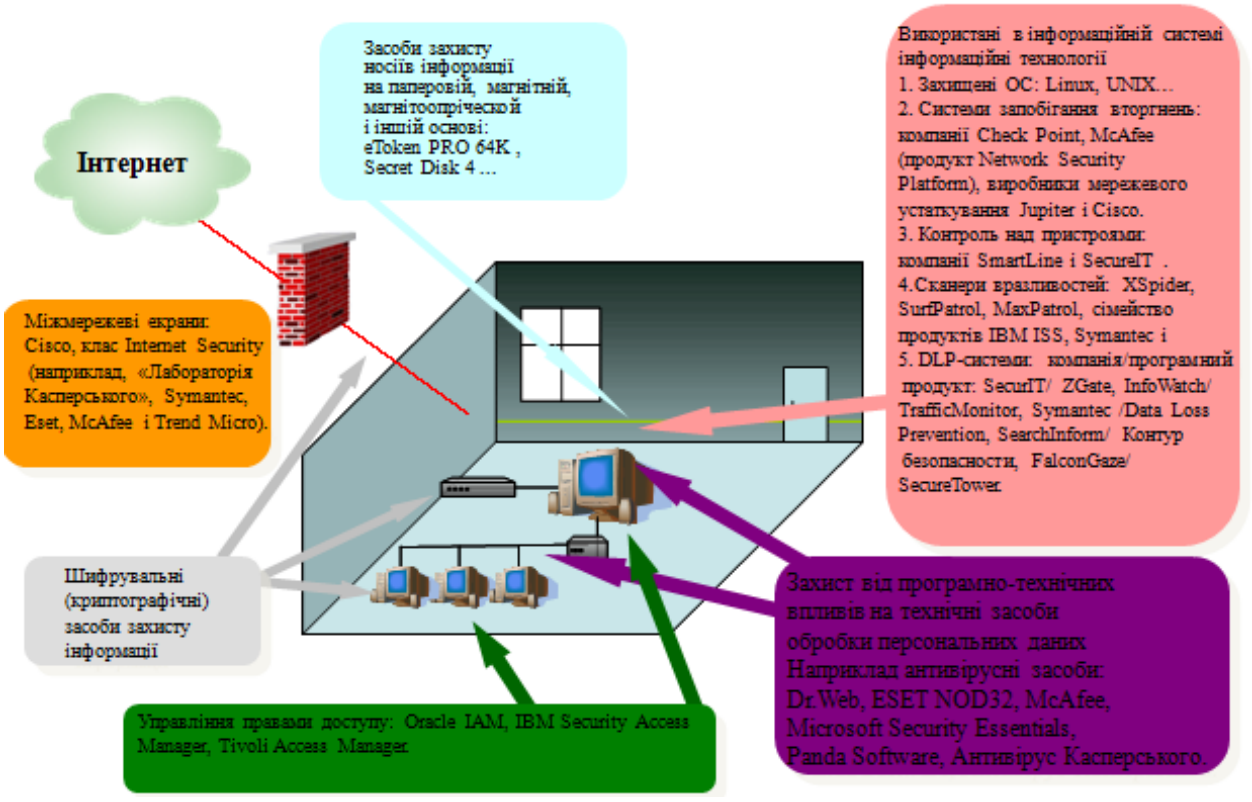

Рис 3.1.Склад КСЗІ

Оціню вигоду від захисту інформації від НСД, розголошення або витоку ПДн на протязі одного року, шести місяців, одного місяця. В таблиці 3.3 показано статистику частоти загроз ПДн.

Таблиця 3.3

Статистика частоти загроз ПДн.

Події, котрі порушують цілісність ПДн	Частота настання загрози			
	В процентах	12 місяців	6 місяців	1 місяць
НСД	60 %	8	4	0,7
Розголошення	20 %	3	1,5	0,25
Витік	20 %	1	0,5	0,08
Сумарна кількість, Р	100 %	12	6	1

Припустимо, аналіз показав, що в середньому ситуація з НСД зустрічається вісім разів на рік, розголошення – 3 рази, витік – 1 раз. Тобто сумарна кількість всіх загроз для ПДн прямопропорційна 12 разів на рік.

$Р_{12\ місяців}$ = 12 загроз;

$Р_{6\ місяців}$ = 6 загроз;

$Р_{1\ місяця}$ = 1 загроза.

Припустимо, величина збитку від реалізації однієї загрози (НСД, розголошення, витік) складає 1000000 грн.

Тобто С=1000000 грн.

Тоді проведемо розрахунки для визначення величини втрат/збитку (СР):

$СР_{12\ місяців} = С*Р_{12\ місяців}$ = 1000000 грн.*12 загроз = 12000000 (грн./12 місяців).

$СР_{6\ місяців} = С*Р_{6\ місяців}$ = 1000000 грн.*6 загроз = 6000000 (грн./6 місяців).

$СР_{1\ місяць} = С*Р_{1\ місяць}$ =1000000 грн.*1загроза = 1000000 (грн./1 місяць).

Тепер оцінено ефективністю методів захисту. Для даного абстрактного випадку в результаті експертної оцінки методів захисту було отримано значення 40 % (у чотирьох випадках з десяти захист спрацьовує), тоді розрахуємо скільки ми виграємо і втратимо коштів в результаті застосування старої, не модернізованої СЗПДн. Отож, ми виграємо (ЕМ):

$ЕМ_{12\ місяців}$ = 40% * $СР_{12\ місяців}$ = 0,4*12000000 (грн./12 місяців) = 4800000 (грн./12 місяців).

$ЕМ_{6\ місяців}$ = 40% * $СР_{6\ місяців}$ = 0,4*6000000 (грн./6 місяців) = 2400000 (грн./6 місяців).

$ЕМ_{1\ місяць}$ = 40% * $СР_{1\ місяць}$ = 0,4*1000000 (грн./1 місяць) = 400000 (грн./1 місяць).

Тоді програємо (LM):

$LM_{12\ місяців}$ = $СР_{12\ місяців}$ – $ЕМ_{12\ місяців}$ = 12000000 (грн./12 місяців) - 4800000 (грн./12 місяців) = 7200000 (грн./12 місяців).

$LM_{6\ місяців}$ = $СР_{6\ місяців}$ – $ЕМ_{6\ місяців}$ = 6000000 (грн./6 місяців) - 2400000 (грн./6 місяців) = 3600000 (грн./6 місяців).

$LM_{1\ місяць}$ = $СР_{1\ місяць}$ – $ЕМ_{1\ місяць}$ = 1000000 (грн./1 місяць) - 400000 (грн./1 місяць) = 600000 (грн./1 місяць).

Тепер порахуємо витрати, що включають в себе обслуговування засобів захисту, які використовуються на даний момент в банку, зміна технології обробки інформації, навчання персоналу, зарплата персоналу і т.д. Все це в сумі склало (СМ) 350000 (грн/місяць).

$СМ_{12\ місяців}$ = 4200000 (грн./12 місяців).

$СМ_{6\ місяців}$ = 2100000 (грн./6 місяців).

$СМ_{1\ місяць}$ = 350000 (грн./1 місяць).

Тоді величина чистої вигоди дорівнює (PR):

$PR_{12\ місяців}$ = $ЕМ_{12\ місяців}$ - $СМ_{12\ місяців}$ = 4800000 (грн./12 місяців) - 4200000 (грн./12 місяців) = 600000(грн./12 місяців).

$PR_{6\ місяців}$ = $ЕМ_{6\ місяців}$ – $СМ_{6\ місяців}$ = 2400000(грн./6 місяців) - 2100000 (грн./6 місяців) = 300000 (грн./6 місяців).

$PR_{1\ місяць}$ = $ЕМ_{1\ місяць}$ - $СМ_{1\ місяць}$ = 400000 (грн./1 місяць) - 350000 (грн./1 місяць) = 50000(грн./1 місяць).

Тож, застосовуючи старі методи захисту, отримуємо результат достатньо низької ефективності СЗПДн, котрий показує нам, що такий метод захисту також мав право на застосування в системах захисту 3-4 роки назад. На

противагу цьому нам хотілося, щоб захист ПДн був більш надійним. Щоб досягти поставлену задачу ми застосуємо кілька передових методів контролю і аудиту СЗПДн, таких як пентест вартістю 81000 грн. два рази на рік, програмно-технічний засіб захисту системи моніторингу подій ІБ ArcSight ESM вартістю 50000. Також використаємо вітчизняні ліцензовані програмні засоби торгової марки «Лоза» вартістю 3000 грн. за штуку, котрі дозволяють надійно зберегти конфіденційну інформацію від витоку, розголошення і НСД. Треба додати, що система Лоза-2 реалізує всі стандартні функції, необхідні для надійного захисту інформації від НСД і для побудови КСЗІ. Система Лоза-2 не має аналогів в Україні, що робить її використання в КСЗІ безцінною поміччю.

Загальна вартість використання цих компонентів захисту буде становити 81000*2+50000+3000 = 215000 грн./рік.

Отож, на рисунку 3.2. зображена оновлена і модернізована КСЗІ.

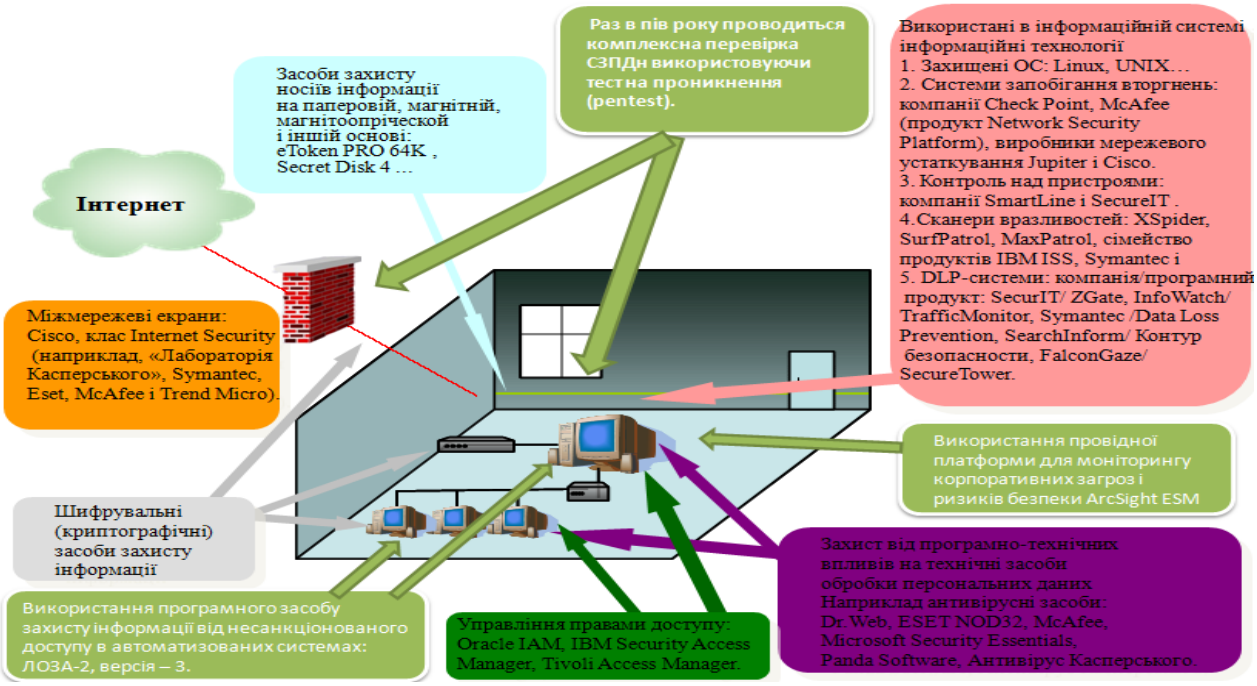

Рис. 3.2.Склад модернізованої КСЗІ.

Для даного випадку в результаті експертної оцінки оновлених методів захисту було отримано значення 90 % (у дев'яти випадках з десяти захист спрацьовує), тоді розрахуємо скільки ми виграємо і втратимо коштів в результаті застосування нової, сучасної, модернізованої СЗПДн. Отож ми виграємо (ЕМ):

$ЕМ_{12\ місяців}$ = 90% * $СР_{12\ місяців}$ = 0,9*12000000 (грн./12 місяців) = 10800000 (грн./12 місяців).

$ЕМ_{6\ місяців}$ = 90% * $СР_{6\ місяців}$ = 0,9*6000000 (грн./6 місяців) = 5400000 (грн./6 місяців).

$ЕМ_{1\ місяць}$ = 90% * $СР_{1\ місяць}$ = 0,9*1000000 (грн./1 місяць) = 900000 (грн./1 місяць).

Тоді програємо (LM):

$LM_{12\ місяців}$ = $СР_{12\ місяців}$ – $ЕМ_{12\ місяців}$ = 12000000 (грн./12 місяців) - 10800000 (грн./12 місяців) = 1200000 (грн./12 місяців).

$LM_{6\ місяців}$ = $СР_{6\ місяців}$ – $ЕМ_{6\ місяців}$ = 6000000 (грн./6 місяців) - 5400000 (грн./6 місяців) = 600000 (грн./6 місяців).

$LM_{1\ місяць}$ = $СР_{1\ місяць}$ – $ЕМ_{1\ місяць}$ = 1000000 (грн./1 місяць) - 900000 (грн./1 місяць) = 100000 (грн./1 місяць).

Тепер порахуємо витрати, що включають в себе обслуговування засобів захисту, які використовуються на даний момент в банку, зміна технології обробки інформації, навчання персоналу, зарплата персоналу, введення додаткових, сучасних методів, технологій і систем захисту і т.д. Все це в сумі склало (СМ) 400000 (грн/1 місяць). До того всього ми додаємо вартість комплексного захисту, котрий складає 215000 грн/рік або приблизно 81000 грн/6 місяців. Тож всі витрати (СМ) будуть становити:

$СМ_{12\ місяців}$ = 4800000+215000 = 5015000 (грн./12 місяців).

$СМ_{6\ місяців}$ = 2400000+81000 = 2481000 (грн./6 місяців).

$СМ_{1\ місяць}$ = 400000 (грн./1 місяць).

Тоді величина чистої вигоди (PR) буде дорівнювати:

$PR_{12\ місяців}$ = $ЕМ_{12\ місяців}$ - $СМ_{12\ місяців}$ = 10800000 (грн./12 місяців) - 5015000 (грн./12 місяців) = 5785000 (грн./12 місяців).

$PR_{6\ місяців}$ = $ЕМ_{6\ місяців}$ – $СМ_{6\ місяців}$ = 5400000(грн./6 місяців) - 2481000 (грн./6 місяців) = 2919000 (грн./6 місяців).

$PR_{1\ місяць}$ = $ЕМ_{1\ місяць}$ - $СМ_{1\ місяць}$ = 900000 (грн./1 місяць) - 400000 (грн./1 місяць) = 500000(грн./1 місяць).

У другому розглянутому випадку величина чистої вигоди має позитивне значення, що говорить про доцільність і необхідність застосування обраних методів захисту. Тепер детально проаналізуємо результати до і після застосування нових методів захисту і технологій в СЗПДн в таблиці 3.4.

Таблиця 3.4

Результати дослідження застосування обраних методів захисту.

		До	Після	Різниця, грн (+/-)	Темпи росту, %
Збережені кошти, грн.	12 місяців	4800000	10800000	6000000	225
	6 місяців	2400000	5400000	3000000	225
	1 місяць	600000	900000	300000	150
Втрати від реалізації загроз, грн	12 місяців	7200000	1200000	-6000000	17
	6 місяців	3600000	600000	-3000000	17
	1 місяць	600000	100000	-500000	17
Витрати на технології, персонал і т.д., грн	12 місяців	4200000	5015000	815000	119
	6 місяців	2100000	2481000	381000	118
	1 місяць	350000	400000	50000	114
Чиста вигода, грн	12 місяців	600000	5785000	5185000	964
	6 місяців	300000	2915000	2615000	972
	1 місяць	50000	500000	450000	1000

Отож, в таблиці ми маємо змогу побачити як змінилися показники до і після застосування нових методів захисту і технологій в СЗПДн. В рядку «Збережені кошти» ми маємо змогу побачити, що після введення нових методів і технологій захисту збережені гроші за 12 місяців, 6 місяців і місяць збільшилися на 6000000 (грн/12 місяців), 3000000 (грн/6 місяців), 300000 (грн/місяць) відповідно. Темпи росту склали 225, 225 і 150 відсотків відповідно.

Втрати від реалізації загроз за 12 місяців, 6 місяців, 1 місяць зменшилися на 6000000 (грн/12 місяців), 3000000 (грн/6 місяців), 300000 (грн/місяць) відповідно.

Витрати на технології і персонал за 12 місяців, 6 місяців і місяць збільшилися на 815000 (грн/12 місяців), 381000 (грн/6 місяців), 50000 (грн/місяць) відповідно.

Однак чиста вигода за 12 місяців, 6 місяців і місяць збільшилися на 5185000 (грн/12 місяців), 2615000 (грн/6 місяців), 450000 (грн/місяць) відповідно.

Наостанок, проаналізуймо темпи росту всіх показників. Збережені кошти за 12 місяців, 6 місяців і 1 місяць після введення нових методів і технологій захисту збільшилися на 225, 225 і 150 відсотків відповідно.

Втрати від реалізації загроз за 12 місяців, 6 місяців, 1 місяць зменшилися до 17, 17 і 17 відсотків відповідно від суми попередніх втрат.

Витрати на нові технології, персонал і тому подібне за 12 місяців, 6 місяців, 1 місяць збільшилися на 119, 118, 114 відсотків відповідно.

Чиста вигода за 12 місяців, 6 місяців і 1 місяць збільшилися на рекордні 964, 972 і 1000 відсотків відповідно, що саме пособі вже є показником ефективного і доцільного застосування і використання вищенаведених нових технологій і методів захисту ПДн.

Отже, можна зробити висновок, що використання запропонованих нових технологій і методів захисту суттєво збільшить продуктивність СЗПДн і водночас значно зменшить ймовірність реалізації загроз ПДн, котрі спричинюють великі втрати.

Висновки до розділу 3.

Таким чином, можна зробити висновок, що створення і надійне функціонування СЗПДн полягає не в купівлі і впровадженні передових технологій, а в послідовній побудові системи, котра буде спиратися на діючі міжнародні, державні і галузеві нормативні акти. При проектуванні нових систем потрібно застосовувати програмне забезпечення з вбудованими сертифікованими засобами захисту, що пройшло сертифікацію за вимогами безпеки інформації.

Структура системи, склад і зміст елементів, їх взаємозв'язок залежать від об'єму і цінності інформації, що захищається, характеру можливих загроз безпеки інформації, необхідної надійності захисту і вартості системи.

Для того щоб вдосконалити СЗПДн банку необхідно завжди бути в курсі останніх новинок захисту своїх даних і ПДн своїх клієнтів, оскільки останнім часом атаки на банки для заволодіння базами даних стають все більш небезпечними.

За результатами проведеного дослідження можна зробити такі висновки.

При проведення робіт по захисту ПДн, найкращим варіантом для малої та середньої організації буде вибір експертного консалтингу, оскільки це знижує фінансове навантаження на організацію, котра замовила дані послуги, а також дозволяє її фахівцям отримати необхідних досвід в області побудови надійного комплексного захисту.

А щодо модернізації КСЗІ, то впровадження передового методу контролю і аудиту СЗПДн, такого як пентест, програмно-технічного засобу захисту системи моніторингу подій ІБ ArcSight ESM та вітчизняний ліцензований програмний засіб торгової марки «Лоза», котрий дозволить надійно зберегти конфіденційну інформацію від витоку, розголошення і НСД суттєво збільшить продуктивність СЗПДн і водночас значно зменшить ймовірність реалізації загроз ПДн, котрі спричинюють великі втрати.

ВИСНОВОК

Для досягнення поставленої мети, був з’ясований стан вітчизняного та зарубіжного законодавства у сфері захисту ПДн, розглянутий склад існуючої СЗПДн і внесені зміни і пропозиції щодо удосконалення побудови системи захисту на правовому, організаційному та технічному рівнях.

У роботі були вирішені наступні задачі:

розглянутий стан вітчизняного законодавства у сфері захисту ПДн;

охарактеризовані європейські стандарти захисту ПДн;

детально проаналізований комплекс засобів захисту ПДн;

запропоновані напрями удосконалення захисту ПДн в Україні.

Проблема захисту ІБ в цілому та захисту ПДн в конкретному розумінні на економічних об’єктів багатоаспектна і потребує подальшого опрацювання.

З викладеного вище матеріалу можна зробити наступні висновки.

1. Організаційне-правове упорядкування суспільних інформаційних відносин щодо процесів у зв'язку з автоматизованою обробкою ПДн має тенденцію до посилення захисту даних про фізичних осіб і регулювання суспільних інформаційних відносин на базі спеціалізованих законодавчих актів та міжнародних угод. Разом з тим проблема захисту ПДн, коло об'єктів яких дуже широке і різноманітне, вимагає постійного вивчення, аналізу, осмислення і, що важливо, конкретизації елементів упорядкування суспільних інформаційних відносин у підзаконних нормативно-організаційних документах.

Основна мета захисту ПДн – забезпечити за допомогою законодавчих та нормативно-організаційних засобів реально гарантований захист зазначених прав громадян. Кожна ланка механізму захисту повинна бути сформована таким чином, щоб вона не тільки реалізувала свою внутрішню мету і виправдала свою сутність, але й створила умови для досягнення кінцевої мети, а саме відновлення порушеного права. При цьому, на першому етапі (на законодавчому рівні) повинна бути закладена ідеальна модель, тобто, базовий,

рамковий закон про захист ПДн. Реалізація його повинна бути забезпечена відповідними нормативно-організаційними, матеріальними та іншими ресурсами. Положення закону повинні відповідати нормам Конституції України та міжнародного права, а також не суперечити іншим нормативно-правовим актам держави.

На другому етапі дії механізму захисту ПДн (на нормативно-організаційному рівні) повинно відбутися реальне відновлювання порушених суб'єктивних прав за допомогою уповноваженої на це особи (Уповноваженого органу), або винесення рішення у адміністративному чи судовому порядку та належне його виконання у зв'язку із законною вимогою зацікавленої особи.

Сьогодні сучасний міжнародний і європейський досвід дозволяє сформувати законодавство про захист ПДн в Україні з урахуванням досягнутого в стандартах рівня захисту. Це пояснюється намірами суспільства підвищити рівень захисту відомостей про фізичних осіб (що дозволяють міжнародні стандарти), з огляду на існуючий соціально-економічний стан, формування в суспільстві сучасного менталітету та поширення процесів, пов'язаних із розвитком е-середовища.

Отож, найважливіше на законодавчому рівні - створити механізм, що дозволяє узгодити процес розробки законів з реаліями інформаційних технологій. Звичайно, закони не можуть випереджати життя, але важливо, щоб відставання не було занадто великим, так як на практиці, крім інших негативних моментів, це призведе до зниження ІБ.

Крім того неухильне зростання злочинності у сфері захисту ПДн змусив законодавців України вжити адекватних заходів по боротьбі з цим видом протиправних діянь, в тому числі кримінально-правових.

Якщо розглядати нормативні документи з питань управління захистом ПДн клієнтів банку, то необхідно починаючи з міжнародних, національних, галузевих стандартів, законів законодавчого органу закінчуючи внутрішніми документами організації.

Один із основних галузевий стандартів України є [17]. Про нього можна сказати, що він у своїй основі спирається на [21], що саме по собі є запорукою успіху. І що не менш важливо, що цей стандарт узгоджений із стандартами [22] (описує вимоги до системи менеджменту якості організацій і підприємств.) та [23] (створення системи екологічного менеджменту), з метою підтримки послідовного та комплексного впровадження і функціонування разом з іншими пов’язаними стандартами управління.

Також потрібно сказати, що прийняття [1] було однією із вимог співробітництва ЄС та України, з метою наближення правової системи нашої країни до європейських стандартів. Цей закон був створений на базі міжнародних та європейських стандартів у цій сфері. Водночас аналіз норм цього нормативно-правового акту засвідчує про значне розходження у розумінні сутності і змісту ПДн. Крім того, вітчизняне законодавство у сфері захисту ПДн є недостатньо сформованим через наявність значної кількості прогалин та колізій, що сприяє правопорушенням у цій сфері.

Україна, як держава, що проголосила курс на євроінтеграцію, має забезпечити правові механізми захисту ПДн, що відповідають сучасним міжнародним стандартам. Приведення правових норм вітчизняного законодавства до міжнародних стандартів є передумовою для створення та існування системи державного регулювання в сфері захисту ПДн. Оскільки захист має на увазі певні обмеження, необхідно, орієнтуючись на міжнародно-правові норми, при розробці українських законів створити чіткий механізм таких обмежень. Загальні перспективи законодавчого регулювання інформаційних прав і свобод пов'язані насамперед з необхідністю конкретизації, розвитку та створення механізму реалізації конституційно-правових норм, які регулюють цю сферу.

2. Забезпечення ІБ банку – це складна система заходів із забезпечення необхідного рівня інформованості керівництва і персоналу банку, а також зовнішнього середовища, ефективний захист усіх видів інформації від зовнішніх і внутрішніх загроз.

При детальному аналізі основних видів загроз ПДн в банківській сфері, ми визначити:

за направленістю і характером впливу на банки загрози можуть бути економічними, фізичними та інтелектуальними;

дії, що призвели до порушення ІБ поділяються на НСД, розголошення і витік інформації.

Найголовніше в функціонуванні СЗПДн є надійний безперебійний захист від всіх впливів навколишнього та внутрішнього середовища, котрі несуть в собі загрозу для надійної роботи даної системи. Тому потрібно, щоб в організацій була своя служба безпеки.

Дотримання вимог українського законодавства щодо захисту ПДн є необхідною, але недостатньою умовою для забезпечення високого рівня захищеності ІС. Необхідно розуміти, що навіть атестована ІС може бути зламана, якщо в рамках проекту був використаний формальний підхід, який передбачає виконання вимог, викладених у нормативних документах. Реальна захищеність СЗПДн можлива тільки при комплексному підході, який враховує вимоги українського законодавства і рекомендації міжнародних стандартів. Завдання щодо захисту ПДн не повинно розглядатися як разовий проект. Система захисту ПДн має постійно супроводжуватися і вдосконалюватися в рамках процесної моделі управління ІБ. Це передбачає адміністрування засобів захисту інформації, актуалізацію документів, що регламентують питання захисту ПДн, проведення періодичного аудиту захищеності ПДн і т. д. Також повинні ставитися жорсткі вимоги до підбору персоналу, який працює з ПДн, розголошення яких може завдати непоправної шкоди банку.

3. Створення і надійне функціонування СЗПДн полягає не в купівлі і впровадженні передових технологій, а в послідовній побудові системи, котра буде спиратися на діючі міжнародні, державні і галузеві нормативні акти. При проектуванні нових систем потрібно застосовувати програмне забезпечення з вбудованими сертифікованими засобами захисту, що пройшло сертифікацію за

вимогами безпеки інформації. Це дозволить надалі заощадити на закупівлі засобів захисту та навчанні персоналу.

При побудові СЗПДн потрібно обов’язково провести аудит, головними цілями якого є визначення відповідності реальних процесів нормативним документам і вимогам законодавства. Структура системи, склад і зміст елементів, їх взаємозв'язок залежать від об'єму і цінності інформації, що захищається, характеру можливих загроз безпеки інформації, необхідної надійності захисту і вартості системи.

Для того щоб вдосконалити СЗПДн банку необхідно завжди бути в курсі останніх новинок захисту (як технічних, так і законодавчих) своїх даних і ПДн своїх клієнтів, оскільки останнім часом атаки на банки для заволодіння базами даних стають все більш небезпечними. Також до майбутніх головних напрямків розвитку СЗПДн належить інтернет-банкінг.

За результатами проведеного дослідження можна зробити такі висновки.

При проведення робіт по захисту ПДн, найкращим варіантом для малої та середньої організації буде вибір експертного консалтингу, оскільки це знижує фінансове навантаження на організацію, котра замовила дані послуги, а також дозволяє її фахівцям отримати необхідних досвід в області побудови надійного комплексного захисту.

А щодо модернізації КСЗІ, то впровадження передового методу контролю і аудиту СЗПДн, такого як пентест, програмно-технічного засобу захисту системи моніторингу подій ІБ ArcSight ESM та вітчизняний ліцензований програмний засіб торгової марки «Лоза», котрий дозволить надійно зберегти конфіденційну інформацію від витоку, розголошення і НСД суттєво збільшить продуктивність СЗПДн і водночас значно зменшить ймовірність реалізації загроз ПДн, котрі спричинюють великі втрати.

При проведені дослідження була побудована таблиця 3.4., котра наглядно демонструє економічну доцільність застосування запропонованих нами методів захисту ПДн.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про захист персональних даних» [Електронний ресурс]. Режим доступу: http://zakon4.rada.gov.ua/laws/show/2297-17 документ 2297-17, чинний.

2. Закон України «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних» [Електронний ресурс]. Режим доступу:http://zakon1.rada.gov.ua/laws/show/3454-17 документ 3454-17, чинний.

3. Закон України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних данних» [Електронний ресурс]. Режим доступу: http://zakon4.rada.gov.ua/laws/show/383-18 документ 383-18, чинний.

4. Закон України «Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних» [Електронний ресурс]. Режим доступу: http://zakon4.rada.gov.ua/laws/show/2438-17 документ 2438-17, чинний.

5. Указ Президента України «Про Положення про Державну службу України з питань захисту персональних даних» [Електронний ресурс]. Режим доступу: http://zakon4.rada.gov.ua/laws/show/390/2011 документ 390/2011, чинний.

6. Постанова Кабінету Міністрів України Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [Електронний ресурс]. Режим доступу: http://zakon2.rada.gov.ua/laws/show/373-2006-%D0%BF документ 373-2006-п, чинний.

7. Цивільний кодекс України.

8. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. [Електронний ресурс]. Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_326 документ 994_326, чинний.

9. Додатковий протокол до Конвенції стосовно органів нагляду та транскордонних потоків даних. [Електронний ресурс]. Режим доступу: http://zakon4.rada.gov.ua/laws/show/994_363 документ 994_363, чинний.

10. Директива 95/46/ЄС Європейського парламенту та Ради «Про захист осіб у зв'язку з обробкою персональних даних та вільним обігом цих даних». [Електронний ресурс].

11. Директива 97/66/ЄС Європейського парламенту та Ради «Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі». [Електронний ресурс].

12. Загальна декларація прав людини 1948 року (стаття 12) [Електронний ресурс]. Режим доступу:http://zakon2.rada.gov.ua/laws/show/995_015

13. Нормативний документ системи технічного захисту інформації «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» НД ТЗІ 1.1-002-99 [Електронний ресурс]. Режим доступу: http://webcache.googleusercontent.com/search?q=cache:dxIVfArOiNEJ:dstszi.kmu.gov.ua/dstszi/doccatalog/document%3Fid%3D106340+&cd=1&hl=ru&ct=clnk&gl=ua.

14. НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» [Електронний ресурс]. Режим доступу:www.iji.com.ua/kszi/ TZI/3_7-003-05.doc

15. НД ТЗІ 1.4-001 «Типове положення про службу захисту інформації в автоматизованій системі» [Електронний ресурс]. Режим доступу: http://info-stand.com/nb-ukraine/by-type/nd-tzi/6-ndtzi14-001-00

16. СОУ Н НБУ 65.1 СУІБ 1.0:2010 Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005) [Електронний ресурс].

17. СОУ Н НБУ 65.1 СУІБ 2.0:2010 Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою. (ISO/IEC 27001:2005). [Електронний ресурс].

18. Європейська конвенція «Про захист прав людини і основоположних свобод» [Електронний ресурс]. Режим доступу: http://zakon4.rada.gov.ua/laws/show/995_004 документ 995_004, чинний.

19. Конституція України Стаття 32. [Електронний ресурс]. Режим доступу: http://kodeksy.com.ua/konstitutsiya_ukraini/statja-32.htm

20. ISO/IEC 27001:2005 Інформаційна технологія. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. вимоги. [Електронний ресурс]. Режим доступу: http://www.iso.org/iso/ru/catalogue_detail?csnumber=42103

21. ISO 9001:2000 Системи менеджменту якості. Вимоги. [Електронний ресурс]. Режим доступу: http://www.iso.org/iso/ru/catalogue_detail?csnumber=21823

22. ISO 14001:2004 Системи екологічного менеджменту. Вимоги та настанови щодо застосування. [Електронний ресурс]. Режим доступу: http://www.iso.org/iso/ru/catalogue_detail?csnumber=31807

23. BS 10012:2009 «Захист даних. Специфікація системи управління персональними даними». [Електронний ресурс]. Режим доступу: http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030175849

24. ISO / IEC 17799 Інформаційні технології. Технології безпеки. Практичні правила менеджменту інформаційної безпеки. [Електронний ресурс]. Режим доступу: http://www.icc-iso.ru/upload/shop_3/3/0/0/item_300/GOST_R_ISO_MEK_17799-2005.pdf

25. «Положення про Державний реєстр баз персональних даних та порядок його ведення». Документ 616-2011-п, чинний. [Електронний ресурс]. Режим доступу: http://zakon4.rada.gov.ua/laws/show/616-2011-%D0%BF

26. В.В. Домарев Управління інформаційною безпекою в банківських установах (теорія і практика впровадження стандартів серії ISO 27k) / В.В. Домарєв // Донецьк.: Велстар, 2012. 146 с.

27. В.В. Домарєв, В.А. Швець Організаційне забезпечення захисту інформації з обмеженим доступом / В.В. Домарєв, В.А. Швець // НАУ Київ., 2006. 108 с.

28. Загінайлов Ю.Н. Комплексна система захисту інформації на підприємстві: навчально-методичний посібник / Ю.М. Загінайлов та ін. // Алт.держ.техн.ун-т ім.І.І.Ползунова. Барнаул: АлтДТУ. 2010. 209 с.

29. І.М. Сопілко Механізми захисту персональних даних: проблеми та перспективи / І.М. Сопілко // Юридичний вісник 2(27) 2013. [Електронний ресурс]. Режим доступу: file:///C:/Users/A/Downloads/4838-12152-1-SM.pdf

30. Тунік А. В. Правові основи захисту персональних даних / Тунік А. В. // Національна і міжнародна безпека в сучасних трансформаційних процесах: матеріали науково-практичної конференції (Київ, 29 грудня 2011 р.). Київ.: ФОП Ліпкан О.С., 2011. С. 62 – 65.

31. Презентація «Доктор Веб. Захист персональних даних». [Електронний ресурс].

32. Конспект лекцій з дисципліни «Електронна комерція». Тема 7. Проблеми безпеки та захисту інформації при роботі в Internet. [Електронний ресурс].

33. К. Фрумкін Шахрайство та злочини у банківській сфері /К.Фрумкін// Українське агентство фінансового розвитку. [Електронний ресурс]. Режим доступу: http://www.ufin.com.ua/analit_mat/gkr/150.htm

34. Р. Катчиев Захист персональних даних в банках / Р. Катчиев // [Електронний ресурс]. Режим доступу: http://www.crmdaily.ru/novosti-rynka-crm/502-zashhita-personalnyx-dannyx-v-bankax.html

35. Додаток до постанови Центральної виборчої комісії «Технічне завдання на створення комплексної системи захисту інформації в автоматизованій інформаційно-телекомунікаційній системі».

36. Стаття «Кому довірити впровадження захисту персональних даних?» [Електронний ресурс]. Режим доступу: http://www.uipdp.com/about/faq/implementation.html

37. Стаття «Створення системи захисту персональних даних» [Електронний ресурс]. Режим доступу: http://security-testlab.com/uslugi/kszipd/

38. Реферат: «Безпека банківської діяльності» [Електронний ресурс]. - Режим доступу: http://studentam.net.ua/content/view/5474/132/

39. Реферат: «Технологія захисту персональних даних» [Електронний ресурс]. Режим доступу: http://www.elitpasp.ru/gosudarstvo_i_pravo/texnologiya_zashhity_personalnyx_dannyx.html

40. Новости SSL. «Обзор основ криптографии». [Електронний ресурс]. Режим доступу: http://sslnews.com.ua/book_cryptography_overview-russian.html

41. Лекции по дисциплине «Компьютерные технологии в науке и образовании», тема: «Метод «интеллектуального перебора» паролей». [Електронний ресурс]. Режим доступу: http://chaliev.ru/ise/lections-comp-tech-zo.php