Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента *Полєва Михайла Дмитровича*

академічної групи *125м-22-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка рекомендацій та політики безпеки щодо обробки персональних даних в ІКС банківської установи*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Ковальова Ю.В.			
розділів:				
спеціальний	к.т.н., доц. Ковальова Ю.В.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту ***Полєву Михайлу Дмитровичу*** **академічної групи** ***125м-22-2***
(прізвище ім'я по-батькові) (шифр)

спеціальності ***125 Кібербезпека***

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Розробка рекомендацій та політики безпеки щодо обробки персональних даних в ІКС банківської установи***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Стан питання. Постановка задачі	02.11.2023
Розділ 2	Спеціальна частина	16.11.2023
Розділ 3	Економічна частина	30.11.2023

Завдання видано _____ Ковальова Ю.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Полєв М.Д.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи містить: 122 сторінки, 3 рисунки, 8 таблиць, 9 додатки, 14 посилань.

Мета кваліфікаційної роботи: розробити рекомендації та політику безпеки при обробці персональних даних в ІКС у банківській установі, спираючись на Закон України «Про захист персональних даних».

У спеціальній частині представлено аналіз Закону України «Про захист персональних даних», аналітичний огляд та обґрунтування вимог до інформаційної комп'ютерної системи оброки персональних даних відділення ПАТ КБ «Правекс-Банк». Проаналізовано етапи створення комплексної системи захисту інформації та розроблена типова політика безпеки для об'єкта інформаційної діяльності. Виконано аналіз та класифікація інформації, що циркулює в банку.

В економічній частині виконано розрахунок капітальних витрат на створення центру обробки інформації з обмеженим доступом. Зроблено висновок щодо економічної ефективності створення центру.

КЛЮЧОВІ СЛОВА: ПЕРСОНАЛЬНІ ДАНІ, АВТОМАТИЗОВАНІ СИСТЕМИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ, ІНФОРМАЦІЙНА КОМП'ЮТЕРНА СИСТЕМА, ПРОФІЛЬ ЗАХИЩЕНОСТІ, ПОЛІТИКА БЕЗПЕКИ.

ABSTRACT

The explanatory note of qualification work consists of: 122 pages, 3 figures, 8 tables, 9 appendices, 14 references.

The purpose of the qualification work: to develop recommendations and security policy regarding the processing of personal data in the ICS of a banking institution, based on the Law of Ukraine "On the Protection of Personal Data".

The special part presents an analysis of the Law of Ukraine "On the Protection of Personal Data", an analytical review and substantiation of the requirements for the information computer system of personal data processing of the PJSC CB Praveks-Bank branch. The stages of creating a comprehensive information protection system were analyzed and a typical security policy for the object of information activity was developed. The analysis and classification of information circulating in the bank was performed.

In the economic part, the calculation of capital costs for the creation of an information processing center with limited access was performed. A conclusion was made regarding the economic efficiency of the creation of the center.

KEY WORDS: PERSONAL DATA, AUTOMATED PERSONAL DATA PROCESSING SYSTEMS, INFORMATION COMPUTER SYSTEM, SECURITY PROFILE, SECURITY POLICY.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АСОІБ — автоматизована система обробки інформації а банку;

АТ — акціонерне товариство;

БД — база даних;

ВАТ — відкрите акціонерне товариство;

ЗАТ — закрите акціонерне товариство;

ІзОД — інформація з обмеженим доступом;

ІКС — інформаційна комп'ютерна система;

ІС — інформаційні системи;

ІТ — інформаційні технології;

ЗІ — захист інформації;

КМУ — Кабінет Міністрів України;

КЗЗ — комплекс засобів захисту;

КС — комп'ютерні системи;

КСЗІ — комплексна система захисту інформації;

НСД — несанкціонований доступ;

ОІД — об'єкт інформаційної діяльності;

ОС — операційна система;

ПнД — персональні дані;

ПЗ — програмне забезпечення;

ПК — персональний комп'ютер;

ТОВ — товариство з обмеженою відповідальністю.

ЗМІСТ

ВСТУП

Необхідність забезпечення безпеки персональних даних в наш час - об'єктивна реальність. Інформація про людину завжди мала велику цінність, але сьогодні вона перетворилася в найдорожчий товар. Інформація в руках шахрая перетворюється на знаряддя злочину, в руках звільненого співробітника - на засіб помсти, в руках інсайдера - товар для продажу конкурентові. Саме тому персональні дані потребують найсерйознішого захисту.

З розвитком засобів електронної комерції і доступних засобів масових комунікацій зросли також і можливості зловживань, пов'язаних з використанням зібраної та накопиченої інформації про людину. З'явилися і ефективно використовуються зловмисниками засоби інтеграції та швидкої обробки персональних даних, що створюють загрозу правам і законним інтересам людини.

Сьогодні навряд чи можна уявити діяльність організації без обробки інформації про людину а саме без обробки персональних даних. У будь-якому випадку організація зберігає і обробляє дані про співробітників, клієнтів, партнерів, постачальників та інших фізичних осіб. Витік, втрата або несанкціонована зміна персональних даних призводить до непоправних збитків, а часом і до повної зупинки діяльності організації.

Розуміючи важливість і цінність інформації про людину, а також піклуючись про дотримання прав своїх громадян, держава вимагає від організацій та фізичних осіб забезпечити надійний захист персональних даних. Законодавство про захист персональних даних ґрунтується на Конституції України, інших законів і підзаконних нормативно-правових актах, міжнародних договорах України і складається з Державного закону України від 1 червня 2010 року № 2273-VI «Про захист персональних даних», а також інших державних законів, що визначають випадки і особливості обробки персональних даних, галузевих нормативних актів, інструкцій і вимог регуляторів.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Актуальність проблеми

Стрімкий прогрес у сфері розвитку комп'ютерної техніки і комп'ютерних технологій став активно впливати на всі сфери життєдіяльності сучасного суспільства. Тому актуальною стала проблема захисту персональних даних людини в умовах залучення її в процеси інформаційної взаємодії. Велика активність у формуванні баз персональних даних спричинила за собою необхідність захисту прав людини в інформаційній сфері. Необхідність вживання заходів із захисту персональних даних викликана зростаючими технічними можливостями з копіювання та поширення інформації.

Зі вступом в силу Закону України «Про захист персональних даних» мільйони інформаційних систем, що стосуються збору, зберігання, обробки або передачі персональних даних фізичних осіб, стали підлягати модернізації в суворій відповідності з абсолютно новими вимогами до кінця поточного року. Сучасні суспільні відносини характеризуються широким використанням персональних даних під час обігу інформації (соціального, фінансового, правоохоронного, науково-технічного та ін. характеру), товарів, послуг і капіталів, що вимагає не тільки вільний рух інформації про особу, забезпечення її надійного захисту у відповідності до основних прав і свобод людини.

Розуміючи важливість і цінність інформації про людину, а також піклуючись про дотримання прав своїх громадян, держава вимагає від організацій та фізичних осіб забезпечити надійний захист персональних даних.

1.2 Аналіз підходів до захисту персональних даних з точки зору нормативної бази України.

Право на захист персональних даних у більшості розвинутих країн давно є одним з основоположних принципів громадянського суспільства. Захист персональної інформації трактується як невід'ємна частина права людини на

захист особистого життя, закріпленого в таких актах, як Загальна декларація прав людини 1948 р. та Європейська конвенція про захист прав людини і основоположних свобод 1953 р.

З 1 січня 2011 р. набув чинності Закон України «Про захист персональних даних». Документ регулює питання використання персональних даних про фізичних осіб, встановлює вимоги до обробки персональних даних, регламентує порядок їх збору, зберігання і передачі, а також доступу до них третіх осіб.

Громадяни, персональні дані яких піддаються обробці, наділені комплексом прав, спрямованих на недопущення незаконного використання, поширення, зберігання персональних даних, інших неправомірних дій щодо таких даних.

Бази персональних даних підлягають реєстрації уповноваженим державним органом з питань захисту персональних даних. На нього також покладено функції з контролю за дотриманням законодавства про захист персональних даних як органами влади, так і юридичними та фізичними особами, діяльність яких зв'язана з обробкою персональних даних.

Одночасно з набранням чинності Закону України «Про захист персональних даних» набрали чинності спеціальні акти, що регламентують порядок використання персональних даних фізичних осіб при їх обробці в базах даних, а саме:

- Закон України "Про захист персональних даних" від 01.06.2010 р. № 2297-VI (далі - Закон про персональні дані, Закон);
- Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981р. (далі - Конвенція про персональні дані, Конвенція);
- Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних від 08.11.2001 р. (далі - Протокол).

Прийняття зазначених нормативних актів у цілому призвело регулювання використання персональних даних в Україні у відповідність зі стандартами Європейського Союзу, які закріплені, зокрема, в Директиві № 95/46/ЄС.

Крім того, суспільні відносини щодо збирання, зберігання, використання та поширення інформації про особу в автоматизованих системах регулюються Законами України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», та Положеннями «Про державну службу України з питань захисту персональних даних» (Затверджено указом Президента України від 6 квітня 2011 року N 390/2011), «Про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах» (Затверджено постановою Кабінету Міністрів України від 16.02.98р. № 180). Указами Президента України "Про заходи щодо запровадження ідентифікаційних номерів фізичних осіб - платників податків та інших обов'язкових платежів", від 4 червня 1998 року № 794 "Про затвердження Положення про організацію персоніфікованого обліку відомостей у системі загальнообов'язкового державного пенсійного страхування", від 15 березня 2006 року № 327 "Про створення Державної інформаційної системи реєстраційного обліку фізичних осіб та їх документування" тощо.

1.2.1 Аналіз визначення «персональні дані» згідно чинного законодавства України

Необхідність прийняття Закону «Про захист персональних даних» уже давно гостро стояла в усіх учасників інформаційного обміну персональними даними, що перш за все обумовлено тим, що стан нормативно-правової бази неефективно забезпечує захист прав людини щодо виконання положень статей 3, 32, 34 Конституції України стосовно персональних даних. Більш ніж два десятки законів України регулюють суспільні відносини, що пов'язані із збиранням, зберіганням, використанням та поширенням інформації про особу

(персональних даних), однак всі вони не мають чіткого та скорельованого з європейським законодавством визначення персональних даних та визначених вимог щодо їхнього захисту.

Відповідно до Закону України «Про захист персональних даних» персональними даними є будь-яка інформація про фізичну особу, що дозволяє її ідентифікувати, а саме ім'я, вік, місце роботи та проживання, освіта тощо. Персональними даними можуть бути: національність, освіта, сімейний стан, релігійність, стан здоров'я, а також адреса, дата і місце народження. Крім того, згідно з Рішенням Конституційного Суду України № 5-зп від 30.10.97 до персональних даних також відносяться дані про майновий стан і медична інформація (показання про стан здоров'я людини, історія його хвороби, мету запропонованих досліджень і лікувальних заходів, прогноз можливого розвитку захворювання , включаючи наявність ризику для життя і здоров'я).

Відповідно до Рішення Конституційного Суду України від 30.10.1997 р. № 5-зп до персональних даних належить також інформація про стан здоров'я особи (історія хвороби, мета запропонованих досліджень і лікувальних заходів, прогноз можливого розвитку захворювання, в тому числі інформація про наявність ризику для життя і здоров'я).

Визначення персональних даних у Конвенції практично збігається з визначенням у Законі: це "будь-яка інформація, яка відноситься до конкретно ідентифікованої особи або особи, яка може бути конкретно ідентифікована".

Своєю чергою, Європейська Директива "Про захист осіб у зв'язку з обробкою персональних даних та переміщенням (передачею) таких даних" від 24.10.1995 р. (далі - Директива) визначає персональні дані як будь-яку інформацію, що стосується особи, яка ідентифікована або може бути конкретно ідентифікована. Особа, яка може бути ідентифікована, - це особа, яка може бути прямо чи опосередковано ідентифікована, зокрема, шляхом звернення до ідентифікаційного номера або до інших специфічних даних, як-от: фізичні, психологічні, ментальні, економічні, культурні чи соціальні дані.

Інформація про особу, яка ідентифікована, - це інформація, яка одразу асоціюється в суб'єкта - одержувача інформації (або її власника) з конкретною людиною. Отже, особа може бути ідентифікованою для одного суб'єкта, якому вона знайома, і не ідентифікованою для іншого, який цієї особи не знає.

Викладене можна проілюструвати такими прикладами персональних даних, як: ім'я, адреса, дата народження, місце роботи та посада, номер паспорта, номер ідентифікаційного коду тощо. Слід зазначити, що ідентифікація або гіпотетична можливість ідентифікації конкретної людини є ключовим критерієм. Так, список імен та прізвищ, поширених у центральних регіонах України, не є персональними даними, тому що імена і прізвища в такому списку не прив'язані до конкретних осіб.

Захист інформації про особу гарантовано Конституцією України. Частина друга статті 32 Конституції України не допускає збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Закон України "Про інформацію" закріплює загальні принципи доступу громадян до інформації, що стосується їх особисто. Механізм реалізації зазначеного права належним чином не визначений. Відсутнє й регулювання використання конфіденційної інформації про особу.

Статтею 23 Закону України "Про інформацію" встановлено, що інформація про особу – це сукупність документованих або публічно оголошених відомостей про особу.

Основними даними про особу (персональними даними) є: національність, освіта, сімейний стан, релігійність, стан здоров’я, а також адреса, дата і місце народження.

Джерелами документованої інформації про особу є видані на її ім’я документи, підписані нею документи, а також відомості про особу зібрані державними органами влади та органами місцевого самоврядування в межах своїх повноважень.

1.2.2 Об’єкти та суб’єкти захисту відповідно до Закону України «Про персональні дані»

Згідно із Законом про персональні дані об'єктами захисту є тільки ті персональні дані, які обробляються в базах персональних даних. База персональних даних - це іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних.

Відповідно до Закону, власником чи розпорядником бази персональних даних можуть бути будь-які особи, в тому числі органи державної влади чи органи місцевого самоврядування та фізичні особи – підприємці, які обробляють персональні дані. Кожен раз, коли інформація про фізичну особу буде змінюватись, володілець повинен інформувати таку особу та компетентний державний орган.

Однак комплексний аналіз норм Закону свідчить про інше: щоб підпадати під дію Закону, такий список (база) повинен мати певну мету обробки персональних даних. Відповідно до Закону власник бази персональних даних - це фізична або юридична особа, якій законом або за згодою суб'єкта персональних даних надано право на обробку цих даних, яка затверджує мету обробки персональних даних у цій базі даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом.

Статтею 6 Закону про персональні дані передбачено затвердження Типового порядку обробки персональних даних в базах персональних даних. Такий порядок, якщо він буде затверджений уповноваженим державним органом з питань захисту персональних даних (Указом Президента від 09.12.2010 р. № 1085/2010 цим органом визначено Державну службу з питань захисту персональних даних), може запропонувати детальніше визначення персональних даних і конкретніші вимоги до баз даних, що містять персональну інформацію.

Закон направлений на захист фізичних осіб від вимог щодо надмірного та невиправдано детального представлення персональної інформації (див. п 3 ст. 6) та від її несанкціонованого поширення та використання.

Закон про персональні дані крім суб'єкта персональних даних, чиї дані обробляються, передбачає ще кілька суб'єктів.

Власник бази персональних даних - фізична або юридична особа, якій законом або за згодою суб'єкта персональних даних надано право на обробку цих даних, яка затверджує мету обробки персональних даних у цій базі даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом.

Розпорядник бази персональних даних - фізична чи юридична особа, якій власником бази персональних даних або законом надано право обробляти ці дані.

Відповідно до ст. 4 Закону власником чи розпорядником бази персональних даних можуть бути підприємства, установи і організації всіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичні особи - підприємці, які обробляють персональні дані відповідно до закону. Відповідно, фізична особа (що не є підприємцем не може бути володільцем чи розпорядником баз персональних даних в розумінні Закону.

Відповідно до ст. 24 Закону на власника бази персональних даних покладається обов'язок забезпечення захисту персональних даних в базі. Крім того, в органах державної влади та органах місцевого самоврядування, організаціях, установах і на підприємствах усіх форм власності визначається структурний підрозділ або відповідальна особа, яка організовує роботу, пов'язану із захистом персональних даних при їх обробці, відповідно до закону. Фізичні особи - підприємці, у тому числі лікарі, які мають відповідну ліцензію, адвокати, нотаріуси особисто забезпечують захист баз персональних даних, якими володіють, згідно з вимогами закону. Право на обробку персональних даних має бути надане компаніям або самим суб'єктом персональних даних, або законом.

Закон про персональні дані чітко визначив, що згода суб'єкта персональних даних - це будь-яке документоване, зокрема письмове, добровільне волевиявлення фізичної особи щодо надання дозволу на обробку

її персональних даних відповідно до сформульованої мети їх обробки. Таким чином, компаніям, що займаються обробкою персональних даних, необхідно отримати письмову згоду від фізичних осіб, чиї дані обробляються. Така згода може бути оформлена у вигляді одностороннього документа або двостороннього договору і, щоб уникнути можливих претензій з боку суб'єктів персональних даних, контролюючих органів чи третіх осіб, має містити перелік всіх видів обробки персональних даних, які планують здійснювати, а також всіх видів таких даних. Якщо банк після отримання письмової згоди хоче розширити перелік дій з отриманими персональними даними та/або мету таких дій, необхідне письмове підтвердження такої зміни від суб'єкта персональних даних.

1.2.3 Методи захисту персональних даних

У широкому сенсі під забезпеченням захисту від несанкціонованого доступу розуміється комплекс організаційних і технічних заходів. Ці заходи ґрунтуються на розумінні механізмів запобігання несанкціонованого доступу на самих різних рівнях:

- ідентифікація та автентифікація (також двофакторна або сувора). Це може бути (операційна система, інфраструктурне ПЗ, прикладне ПЗ, апаратні засоби, наприклад, електронні ключі);
- реєстрація та облік. Це може бути журнал роботи (логування, протоколювання) подій у всіх перерахованих вище системах, ПО і засобах);
- забезпечення цілісності. Це може бути розрахунок по контрольних сумах контрольованих файлів, забезпечення цілісності програмних компонент, використання замкнутої програмного середовища, а також забезпечення довіреної завантаження ОС);
- міжмережевий екран, як шлюзової, так і локальний;
- антивірусна безпека (застосовується до трьох рівнів оборони, так званий ешелонований або мультивендорний підхід);

— криптографія (функціонально застосовується на різних рівнях моделі OSI (мережний, транспортний і вище), і забезпечує різний захисний функціонал)

Є кілька комплексних продуктів, що мають розвинений НСД функціонал. Всі вони відрізняються типами застосування, підтримкою обладнання, програмне забезпечення та топологією реалізації.

При розподіленій або яка має підключення до мережі загального користування ІСПДн застосовуються продукти аналізу захищеності а також виявлення та запобігання вторгнень (IDS / IPS) - як на рівні шлюзу, так і на рівні кінцевого вузла.

1.3 Захист персональних даних в інформаційних комп'ютерних системах обробки персональних даних

1.3.1 Специфіка захисту інформаційних комп'ютерних систем обробки персональних даних банку

Як правило інформаційні комп'ютерні системи обробки персональних даних обробляють великий потік запитів, які постійно надходять в реальному масштабі часу, кожен з яких не вимагає для обробки численних ресурсів, але всі разом вони можуть бути оброблені тільки високопродуктивною системою.

У автоматизованій системі обробки персональних даних зберігається і обробляється конфіденційна інформація. Її підробка або витік можуть призвести до серйозних (для банку або його клієнтів) наслідків. Тому автоматизовані системи обробки персональних даних приречені залишатися відносно закритими, працювати під управлінням специфічного програмного забезпечення і приділяти велику увагу забезпеченню її безпеки.

Іншою особливістю автоматизованої системи обробки персональних даних є підвищені вимоги до надійності апаратного та програмного забезпечення. Через це багато сучасних автоматизованих системи обробки персональних даних тяжіють до так званої відказостійкої архітектури

комп'ютерів, що дозволяє здійснювати безперервну обробку інформації навіть в умовах різних збоїв і відмов.

1.3.2 Типи завдань, що вирішують інформаційні комп'ютерні системи обробки персональних даних

Аналітичні. До цього типу належать завдання планування, аналізу рахунків і т.д. Вони не є оперативними і можуть вимагати для вирішення тривалого часу, а їх результати можуть вплинути на політику банку щодо конкретного клієнта або проекту. Тому підсистема, за допомогою якої вирішуються аналітичні завдання, повинна бути надійно ізольована від основної системи обробки інформації. Для вирішення такого роду завдань зазвичай не потрібно потужних обчислювальних ресурсів, зазвичай достатньо 10-20% потужності всієї системи. Однак зважаючи на можливу цінності результатів їх захист повинен бути постійним.

Повсякденні. До цього типу належать завдання, які вирішуються в повсякденній діяльності, в першу чергу виконання платежів і коригування рахунків. Саме вони і визначають розмір і потужність основної системи банку; для їх вирішення зазвичай потрібно набагато більше ресурсів, ніж для аналітичних завдань. У той же час цінність інформації, що обробляється при вирішенні таких завдань, має тимчасовий характер. Поступово цінність інформації, наприклад, про виконання якого-небудь платежу, ставати не актуальною. Природно, це залежить від багатьох факторів, як-то: суми і часу платежу, номера рахунку, додаткових характеристик і т.д. Тому, звичайно буває достатнім забезпечити захист платежу саме в момент його здійснення. При цьому захист самого процесу обробки і кінцевих результатів повинна бути постійною.

1.3.3 Аналіз стану банківських інформаційних комп'ютерних систем з точки зору безпеки

Під безпекою системи розуміється її захищеність від випадкового або навмисного втручання в нормальний процес її функціонування, а також від спроб розкрадання, модифікації або руйнування її компонентів. Слід зазначити, що природа впливу може бути самою різною. Це і спроби проникнення зловмисника, і помилки персоналу, і стихійні лиха (ураган, пожежа), і вихід з ладу складових частин. Безпека автоматизованих систем обробки персональних даних досягається забезпеченням конфіденційності оброблюваної нею інформації, а також цілісності та доступності компонентів і ресурсів системи.

Конфіденційність інформації - це властивість інформації бути відомою лише допущеним і які пройшли перевірку (авторизованим) суб'єктам системи (користувачам, програмам, процесам і т.д.). Для інших суб'єктів системи ця інформація як би не існує.

Цілісність компонента (ресурсу) системи - властивість компонента (ресурсу) бути незмінним (в семантичному сенсі) при функціонуванні системи.

Доступність компонента (ресурсу) системи - властивість компонента (ресурсу) бути доступним для використання авторизованими суб'єктами системи в будь-який час.

При розроблені підходів щодо вирішення проблеми безпеки слід завжди виходити з того, що кінцевою метою застосування будь-яких заходів протидії загрозам є захист власника і законних користувачів автоматизованих систем обробки персональних даних від нанесення їм матеріального або морального збитку в результаті випадкових чи навмисних впливів на неї.

Зазвичай розрізняють зовнішню і внутрішню безпеку інформаційних систем обробки персональних даних:

- Зовнішня безпека включає захист від стихійних лих (пожежа, повінь тощо) і від проникнення зловмисників ззовні з цілями

розкрадання, отримання доступу до носіїв інформації або виведення системи з ладу.

- Внутрішня безпеки включає забезпечення надійної і коректної роботи системи, цілісності її програм і даних.

Всі зусилля щодо забезпечення внутрішньої безпеки інформаційних комп'ютерних систем обробки персональних даних фокусуються на створенні надійних і зручних механізмів регламентації діяльності всіх її користувачів і обслуговуючого персоналу, дотримання встановленої в організації дисципліни прямого чи непрямого доступу до ресурсів системи і до інформації.

Аналіз побудови система інформаційної безпеки слід починати з аналізу ризиків можливих загроз.

Перед тим, як вибирати різні засоби захисту необхідно чітко уявляти які компоненти автоматизованих систем обробки персональних даних, від яких посягань і наскільки надійно потрібно захистити. Безумовно, основою системи захисту автоматизованих систем обробки персональних даних повинні бути організаційні (адміністративні) заходи, стрижнем якого є розробка і реалізація плану захисту. Але організаційні заходи без повсюдної підтримки їх фізичними і технічними (програмними та апаратними) засобами будуть слабкі. Тому при виборі засобів захисту необхідно звертати увагу не тільки на їх надійність, але і на те, як вони будуть підтримувати розроблені організаційні заходи.

Необхідно використовувати аналіз ризику для вибору найбільш реальних загроз системи і доцільних способів захисту від них.

Аналіз ризику потрібен:

1. Для підвищення обізнаності персоналу. Обговорення питань захисту автоматизованої системи обробки персональних даних може підняти рівень інтересу до цієї проблеми серед співробітників, що приведе до більш точного виконання вимог інструкцій.

2. Для визначення сильних і слабких сторін існуючих та пропонованих заходів захисту. Багато організацій не мають повної інформації про свою систему та її слабкі сторони. Систематичний аналіз дає всебічну інформацію про стан апаратного та програмного забезпечення автоматизованих систем обробки персональних даних і ступеня ризику втрати (спотворення, витоку) інформації при її обробці та зберіганні в електронному вигляді.

3. Для підготовки і прийняття рішення щодо вибору заходів та засобів захисту. Захист знижує продуктивність системи, вносячи при цьому незручності (іноді істотні) у роботу користувачів. Деякі заходи захисту занадто складні і дорогі, та їх застосування не може бути виправдано тими функціями, які вони виконують. У той же час існують настільки серйозні види загроз, що пошук та розробка нових, більш ефективних методів і засобів захисту від них є просто необхідними. В обох випадках ступінь ризику визначає рівень і масштаб застосовуваних засобів захисту.

4. Для визначення витрат на захист. Деякі механізми захисту потребують чималих ресурсів, і їх робота прихована від користувачів. Аналіз ризику може допомогти визначити найголовніші вимоги до системи захисту автоматизованої системи обробки персональних даних.

Аналіз ризику - це процес отримання кількісної або якісної оцінки збитку, який може статися в разі реалізації загрози безпеці системи.

Кожну систему обробки інформації захисту потрібно розробляти, індивідуально враховуючи такі особливості:

- організаційну структуру банку;
- обсяг і характер інформаційних потоків (всередині банку в цілому, всередині відділів, між відділами, зовнішніх);

1.4 Забезпечення безпеки персональних даних в інформаційних комп'ютерних системах обробки персональних даних

Обґрунтування комплексу заходів із забезпечення безпеки персональних даних в ІКС обробки персональних даних здійснюється з урахуванням

результатів оцінки небезпеки загроз та визначення класу інформаційної системи обробки персональних даних на основі «Основних заходів з організації та технічного забезпечення безпеки персональних даних, що обробляються в інформаційних системах персональних даних».

При цьому повинні бути визначені заходи щодо:

- виявлення та закриття технічних каналів витоку персональних даних в автоматизованій системі обробки персональних;
- захист персональних даних від несанкціонованого доступу та неправомірних дій;
- встановлення, налагодження і застосування засобів захисту.

Заходи з виявлення та закриття технічних каналів витоку персональних даних в автоматизованій системі обробки персональних формулюються на основі аналізу та оцінки загроз безпеки персональних даних.

Заходи щодо захисту персональних даних при їх обробці в автоматизованій системі обробки персональних від несанкціонованого доступу та неправомірних дій включають:

- управління доступом;
- реєстрацію та облік;
- забезпечення цілісності;
- контроль відсутності декларованих можливостей;
- антивірусний захист;
- забезпечення безпечного міжмережевої взаємодії автоматизованої системи обробки - персональних даних;
- аналіз захищеності;
- виявлення вторгнень.

Підсистему управління доступом, реєстрації та обліку рекомендується реалізовувати на базі програмних засобів блокування несанкціонованих дій, сигналізації і реєстрації. Це спеціальні, що не входять в ядро будь-якої операційної системи програмні та програмно-апаратні засоби захисту самих операційних систем, електронних баз персональних даних і прикладних

програм. Вони виконують функції захисту самостійно або в комплексі з іншими засобами захисту і спрямовані на виключення або утруднення виконання небезпечних для автоматизованої системи обробки персональних даних дій користувача або порушника. До них відносяться спеціальні утиліти та програмні комплекси захисту, в яких реалізуються функції діагностики, реєстрації, знищення, сигналізації та імітації.

Засоби діагностики здійснюють тестування файлової системи та баз персональних даних, постійний збір інформації про функціонування елементів підсистеми забезпечення безпеки інформації.

Засоби знищення призначені для знищення залишкових даних і можуть передбачати аварійне знищення даних у разі загрози несанкціонованого доступу, який не може бути блокований системою.

Засоби сигналізації призначені для попередження операторів при їх зверненні до захищуваних персональних даних і для попередження адміністратора при виявленні факту несанкціонованого доступу до персональних даних та інших фактів порушення штатного режиму функціонування автоматизованої системи обробки персональних даних.

Засоби імітації моделюють роботу з порушниками при виявленні спроби несанкціонованого доступу до захищуваних персональних даних або програмних засобів. Імітація дозволяє збільшити час на визначення місця і характеру несанкціонованого доступу, що особливо важливо в територіально розподілених мережах, і дезінформувати порушника про місце знаходження захищуваних персональних даних.

Підсистема забезпечення цілісності реалізується переважно операційними системами і системами управління базами даних. Засоби підвищення достовірності та забезпечення цілісності переданих даних і надійності транзакцій, що вбудовуються в операційні системи і системи управління базами даних, засновані на розрахунку контрольних сум, повідомлення про збій у передачі пакету повідомлення, повторі передачі не прийнятого пакету.

Підсистема контролю відсутності декларованих можливостей реалізується в більшості випадку на базі систем управління базами даних, засобів захисту інформації, антивірусних засобів захисту інформації.

Для забезпечення безпеки персональних даних та програмно-апаратної середовища автоматизованої системи обробки персональних даних, що здійснює обробку цієї інформації, рекомендується застосовувати спеціальні засоби антивірусного захисту, які виконують:

- виявлення і (або) блокування деструктивних вірусних впливів на загальносистемне і прикладне програмне забезпечення, що реалізує обробку персональних даних, а також на персональні дані;
- виявлення і видалення невідомих вірусів;
- забезпечення самоконтролю (запобігання інфікування) даного антивірусного засобу при його запуску.

При виборі засобів антивірусного захисту доцільно враховувати наступні фактори:

- сумісність зазначених коштів з штатним програмним забезпеченням автоматизованої системи обробки персональних даних;
- ступінь зниження продуктивності функціонування автоматизованої системи обробки персональних даних за основним призначенням;
- наявність засобів централізованого управління функціонуванням засобів антивірусного захисту з робочого місця адміністратора безпеки інформації в автоматизованій системі обробки персональних даних ;
- можливість оперативного оповіщення адміністратора безпеки інформації в автоматизованій системі обробки персональних даних про всі події та факти прояву програмно-математичних дій;

- наявність докладної документації по експлуатації засоби антивірусного захисту;
- можливість здійснення періодичного тестування або самотестування засобів антивірусного захисту;
- можливість нарощування складу засобів захисту від прояву програмно-математичних дій новими додатковими засобами без істотних обмежень працездатності автоматизованої системи обробки персональних даних і «конфлікту» з іншими типами засобів захисту.

Опис порядку встановлення, налаштування, конфігурування та адміністрування засобів антивірусного захисту, а також порядку дій у разі виявлення факту вірусної атаки або інших порушень вимог щодо захисту від програмно-математичних впливів повинні бути включені в керівництво адміністратора безпеки інформації в автоматизованій системі обробки персональних даних.

Для здійснення розмежування доступу до ресурсів автоматизованої системи обробки персональних даних при міжмережній взаємодії застосовується міжмережеве екранування, яке реалізується програмними та програмно-апаратними міжмережевими екранами. Міжмережевий екран встановлюється між мережею що захищається, яку називають внутрішньою, і зовнішньої мережею. Міжмережевий екран входить до складу мережі, що захищається. Для нього шляхом налаштувань окремо задаються правила, що обмежують доступ з внутрішньої мережі в зовнішню і навпаки.

Підсистема аналізу захищеності реалізується на основі використання коштів тестування (аналізу захищеності) і контролю (аудиту) безпеки інформації.

Засоби аналізу захищеності застосовуються з метою контролю установок захисту операційних систем на робочих станціях і серверах і дозволяють оцінити можливість проведення порушниками атак на мережеве обладнання, контролюють безпеку програмного забезпечення. Для цього вони

досліджують топологію мережі, шукають незахищені або несанкціоновані мережеві підключення, перевіряють налаштування міжмережевих екранів. Подібний аналіз проводиться на підставі детальних описів вразливостей налаштувань засобів захисту (наприклад, комутаторів, маршрутизаторів, міжмережевих екранів) або вразливостей операційних систем або прикладного програмного забезпечення. Результатом роботи засоби аналізу захищеності є звіт, в якому узагальнюються відомості про виявлені вразливості.

Засоби виявлення вразливостей можуть функціонувати на мережевому рівні (у цьому випадку вони називаються «network-based»), рівні операційної системи («host-based») і рівні додатка («application-based»). Застосовуючи скануюче програмне забезпечення, можна швидко скласти карту всіх доступних вузлів автоматизованої системи обробки персональних даних, виявити які використовуються на кожному з них сервіси та протоколи, визначити їх основні параметри і зробити припущення щодо ймовірності реалізації несанкціонованого доступу.

В інтересах виявлення загроз несанкціонованого доступу за рахунок міжмережевої взаємодії застосовуються системи виявлення вторгнень. Такі системи будуються з урахуванням особливостей реалізації атак, етапів їх розвитку і засновані на цілому ряді методів виявлення атак.

Виділяють три групи методів виявлення атак:

- сигнатурні методи;
- методи виявлення аномалій;
- комбіновані методи (що використовують спільно алгоритми, визначені в сигнатурних методах і методах виявлення аномалій).

Для виявлення вторгнень в автоматизовані системи обробки персональних даних 3 та 4 класів рекомендується використовувати системи виявлення мережевих атак, що використовують сигнатурні методи аналізу.

Для виявлення вторгнень в автоматизовані системи обробки персональних даних 1 і 2 класів рекомендується використовувати системи

виявлення мережевих атак, що використовують поряд з сигнатурними методами аналізу методи виявлення аномалій.

Для захисту персональних даних від витоку по технічних каналах застосовуються організаційні і технічні заходи, спрямовані на виключення витоку акустичної (мовної), видової інформації, а також витоку інформації за рахунок побічних електромагнітних випромінювань і наведень.

1.5 Постановка задачі

Мета роботи: обґрунтування вимог до обробки персональних даних в інформаційних комп'ютерних системах банківських установ з розробкою типової політики безпеки відділення банку а також посадових інструкцій спираючись на положення Закону України «Про захист персональних даних»

Задачі:

- проаналізувати нормативну базу з питань захисту персональних даних;
- проаналізувати загрози автоматизованих систем банківських установ;
- розробка рекомендацій щодо захисту персональних даних в інформаційних комп'ютерних системах банківських установ.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Характеристика об'єкта інформаційної діяльності

Організаційна структура банку схожа і з іншими підприємницькими структурами і регламентується Законами України «Про господарські товариства», «Про банки і банківську діяльність» і т. д.

Дія банків, як й інших господарських товариств, ґрунтується на корпоративно-нормативних актах, до яких належать установчий договір і статут.

В Україні банки діють як акціонерні товариства (АТ) та товариства з обмеженою відповідальністю (ТОВ). В обох випадках майнова відповідальність учасників товариства обмежена розміром коштів, вкладених у статутний фонд товариства. Учасники відкритого акціонерного товариства (ВАТ) на суму своєї частки в товаристві отримують акції, які можуть вільно обертатися. Учасники закритого акціонерного товариства (ЗАТ) розподіляють акції між собою, і ці акції не можуть вільно обертатися.

В Україні існує безліч різноманітних банків та їх відділень. Проаналізувавши їхню організаційну структуру можна зробити висновок, що у більшості з них вона схожа.

На сьогоднішній день ринок банківських послуг є досить широким. З розширенням послуг водночас зросла потреба в обробці персональних даних клієнтів банку. Тому виникла потреба в їх автоматизованій обробці даних – це дозволяє ефективно взаємодіяти з клієнтами та і при цьому заощаджувати ресурси банку.

Автоматизована банківська система (АБС) - комплекс програмного і технічного забезпечення, спрямований на автоматизацію банківської діяльності.

Однією з цілей функціонування АБС є обробка персональних даних співробітників і клієнтів банку. У такому випадку, АБС класифікується як

інформаційна система персональних даних (ІСПДн) і повинна бути захищена у відповідність до вимог Закону України "Про захист персональних даних".

Прикладні програми АБС представляють собою набір програмних модулів, функціонально та інформаційно пов'язаних між собою. Функціональні зв'язку модулів забезпечують необхідну послідовність їх виконання, а інформаційний зв'язок визначається використанням модулем у своїй роботі інформації, згенерованої іншим модулем. Як правило, обмін інформацією між модулями йде через базу даних. Один модуль пише інформацію в базу даних, а інший її прочитує при реалізації своїх функцій. [9].

Аналіз проектних рішень ряду АБС показав, що ці модулі групуються приблизно в однакові комплекси. Типовий склад цих комплексів зображений на рисунку 2.1.

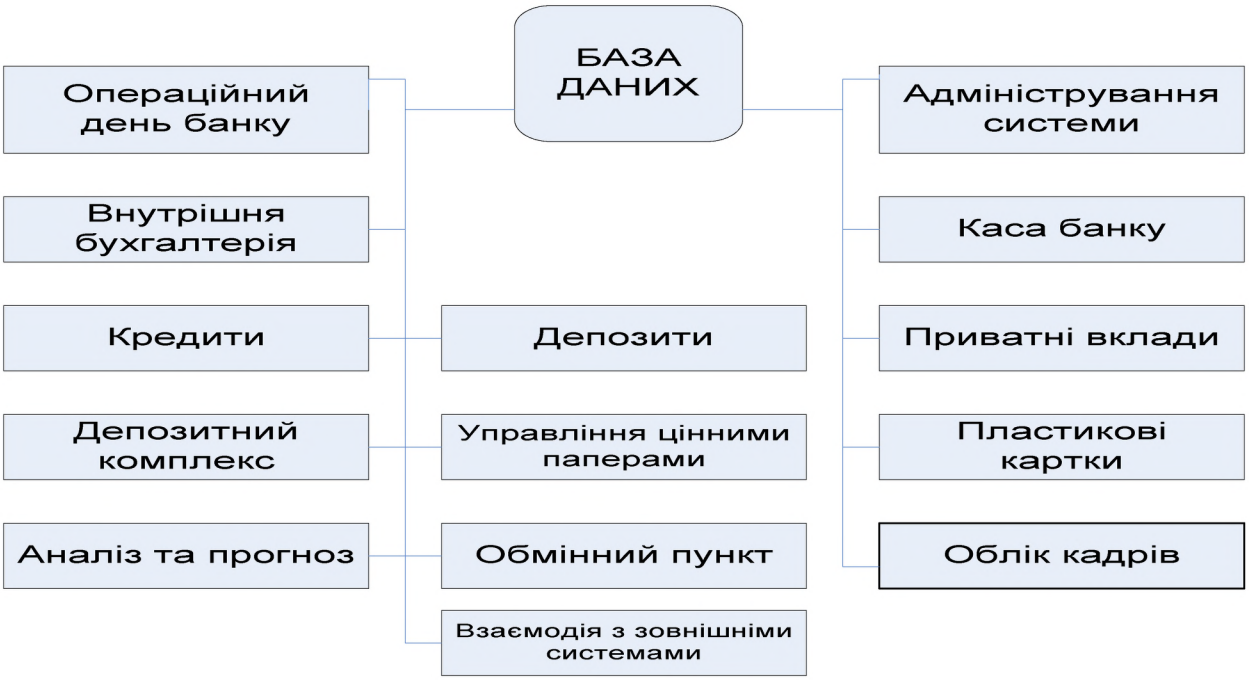

Рисунок 2.1 – Функції, що вирішуються автоматизованою банківською системо обробки інформації.

Функції, що вирішуються автоматизованою банківською системою (АБС), можна розділити на три великі групи:

- Облікові функції,
- Аналітичні функції,
- Технологічні функції.

Опції автоматизованих банківських систем (АБС):

- операційний день;
- операції на фондовому ринку, робота банку з цінними паперами;
- внутрішньогосподарська діяльність;
- роздрібні банківські послуги;
- дистанційне банківське обслуговування;
- електронні банківські послуги;
- розрахунковий центр і платіжна система (карткові продукти);
- інтеграція бек-офісу банку з його зовнішніми операціями;
- управління діяльністю банку, реалізація бізнес-логіки, контроль, облік, у тому числі податковий, і звітність;
- управління ризиками та стратегічне планування;
- програми лояльності клієнтів, маркетингова, рекламна та PR-служби.

Розглянуте відділення ПАТ КБ "Правекс-Банк" є типовим відділенням банківської установи, на прикладі якого проілюстровано обґрунтування вимог до обробки персональних даних в автоматизованій системі установи.

2.1.1 Вид діяльності

Об’єкт інформаційної діяльності займається:

- прийняттям вкладів (депозитів) від юридичних і фізичних осіб;
- відкриттям та веденням поточних рахунків клієнтів і банків-кореспондентів, у тому числі переказом грошових коштів з цих рахунків за допомогою платіжних інструментів та зарахування коштів на них;
- наданням кредитів на купівлю житла, для придбання автомобіля вітчизняного чи іноземного виробництва у будь-якому автосалоні України, наданням коштів для відкриття свого бізнесу, відпочинку, отримання освіти, ремонту, будівництва тощо.
- депозитарною діяльністю збереження цінних паперів;
- лізингом;

- послугами з відповідального зберігання та надання в оренду сейфів для зберігання цінностей та документів;
- випуском, купівлею, продажем і обслуговуванням чеків, векселів та інших оборотних платіжних інструментів;
- випуском банківських платіжних карток і здійснення операцій з використанням цих карток;
- наданням консультаційних та інформаційних послуг щодо банківських операцій.
- операціями з валютними цінностями.
- організацією купівлі та продажу цінних паперів за дорученням клієнтів.
- здійсненням операцій на ринку цінних паперів від свого імені (включаючи андеррайтинг).
- здійсненням інвестицій у статутні фонди та акції інших юридичних осіб та інше.

Об'єкт інформаційної діяльності зобов'язаний:

- забезпечувати комплексне обслуговування клієнтів, включаючи видачу й обслуговування пластикових карт;
- забезпечувати захист інформації в автоматизованих системах відповідно до законодавства;
- забезпечувати захист персональних даних, отриманих від клієнтів банку, згідно із законодавством;
- надавати консультації з питань, пов'язаних з банківськими послугами.

2.1.2 Персонал об'єкта інформаційної діяльності

Штат співробітників Кам'янського відділення ПАТ АКБ «Правекс-Банк» включає 10 осіб:

- Начальник відділу банку: 1 чол.
- Головний бухгалтер: 1 чол.
- Бухгалтер: 1 чол.
- Касир: 2 чол.

- Менеджер з продажу: 1 чол.
- Адміністратор безпеки відділення: 1 чол.
- Охоронці: 2 чол.
- Прибиральниця: 1 чол.

2.1.3 Режим роботи об’єкта інформаційної діяльності

Графік роботи відділення: з понеділка по п'ятницю з 9:00-19:00, субота з 9:00-16:00. Неділя-вихідний день.

Робочий день з 9.00 до 18.00.

Вихідні: субота, неділя.

Прибирання здійснюється кожні два дні в період з 8.00 до 9.00

Охороняється об’єкт цілодобово.

2.1.4 Інформація що циркулює на об’єкті інформаційної діяльності

На об’єкті інформаційної діяльності циркулює така інформація з обмеженим доступом:

- Персональні дані фізичних та юридичних осіб;
- Інформація про фінансово-економічну діяльність відділення банку;
- Інформація про формування фінансових та юридичних договорів з фізичними та юридичними особами;
- Інформація про джерела та обіг коштів.

2.1.5 Характеристика будівлі

Кам’янське відділення ПАТ КБ «Правекс-Банк» розташоване в шестиповерховій будівлі. Займає площу 200 м. кв.

Контрольована зона знаходиться в межах стін будівлі.

З південного боку розташований торговий центр, відстань до якого 200 м, з інших сторін знаходяться житлові будинки.

У відділені встановлено автономне опалення. Каналізаційний канал має вихід за межі контрольованої зони. Водопостачання від міського

водоканалу і, також, виходить за межі контрольованої зони. У всіх кабінетах і відділах встановлені кондиціонери.

Комп'ютери об'єднані в локальну мережу, є вихід в Інтернет. Інтернет надає ВАТ «Укртелеком». Також присутні телефонні лінії, прокладені під землею, від постачальника послуг ВАТ «Укртелеком». Електропостачання приміщення здійснюється від міської підстанції. Даний об’єкт включає в себе такі приміщення:

1. Кабінет начальника відділення
2. Кабінет головного бухгалтера
3. Кабінет заступника головного бухгалтера
4. Кабінет адміністратора безпеки
5. Каса (2 вікна)
6. Кабінет менеджера з продажу

2.1.6 Загальна характеристика об’єкта інформаційної діяльності

Таблиця 2.1 – Характеристика об’єкта інформаційної діяльності

1	Назва організації	Кам’янське відділення ПАТ КБ «Правекс-Банк»
2	Форма власності	Публічне акціонерне товариство
3	Тип організації, наявність структурних підрозділів	Публічне акціонерне товариство, з структурними підрозділами
4	Вид діяльності банку	Надання різноманітних банківських послуг
5	Розміщення відділення	1 офіс на одному майданчику будівлі (1 поверх), який складається з трьох відділів (юридичний, каса (2 вікна), кабінету начальника відділення, кабінету заступника начальника відділення, кабінету головного бухгалтера, кабінету заступника головного бухгалтера
6	Контрольована зона	Обмежена стінами приміщень
7	Наявність розгалуженої ІС	нема
8	Персонал організації (весь)	Начальник відділу банку: 1 чол; чол;Головний бухгалтер: 1 чол;Бухгалтер: 1 чол;Касир: 2 чол;Менеджер з продажу: 1 чол; Адміністратор безпеки відділення: 1 чол; Охоронці: 2 чол; Прибиральниця: 1 чол.

Продовження таблиці 2.1

9	Персонал, відповідальний за роботу ІС	Адміністратор безпеки
10	Персонал, який використовує роботу в ІС	Головний бухгалтер, бухгалтер, начальник відділення, адміністратор безпеки, юрист, касир.
11	Тип циркулюючої інформації	Конфіденційна інформація
12	Види циркулюючої інформації	Паперова, електронна
13	Основні інформаційні потоки підприємства	Надання різноманітних банківських послуг, обробка інформації про клієнтів, формування звітів по фінансовій діяльності, формування договорів з фізичними та юридичними особами, формування договорів з партнерами, обробка інформації про джерела коштів, зв'язки і можливості керівництва, формування даних про партнерів.
14	За рахунок чого	ПК бухгалтерії, паперовий архів, магнітних носіїв, корпоративної електронної пошти.
15	Другорядні інформаційні потоки підприємства	Обробка копій документів, копій факсів, платежів
16	За рахунок чого	Факси, принтери.
17	Комп'ютерна мережа підприємства	1 ПК бухгалтера, 1 ПК головного бухгалтера,1 ПК начальника відділення, 1 ПК менеджера з продажу, 2 РС касирів, 1 концентратор, 1 ADSL-модем
18	Тип ОС	операційна система, встановленою на серверах (MS Windows Server 2022 Enterprise Edition)) + операційна система, встановленою на робочих станціях (MS Windows 11);
19	Основне прикладне ПЗ	Онлайн-бухгалтерія Dilovod, СУБД Interbase 2020
20	Другорядне ПЗ	MS Office XP/07, антивірус Avast Professional
21	Протоколи	TCP/IP, HTTP, FTP

2.1.7 Класифікація інформаційної системи та її об’єктів

Класифікація інформаційної системи та її об’єктів представлена в Таблиці 2.2

1. За доступністю або наявністю:

Д4 - дуже важлива інформація (суб'єкт буде працювати, але короткий час);

Д3 - важлива інформація (суб'єкт може працювати без цієї інформації деякий час, але вона скоро знадобиться);

Д2 - корисна інформація (без інформації можна працювати, але її використання економить час);

Д1 - не суттєва інформація (застаріла або не використовувана, що не впливає на роботу суб'єктів інформація);

Таблиця 2.2 - Класифікація інформаційної системи та її об’єктів

№	Найменування	По доступності	По цілісності	По конфіденційності
1	Фінансова інформація (звіти для податкової інспекції, фінансові звіти, бухгалтерський облік)	Д4	Ц3	К3
2	Інформація про клієнтів	Д4	Ц3	К4
3	Інформація про працівників	Д1	Ц1	К2
4	Договори з клієнтами	Д3	Ц2	К3
5	Інформація про партнерів банку	Д2	Ц1	К2

2. За несанкціонованої модифікації або цілісності:

Ц3 - дуже важлива інформація (несанкціоноване зміна призводить до невірної роботі організації або його частини через деякий час, якщо не будуть зроблені деякі дії; наслідки такої модифікації незворотні);

Ц2 - важлива інформація (несанкціоноване зміна призводить до неправильної роботи організації через деякий час, якщо не будуть зроблені деякі дії; наслідки такої модифікації оборотні);

Ц1 - значуща інформація (несанкціоноване зміна позначиться через деякий час, але не призведе до збою в системі; наслідки такої модифікації оборотні);

3. За розголошенню чи конфіденційністю:

К4 - дуже важлива інформація (розголошення призведе до значних матеріальних втрат, якщо не будуть прийняті які-небудь заходи);

К3 - важлива інформація (розголошення призведе до деяких матеріальним або моральних втрат, якщо не будуть зроблені деякі дії);

К2 - значуща інформація (приносить моральну шкоду, може бути використана в певний момент);

К1 - малозначима інформація (може принести моральну шкоду в дуже рідкісних випадках);

2.1.8 Модель інформаційних потоків об’єкта інформаційної діяльності

Рисунок 2.2 Модель інформаційних потоків об’єкта інформаційної діяльності

1. Касир здійснює операції з приймання, обліку, видачі та зберігання грошових коштів і цінних паперів з обов'язковим дотриманням правил, що забезпечують їх збереження. Отримує за оформленими відповідно до встановленого порядку документами кошти і цінні папери в установах банку для виплати робітникам і службовцям заробітної плати, премій, оплати відряджень і інших витрат. Веде на основі прибуткових і витратних документів касову книгу, звіряє фактичну наявність грошових сум і цінних паперів з книжковим залишком. Складає описи старих купюр, а також відповідні документи для їх передачі до установ банку з метою заміни на нові.

Передає відповідно до встановленого порядку грошові кошти інкасаторам. Складає касову звітність.

2. Бухгалтер здійснює організацію бухгалтерського. Вживає заходів з нагромадження фінансових коштів для забезпечення фінансової стійкості підприємства. Здійснює взаємодію з банками з питань розміщення вільних фінансових коштів на банківських депозитних внесках (сертифікатах) і придбання високоліквідних державних цінних паперів, контроль за проведенням облікових операцій з депозитними і кредитними договорами, цінними паперами. Веде роботу по забезпеченню суворого дотримання штатної, фінансової і касової дисципліни, кошторисів адміністративно-господарських та інших витрат, законності списання з рахунків бухгалтерського обліку нестач, дебіторської заборгованості та інших втрат, збереження бухгалтерських документів, оформлення і здачі їх у встановленому порядку в архів. Бере участь у розробці і впровадженні раціональної планової та облікової документації, прогресивних форм і методів ведення бухгалтерського обліку на основі застосування сучасних засобів обчислювальної техніки. Забезпечує складання балансу й оперативних зведених звітів про доходи і витрати коштів, про використання бюджету, іншої бухгалтерської та статистичної звітності, подання їх у встановленому порядку до відповідних органів.

3. Менеджер з продажу здійснює залучення нових клієнтів, підтримку відносин з старими клієнтами, складає договори, рахунки та інші документи, проводить консультування клієнтів з різних питань пов'язаних з наданням банківських послуг.

4. Начальник відділення здійснює керівництво діяльністю відділу банку і несе персональну відповідальність за якість виконуваних відділом робіт і результати його діяльності. Забезпечує підготовку проектів поточних і перспективних планів робіт та здійснює контроль за виконанням стоять перед відділом банку завдань. Організовує систематичний аналіз діяльності відділу банку і на його основі готує необхідні проекти документів з питань, що

входять в його компетенцію. Готує проекти положення про відділ банку і посадових інструкцій працівників відділу. Очолює розробку проектів нормативних, методичних та інструктивних матеріалів по напрямках діяльності відділу банку. Вивчає ефективність діючих правил та інструкцій, що стосуються діяльності банку і одночасно стосуються роботи відділу банку. На основі аналізу специфіки ринку банківських послуг в різних регіонах вносить пропозиції щодо вдосконалення зазначених документів. Вживає заходів до впровадження в роботу відділу банку найбільш ефективних методів і технологій банківської діяльності. Сприяє створенню необхідних умов праці і сприятливого морально-психологічного клімату в колективі. Забезпечує дотримання працівниками відділу банку трудової дисципліни. Дозволяє оперативні питання, готує довідки, проекти відповідей на заяви, листи і скарги громадян, що стосуються роботи відділу банку. Здійснює контроль, надає практичну і методичну допомогу відповідним структурним підрозділам банку, у тому числі з виїздом на місце. Забезпечує збереження комерційної таємниці про діяльність банку і його клієнтів. Забезпечує правильне застосування в роботі відділу банку діючого законодавства і ведення діловодства в установленому порядку.

2.2 Класифікація загроз банківських установ

Загрози безпеці банків за походженням поділяються на внутрішні та зовнішні. У свою чергу, як перші, так і другі за направленістю і характером впливу на банки можуть бути економічними, фізичними та інтелектуальними. Класифікація загроз представлена на рис. 2.3

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

Основними причинами виникнення економічних загроз можуть бути: недостатня адаптація банківської системи до постійно змінних умов ринку;

загальна неплатоспроможність суб'єктів господарювання; зростаюча злочинність; споживчий менталітет значної кількості громадян; низький рівень трудової дисципліни та відповідальності працівників банківських установ; недостатнє правове регулювання банківської діяльності; низький професійний рівень частини керівного складу і працівників банку.

Фізичні загрози реалізуються у формі крадіжок, пограбувань майна та

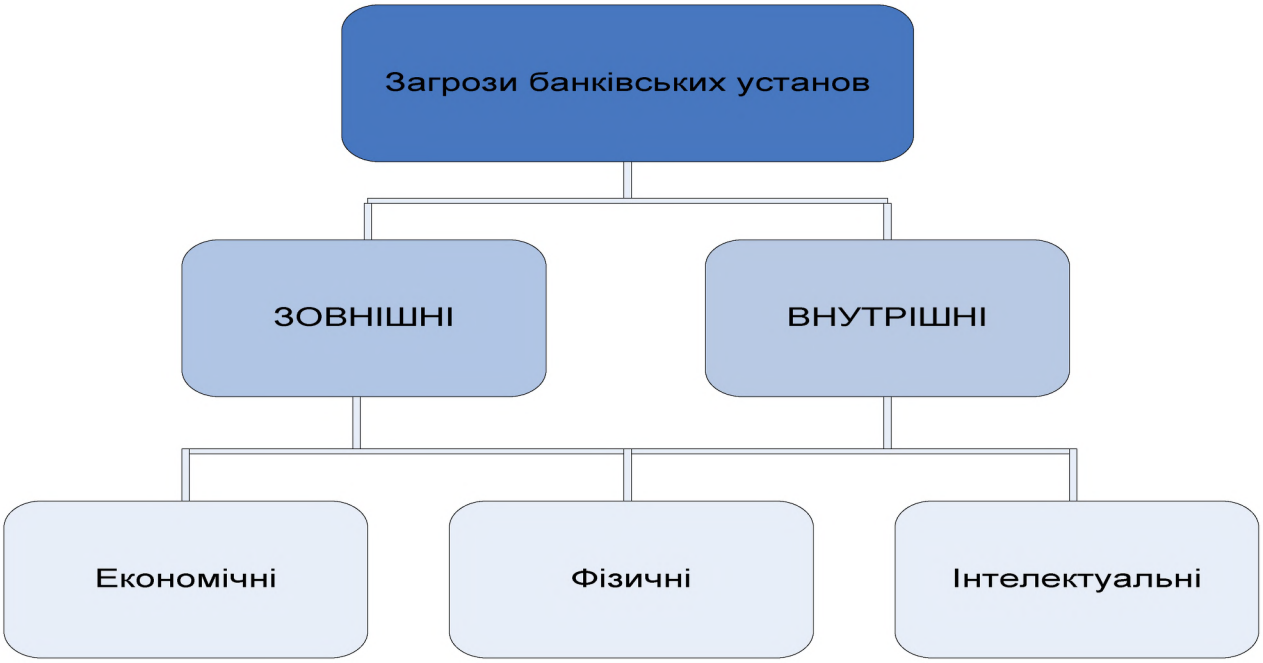

Рисунок 2.3- Загрози банківських установ

коштів банків, поломок, виведення із ладу обладнання банків, неефективної його експлуатації. У результаті реалізації таких загроз завдаються прямі збитки банкам, пов'язані з втратою своєї власності та необхідністю внесення додаткових витрат 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, а також можуть бути реалізованими у формі різного роду

соціальних конфліктів навколо банківських установ або в них самих. Результатом реалізації таких загроз можуть бути збитки банків, погіршення їх іміджу, соціальна чи психологічна напруженість навколо установ банків або в їх колективах. Причинами таких загроз, як правило, є загострення конкуренції на регіональних ринках банківських послуг, неефективна кадрова політика банків, порушення принципу гласності результатів банківської діяльності, відсутність або низька ефективність заходів інформаційного режиму в банках.

Зовнішні загрози для безпеки банків, можуть утворюватись:

- спецслужбами іноземних держав, пов'язаними з ними особами та організаціями, метою діяльності яких є добування економічної інформації;
- вітчизняними й іноземними кримінальними елементами і структурами;
- конкурентами;
- засобами масової інформації;
- окремими представниками державних установ;
- приватними детективними фірмами;
- колишніми працівниками банків;
- консультантами та радниками, які не є працівниками банківських установ;
- клієнтами та партнерами;
- контролюючими органами та аудиторськими організаціями;
- стихійними лихами.

У свою чергу, внутрішні загрози в основному утворюються:

- працівниками банків;
- недосконалими технологіями банківського виробництва та неповним;
- його врегулюванням нормативними актами банків;
- через недосконалу систему безпеки банків та захисту їх інформації.

Внутрішні загрози, як правило, обумовлюються наявністю передумов для негативних, протиправних дій персоналу банку, безконтрольним використанням засобів виробництва, порушенням режимів діяльності банку.

Враховуючи, що значна частина внутрішніх загроз реалізуються з участю або за сприяння персоналу банків, можна вважати, що основним джерелом таких загроз є банківські працівники.

Виходячи з цього внутрішні загрози банкам можуть утворюватися внаслідок:

- непрофесійних дій працівників банків;
- низького стану виховної та профілактичної роботи в банках;
- недосконалої системи заробітної плати та стимулювання праці персоналу банків;
- порушень правил кадрової роботи, невідповідності кадрової політики умовам роботи банків;
- психологічних та комунікаційних особливостей працівників банків;
- відсутності нормативної бази банків, яка б установлювала режими їх діяльності та правила поведінки персоналу;
- низького стану трудової і виробничої дисципліни, слабкої вимогливості керівного складу банків.

Реалізація загроз має свої особливості відповідно до об'єктів загроз. Для більш повного розуміння можна зазначити, що основними об'єктами загроз банку можуть бути персонал, фінанси, матеріальні цінності та інформація банку.

Реалізація загроз щодо персоналу банку може призводити до моральних або фізичних страждань окремих осіб, втрати ними своєї власності, нанесення економічної шкоди.

Загрози фінансам банку можуть реалізовуватись через крадіжки фінансових ресурсів банку, шахрайство з коштами банку, фальсифікацію фінансових документів та підроблення банкнот, недосконалі технології банківського виробництва.

Матеріальним цінностям банку може загрожувати пошкодження будівель, приміщень та іншої нерухомості, виведення із ладу засобів зв'язку і

систем комунального обслуговування, пошкодження, крадіжки банківського обладнання, техніки, транспортних засобів.

Інформаційні загрози можуть реалізовуватись через несанкціоноване ознайомлення сторонніх осіб з відомостями банку, що мають обмежений доступ, модифікацію банківської інформації, її знищення або розголошення.

2.2.1 Типова модель загроз

У Таблиці 2.3 представлено модель загроз інформації в інформаційній системі. Для кожної загрози визначено властивість інформації, яка буде порушено в разі її реалізації.

Таблиця 2.3 – Типова модель загроз

№	Загроза	Властивості інформації, які порушуються		
		К	Ц	Д
1	Ненавмисне знищення інформації співробітником, який працює з нею		+	+
2	Шантаж, підкуп, психологічний вплив на персонал конкурентами з метою примушення співробітника видалити інформацію з обмеженим доступом		+	+
3	Шантаж, підкуп, психологічний вплив на персонал конкурентами з метою отримання інформації з обмеженим доступом	+		
4	Знищення матеріальних носіїв секретної інформації, інформації внаслідок пожежі		+	+
5	Умисне знищення технічних засобів, носіїв інформації, ПЗ, інформації з обмеженим доступом співробітником, впровадженим з конкуруючої організації		**+**	**+**

Продовження таблиці 2.3

6	Крадіжка, підміна паролів з метою ознайомлення з секретною інформацією	+	+	+
7	Порушення нормальної роботи електроживлення технічних засобів			+
8	Помилки співробітників при роботі з ПЗ, технічними засобами, які тягнуть за собою зміну, модифікацію інформації		+	+
9	Перехоплення зловмисниками інформації за рахунок ПЕМВ від технічних засобів, наведень по лініях електроживлення, наведень по стороннім лідерів	+		
10	Перехоплення зловмисниками інформації по акустичному каналу від засобів виведення, при обговоренні питань	+		
11	Перехоплення інформації зловмисником при підключенні до каналів передачі інформації до віддаленої ЛВС	+		
12	Навмисна модифікація інформації співробітниками, які полягають у змові зі зловмисниками.		+	+
13	Зараження ПЗ вірусами через мережу Інтернет, заражені матеріальні носії	+	+	+
14	Невиконання співробітниками правил і норм, встановлених в банку	+	+	+
15	Крадіжка технічних засобів, носіїв інформації, інформації	+	+	+
16	Модифікація інформації зловмисником при передачі по каналах зв'язку до віддаленої ЛВС	+	+	+

2.2.2 Характеристика користувачів автоматизованої системи

Користувачі автоматизованої системи обробки персональних даних в відділені банку розділені за рівнями повноважень, з урахуванням необхідності співробітників роботи з певними ресурсами даної системи на наступні категорії:

- Працівників, яким надано доступ до певної секретної інформації, яка необхідна для роботи. До яких саме ресурсів дозволяється доступ кожному співробітнику визначає директор і надає інформацію системного адміністратора, який виконує розмежування доступу

(бухгалтер, головний бухгалтер, працівник юридичного відділу, касир, начальник відділення його заступник).

– Працівники, яким надані повноваження забезпечувати управління КС, забезпечувати її безпеку, виявляти та попереджати можливі загрози (адміністратор безпеки).

2.2.3 Модель порушника

Таблиця 2.4 Зведена характеристика ймовірного порушника

Порушник автоматизованої системи	Мета порушника	За місцем дії	Вірогідність реалізації загрози
Внутрішній (співробітники)	-отримання необхідної інформації в корисливих цілях; -зміна, модифікація інформації що містить персональні дані клієнтів банку, і їх використання у власних цілях.	З робочих місць користувачів автоматизованої системи обробки персональних даних	II
		З доступом до баз даних, архівів з персональними даними	II
Зовнішній (конкуренти, клієнти, хакери)	Крадіжка, знищення, підміна інформації що містить персональні дані клієнтів банку з метою нанесення збитків, а також удару по репутації банку.	Без доступу на контрольовану територію	III
		Усередині приміщень, але без доступу до технічних засобів автоматизованої системи	III

Оцінка ймовірності реалізації загрози:

I - прагне до значення 1(висока вірогідність);

II - прагне до значення 0,5(середня вірогідність);

III - прагне до значення 0(низька вірогідність).

В якості потенційного порушника інформаційної безпеки Кам'янського відділення ПАТ КБ «Правекс-Банк» розглядається особа або група осіб, які перебувають або не перебувають у змові, які в результаті навмисних або ненавмисних дій можуть реалізувати різноманітні загрози інформаційної безпеки, які можуть призвести до втрати чи неправомірного використання персональних даних клієнтів банку зловмисниками, і завдати моральної та /

або матеріальну шкоду інтересам відділення банку. Потенційним порушником може бути як співробітник даного відділення, так і людина яка не є працівником відділення (конкурент, зловмисник).

2.3 Розробка рекомендацій, щодо захисту інформації яка обробляється в автоматизованій системі

У зв’язку набранням чинності Закону про захист персональних даних для мінімізації ризиків відділення банку, яке фактично є чи планує бути власником бази персональних даних, можна зробити таке:

- закріпити внутрішнім порядком, наказом або іншим документом мету обробки персональних даних, їх зміст та обсяг, процедуру їх обробки, а також визначити/призначити структурний підрозділ/відповідальну особу, на який/яку буде покладено обов'язок організовувати роботу, пов'язану із захистом персональних даних при їх обробці, відповідно до вимог Закону (згідно з п. 5 ст. 24 Закону);
- отримати письмову згоду на обробку даних від кожного суб'єкта персональних даних, внесеного до бази даних, передбачивши максимально широкий список видів обробки персональних даних та її цілей;
- у випадках, коли йдеться про фактично існуючі бази персональних даних, рекомендуємо додатково упевнитися в тому, що збір даних здійснювався відповідно до описаних вище вимог. Якщо ж описані вимоги при обробці (і зборі) інформації не дотримувалися, необхідно забезпечити відповідно до зазначеного порядку отримання документованої згоди суб'єктів персональних даних, інформація про які міститься в таких базах. Якщо окремі суб'єкти з яких-небудь причин відмовляються надати таку згоду, рекомендуємо видалити інформацію про них з відповідних баз.

У цьому контексті необхідно звернути увагу на ситуацію, коли певна особа (наприклад, банк) на момент набрання чинності Законом вже володіє

базою персональних даних (клієнтів), однак згоду на обробку даних вдається отримати не від всіх суб'єктів (клієнтів). Водночас видалення персональних даних таких суб'єктів заперечуватиме інтересам банку, бо вони, наприклад, є боржниками. На даний момент неможливо однозначно трактувати цю ситуацію.

Персональні дані у банку можуть знаходитись у таких системах:

- автоматизована система обробки персональних даних (АСОПнД);
- системи Клієнт-Банк;
- системи миттєвого переказу грошей;
- бухгалтерські системи обліку;
- кадрові системи обліку;
- корпоративна інформаційна система;
- внутрішній web-портал.

Згідно з вимогами методичних документів для захисту персональних даних, спільним для всіх видів інформаційних систем персональних даних, є наступні підсистеми:

- підсистема контролю доступу;
- підсистема реєстрації і обліку;
- підсистема забезпечення цілісності;
- підсистема міжмережевий безпеки.

Якщо інформаційна система персональних даних підключена до мережі Інтернет, то необхідно додатково використовувати наступні підсистеми:

- підсистема антивірусної безпеки;
- підсистема виявлення вторгнень;
- підсистема аналізу захищеності.

Також необхідно використовувати електронні замки та / або електронні ключі для надійної ідентифікації і автентифікації користувачів.

Якщо інформаційна система персональних даних є розподіленою додатково для запобігання несанкціонованого доступу, шляхом відділення інформації, що захищається від загальнодоступної, необхідно використати

криптографію при передачі персональних даних по незахищених каналах зв'язку, а також, електронний цифровий підпис, для підтвердження достовірності даних.

Така розбивка на підсистеми і формування на їх основі переліку продуктів для захисту персональних даних є загальноприйнятою і використовується в більшості випадків.

Якщо додатково пред'являються вимоги щодо забезпечення інших властивостей інформаційної безпеки, таких як забезпечення цілісності, доступності, а також їх похідних (неспростовності, підзвітність, адекватність, надійність тощо), то така інформаційна система персональних даних стає спеціальною. У більшості випадків будь-яка інформаційна система персональних даних буде спеціальної, тобто, крім класів персональних даних для визначення механізмів захисту потрібно керуватися створюваної для цього моделлю загроз.

Для того щоб зменшити і спростити заходи щодо захисту персональних даних, можна використати різні способи. Нижче наведені найбільш типові способи, що дозволяють зменшити вартість засобів захисту.

Зменшення кількості майданчиків

Як було показано вище, якщо інформаційна система розподіленою, то до її захисту пред'являються підвищені вимоги, щоб їх зменшити потрібно спробувати відмовитись від розподілених інформаційних системах персональних даних.

При розподіленій інформаційна система персональних даних персональних даних знаходяться на різних майданчиках, персональних даних передаються по неконтрольованим банком каналах зв'язку, а в загальному випадку це означає, що персональні дані виходять або залишають контрольовану зону. Тоді, перш за все, необхідно локалізувати персональні дані, зменшивши кількість майданчиків, на яких вони знаходитимуться. У деяких випадках це реально, але якщо розглядати АСОПнД, то такої можливості, швидше за все, не буде.

Зменшення кількості серверів

Якщо інформаційна система персональних даних є локальною, тобто функціонує в межах локальної мережі банку, то найбільш простим способом зменшення вартості витрат на захист буде зменшення кількості серверного обладнання, на яких присутні і / або обробляються персональних даних.

Поділ інформаційної системи за допомогою мереж на сегменти

Для того щоб зменшити кількість персональних даних, а значить і зменшити вартість засобів захисту, гарним способом є поділ інформаційних мереж на сегменти, в яких ведеться обробка персональних даних. Для цього необхідно встановити і використовувати міжмережеві екрани, до портів яких слід приєднати сегменти з персональних даних. Часто все серверне обладнання розташоване в демілітаризованій зоні, тобто в сегментах відокремлених від загальнодоступних і банківських мереж міжмережевими екранами. Цей спосіб також вимагає істотного «перекроювання» інформаційних мереж. Існує метод, заснований на, так званому, «лінійному шифруванні», тобто шифруванні каналу клієнт-клієнт, клієнт-сервер, сервер-сервер. Таке шифрування мережевого трафіку може бути реалізовано при використанні спеціальних засобів захисту.

Розподіл баз даних на частини

Припустимо, що є база даних, що складається з тисячі записів: П.І.Б. і сума внеску.

Табл.1 БД П.І.Б. і сума внеску

П.І.Б.	Сума вкладу
Коваленко	100 000
Петренко	200 000
Сидоренко	300 000

Це автоматично визначає клас інформаційної системи персональних даних як найбільш високий, що означає суттєву небезпеку від розкриття даних і тим самим спричиняє необхідність застосування дорогих засобів захисту.

Створимо дві інші бази даних. Введемо додатковий унікальний ідентифікатор. Розділимо таблицю на дві частини, у першу помістимо поля П.І.Б та ідентифікатор, в іншу ідентифікатор та суму вкладу.

Табл.2. Нова база даних прізвищ

П.І.Б.	Ідентефікатор
Коваленко	000 0001
Петренко	000 0002
Сидоренко	000 0003

Таким чином, якщо кожен співробітник може відображати лише одну з цих нових баз даних, то захист персональних даних істотно спрощується, якщо не зводиться нанівець.

Табл.3 Нова база даних вкладів

П.І.Б.	Сума вкладу
000 0001	1000 000
000 0002	200 000
000 0003	300 000

Очевидно, що цінність такої бази даних істотно нижче, ніж вихідної. Обидві ж бази даних будуть знаходитися на найбільш захищеному сервері. У реальності, полів у базі даних набагато більше, проте даний принцип може

працювати практично в кожному випадку, тому що кількість значущих з точки зору безпеки персональних даних полів не так вже й велике, а скоріше дуже обмежена. У граничному випадку можна зберігати ключові відповідності на ПК, що не входить в локальну мережу або навіть не використовувати автоматизовану обробку.

Знеособлювання Персональних даних

Згідно з визначенням з ст. 2 Закону «Про захист персональних даних», знеособлення ПДН – вилучення відомостей, які дають змогу ідентифікувати особу. З цього визначення випливає серія способів, за допомогою яких можна отримати ПнД, за якими неможливо визначити приналежність ПнД. Наприклад, якщо для цілей обробки не важливі точні дані певних полів, їх можна або не відображати, або відображати лише діапазони, в які вони потрапляють. Наприклад, вік 20-30, 30-40 і т.д. Адреса можна «округлити» до області або міста: Дніпропетровська, Кам'янське.

2.3.1 Рекомендації щодо комплексу заходів по захисту інформації з персональними даними, яка зберігається у архіві

Для того, щоб ідентифікувати працівників, яким потрібен доступ до приміщення де зберігаються бази персональних даних, передбачені такі заходи, які дозволять не допустити ознайомленню з секретною інформацією сторонніх осіб, які не мають права доступу до неї.

Для входу в приміщення пропонується встановити біометричну систему розпізнавання особистості по відбитку пальців. Даний вид біометричної автентифікації зручний в експлуатації, займає небагато часу, не доставляє психологічного дискомфорту людини і має високу надійність.

Для входу в приміщення пропонується використовувати смарт-карти. Працівники повинні мати при собі смарт-карти і знати свій ПІН-код. Вимога двох чинників значно зменшує вірогідність несанкціонованого доступу до архіву.

2.3.2 Рекомендації щодо заходів захисту інформації від випадкового видалення

- Розміщення найбільш цінної інформації з персональними даними на захищених від запису дисках.

- Швидке відновлення помилково видалених файлів за допомогою спеціальних програм. Для відновлення помилково видалених файлів існують спеціальні програми. В операційній системі Windows копії вилучених файлів автоматично розміщуються у спеціальну папку (каталог) - «Кошик», звідки в разі потреби їх можна відновити. Якщо ж документ був вилучений і з кошика, то відновити його можна за допомогою програми EasyRecovery. EasyRecovery - пакет програм, що дозволяють відновлювати дані на жорсткому диску після їх видалення з кошика, помилкового форматування, вірусної атаки або збою в роботі системи або програми. На випадок можливих збоїв при завантаженні операційної системи EasyRecovery дозволяє створити аварійну дискету, після завантаження з якою можна буде відновити дані, перенісши їх на інший диск. Пакет призначений для використання в Windows і DOS.

2.3.3 Рекомендації щодо заходів захисту інформації від збоїв в роботі пристроїв

- Періодична перевірка справності обладнання (зокрема поверхні жорсткого диска). Іноді для виправлення помилок використовується спеціальна процедура - коригуючий код.
- Періодична оптимізація (дефрагментація) диска для раціонального розміщення файлів на ньому, прискорення роботи та зменшення його зносу.
- Наявність завантажувальних (системних) дискет або дисків, з яких можна запустити комп'ютер (тобто завантажити операційну систему) у разі збоїв системного диска. Наприклад, створення LiveCD дистрибутиву необхідного програмного забезпечення яких програм.

— Поділ повноважень полягає у визначенні для будь-якої програми і будь-якого працівника в системі мінімального кола повноважень. Це дозволяє зменшити збитки від збоїв і випадкових порушень і скоротити ймовірність навмисного або помилкового застосування повноважень.

2.3.4 Рекомендації щодо захисту від випадкового видалення (зміни) інформації іншого працівника

Необхідно ретельно розставляти права на всі ресурси, щоб інші працівники не могли модифіковані чужі файли. Виняток робиться для адміністратора безпеки, який повинен мати всі права на всі ресурси, щоб бути здатним виправити помилки працівників банку, програм і т. д.

2.3.5 Рекомендації щодо запобігання видалення інформації через неузгодженість дій

Працівники повинні зберігати цінну інформацію в місцях, відомих адміністратору. Якщо працівник банку зберігає інформацію в будь-яких інших місцях - вся відповідальність за збереження лягає на працівника. При цьому адміністратор безпеки не повинен видаляти без відома користувача ніякі «незрозумілі» папки з комп'ютера користувача. Перед переустановлення операційної системи слід обов'язково копіювати весь вміст розділу (на якій буде встановлена ОС) на сервер, на інший розділ або на CD / DVD.

2.3.6 Рекомендації щодо резервного копіювання для запобігання втрати інформації

Резервне копіювання необхідно для можливості швидкого і недорогого відновлення інформації (документів, програм, настройок і т. д.) у випадку втрати робочої копії інформації з якої-небудь причини. Крім цього вирішуються суміжні проблеми:

— Дублювання даних

— Передача даних і робота з загальними документами

Для резервного копіювання дуже важливим питанням є вибір відповідної схеми ротації носіїв. Найбільш часто використовують схему одноразового копіювання-це найпростіша схема, що не передбачає ротації носіїв. Всі операції проводяться вручну. Перед копіюванням адміністратор задає час початку резервування, перераховує файлові системи або каталоги, які потрібно копіювати. Цю інформацію можна зберегти в базі, щоб її можна було використовувати знову. При одноразовому копіюванні найчастіше застосовується повне копіювання. Запис резервних копій проводиться на жорсткий диск комп'ютера.

Дублювання інформації є одним з найбільш ефективних способів забезпечення цілісності інформації. Воно забезпечує захист інформації як від випадкових загроз, так і від навмисних впливів. Ідеологія надійного і ефективного зберігання інформації на жорстких дисках знайшла своє відображення у так званій технології RAID (Redundant Array of Independent Disks). Ця технологія реалізує концепцію створення блокового пристрою зберігання даних з можливостями паралельного виконання запитів і відновлення інформації при відмовах окремих блоків накопичувачів на жорстких магнітних дисках. Пристрої, що реалізують цю технологію, називають підсистемами RAID або дисковими масивами RAID.

Враховуючи вищенаведене, для даного об'єкта пропонується використовувати однорівневе зосереджене - дублювання з використанням додаткового зовнішнього запам'ятовуючого пристрою методом дзеркального копіювання (оскільки за завданням відновлення даних має бути оперативним для високої продуктивності КС) за допомогою технології RAID.

Для цього можна використовувати сервер Adaptec Serial Attached SCSI RAID 4805SAS з технологією RAID, який забезпечує безперебійне функціонування корпоративних серверів довічно, що важливо для будь-якого підприємства і організації. Acronis True Image 9.1 Enterprise Server дає можливість в лічені хвилини відновити роботу сервера і відновити втрачені або пошкоджені дані.

2.3.7 Розробка рекомендацій, що регламентують взаємодію працівників відділення банку, які обробляють персональні дані

Мета розробки рекомендацій – зменшити ризик помилок працівників відділення, крадіжок, шахрайства або незаконного використання ресурсів.

Аспекти, пов'язані з безпекою, слід враховувати ще на стадії набору персоналу, включати їх у посадові інструкції та договори, а також контролювати протягом усього часу роботи даного співробітника.

Начальник відділення банку повинен переконатися в тому, що в посадових інструкціях відображена вся відповідна даній посаді відповідальність за безпеку збереження персональних даних клієнтів банку. Слід належним чином перевірити прийнятих на роботу осіб, особливо якщо вони будуть працювати з конфіденційною інформацією. Весь персонал відділення банку, який буде допущено до конфіденційної інформації повинні підписати зобов'язання про конфіденційність (нерозголошення).

2.3.8 Реалізація пунктів безпеки в посадових інструкціях

Обов'язки та відповідальність за безпеку, встановлені прийнятої в організації політикою інформаційної безпеки, слід включати до посадових інструкцій, де це необхідно. В інструкціях необхідно відобразити як спільну відповідальність за проведення в життя або підтримку політики безпеки, так і конкретні обов'язки щодо захисту певних ресурсів або відповідальність за виконання певних процедур або дій щодо захисту.

2.3.9 Угода про конфіденційність (нерозголошення)

Працівники які здійснюють роботу в автоматизованій системі обробки персональних даних клієнтів банку повинні підписати відповідне зобов'язання про конфіденційність (нерозголошення). Зазвичай працівники організації підписують таке зобов'язання при прийомі на роботу.

Третім особам (наприклад, організаціям-партнерам банку) яким потрібен доступ до баз персональних даних, яким володільцем чи

розпорядником бази персональних даних здійснюється передача персональних даних відповідно до закону, повинні підписати зобов'язання про нерозголошення, перш ніж їм буде надано доступ до інформаційних ресурсів організації.

Зобов'язання про нерозголошення необхідно переглядати, коли змінюються умови найму або договір, особливо якщо працівники повинні звільнитися з організації або якщо закінчуються терміни дії договору.

2.4 Вибір профілю захищеності для автоматизованої системи обробки персональних даних об'єкта інформаційної діяльності

Згідно з НД ТЗІ 2.5-005-99 дана автоматизована система відноситься до класу «3» тому що це розподілений багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності. Для даної автоматизованої системи був вибраний стандартний функціональний профіль захищеності, з підвищеними вимоги до забезпечення цілісності, доступності та конфіденційності оброблюваної інформації.

3.КЦД.3 = {КД-2, КА-2, КО-1, КК-1, КВ-3,
ЦД-1, ЦА-3, ДР-2, ДС-1, ДЗ-1,
ДВ-2, НР-3, НИ-2, НК-1, НТ-2,
НВ-2}

КД-2 – довірча конфіденційність;

КА-2 – адміністративна конфіденційність;

КО-1 – повторне використання об'єктів;

КК-1 – аналіз прихованих каналів;

КВ-3 – конфіденційність при обміні;

ЦД-1 – довірча цілісність;

ЦА-3 – адміністративна цілісність;

ЦВ-2 – цілісність при обміні;

ДР-2 – використання ресурсів;

ДС-1– стійкість до відмов;

ДЗ-1 – гаряча зміна;

ДВ-2 – відновлення після збоїв;

НР-3 – реєстрація;

НИ-2 – ідентифікація и автентифікація;

НК-1 – достовірний канал;

НО-2 – розподіл обов'язків адміністраторів;

НЦ-3 – цілісність КЗЗ;

НТ-2 – самотестування;

НВ-2– автентифікація при обміні.

2.5 Вибір типової політики безпеки в автоматизованих системах обробки персональних даних банку

В розділі 4. Терміни та визначення потрібно додати такі пункти.

Інформація про особу (персональні дані) може бути представлена в різних формах. Інформація може бути збережена на персональних комп'ютерах або серверах, передана по мережі, роздрукована або переписана на папір, і зберігатися в архівах підприємства.

Автоматизована система обробки персональних даних - це система, що здійснює автоматизовану обробку даних і до складу якої входять технічні засоби, а також їх обробка (засоби обчислювальної техніки і зв'язку), а також методи та процедури, програмне забезпечення.

База персональних даних - іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних;

Власник бази персональних даних - фізична або юридична особа, якій законом або за згодою суб'єкта персональних даних надано право на обробку цих даних, яка затверджує мету обробки персональних даних у цій базі даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом;

В розділі 6. Логічний доступ до інформаційних ресурсів додати такі пункти

6.20 Всі файли, що містять персональні дані клієнтів банку, користувач зобов'язаний створювати, обробляти і зберігати в директорії підрозділу на файловому сервері або в папках системи корпоративної електронної пошти. Забороняється для зберігання конфіденційної інформації

використовувати диск ПК або загальнодоступні мережеві диски.

6.21 Забороняється несанкціоноване копіювання, зміна, знищення персональних даних, що зберігаються в Системі підприємства.

6.22 Жоден співробітник підприємства не має права з усією повнотою повноважень для безконтрольного створення, авторизації, знищення та зміни платіжної інформації, інформації про клієнтів банку, їх персональних даних а також проведення інформацій щодо зміни стану систем.

Додати до даної політики розділ 13 Загальні вимоги до обробки персональних даних з такими пунктами.

13.1 Спираючись на Закон України «Про захист персональних даних» мета обробки персональних даних має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця бази персональних даних, та відповідати законодавству про захист персональних даних.

13.2 Персональні дані в системі мають бути точними, достовірними, у разі необхідності - оновлюватися.

13.3 Склад та зміст персональних даних мають бути відповідними та не надмірними стосовно визначеної мети їх обробки.

13.4 Обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством.

13.5 Типовий порядок обробки персональних даних у базах персональних даних затверджується уповноваженим державним органом з

питань захисту персональних даних. Указом Президента від 09.12.2010 р. № 1085/2010 «Про оптимізацію системи центральних органів виконавчої влади» передбачено створення Державної служби України з питань захисту персональних даних, якій надається статус центрального органу виконавчої влади. Він і буде уповноваженим державним органом з питань захисту персональних даних.

13.6 Персональні дані обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, у строк, не більший ніж це необхідно відповідно до їх законного призначення.

13.7 Порядок обробки персональних даних, які належать до банківської таємниці, затверджується Національним банком України.

13.8 Обсяг персональних даних, які можуть бути включені до бази персональних даних, визначається умовами згоди суб'єкта персональних даних або відповідно до закону.

13.9 Первинними джерелами відомостей про фізичну особу є: видані на її ім'я документи; підписані нею документи; відомості, які особа надає про себе.

Внести до політики розділ 14. Архівування персональних даних з такими пунктами.

14.1 Архівування баз персональних даних має забезпечувати збереження юридично значимої інформації, що представляє цінність для банку, можливість вирішення спірних ситуацій та проведення розслідувань у випадках порушення інформаційної безпеки.

14.2 Архівуванню підлягає:

- Електронні документи з персональними даними;
- Електронні зразки паперових документів з персональними даними;
- Електронні протоколи роботи Систем;
- Відкриті ключі електронного цифрового підпису;
- Будь-яка інша інформація в електронному вигляді, для якої визначено необхідність архівування.

14.3 Для кожного архіву повинен бути розроблений порядок його ведення, в якому встановлюються технологія, періодичність оновлення та термін зберігання інформації.

14.4 Електронні архіви повинні відповідати таким вимогам:

- Архів не доступний для запису або видалення інформації будь-якою особою, крім відповідального за ведення архіву;
- Документи в архіві зберігаються з усіма можливими підтвердженнями їх справжності, зокрема, з електронним цифровим підписом;
- Архів надійно захищений від втрати і знищення (дублювання, зберігання в сейфі, сейф, вибір носіїв відповідної надійності).

14.5 Для забезпечення доступності до автоматизованих систем обробки персональних даних повинна проводитися постійна робота за такими напрямами:

- Супровід роботи апаратного і програмного забезпечення;
- Резервне копіювання;
- Регламентні (профілактичні) роботи.

Внести до політики розділ 15. Знищення персональних даних в базах персональних даних з такими пунктами.

15.1 Персональні дані в базах персональних даних знищуються в порядку, встановленому відповідно до вимог закону.

15.2 Персональні дані в базах персональних даних підлягають знищенню у разі:

15.2.1 Закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом;

15.2.2 Припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником бази, якщо інше не передбачено законом;

15.2.3 Набрання законної сили рішенням суду щодо вилучення даних про фізичну особу з бази персональних даних.

15.3 Персональні дані, зібрані з порушенням вимог цього Закону, підлягають знищенню в базах персональних даних у встановленому законодавством порядку.

Внести до політики розділ 16. Захист персональних даних з такими пунктами.

16.1 Держава гарантує захист персональних даних.

16.2 Суб'єкти відносин, пов'язаних із персональними даними, зобов'язані забезпечити захист цих даних від незаконної обробки, а також від незаконного доступу до них.

16.3 Забезпечення захисту персональних даних у базі персональних даних покладається на володільця цієї бази.

16.4 Володілець бази персональних даних в електронній формі забезпечує її захист відповідно до закону.

16.5 В організації визначається структурний підрозділ або відповідальна особа, яка організовує роботу, пов'язану із захистом персональних даних при їх обробці, відповідно до закону.

Повна політика безпеки для автоматизованої системи обробки персональних даних об’єкта інформаційної діяльності наведено у додатку А.

2.6 Реалізація пунктів безпеки при обробці ПД в посадових інструкціях

Обов’язки та відповідальність за безпеку при обробці персональних даних, встановлені прийнятою в організації політикою інформаційної безпеки, слід також включити до посадових інструкцій, де це необхідно. В інструкціях необхідно відобразити відповідальність за нерозголошення персональних даних, так і конкретні обов’язки кожного працівника щодо

захисту певних ресурсів, які містять персональні дані фізичних та юридичних осіб та відповідальність за виконання певних процедур або дій щодо їх захисту.

2.6.1 Рекомендації щодо розробки посадової інструкції начальника відділу банку

До пункту 2. Загальні положення внести такий пункт:

4.14. Забезпечує збереження персональних даних клієнтів банку.

До пункту 6. Відповідальність внести такі пункти:

6.4 За використання персональних даних фізичних або юридичних осіб, а також надання третім особам часткового або повного права обробки баз персональних даних цих осіб іншим суб'єктам відносин, без надання згоди суб'єкта персональних даних.

Повна посадова інструкція начальника відділу банку приведена в додатку.

2.6.2 Рекомендації щодо розробки посадової інструкції головного бухгалтера банку

До пункту 2. Посадові обов'язки вести такі пункти

2.15. Забезпечує збереження бухгалтерських документів, що містять персональні дані фізичних та юридичних осі, оформлення і здачу їх в установленому порядку в архів.

2.21. Забезпечує збереження комерційної таємниці про діяльність банку, його клієнтів та їх персональних даних.

2.22. Зобов'язаний не допускати розголошення у будь-який спосіб персональних даних, які було довірено банку фізичною або юридичною особою, які стали відомі у зв'язку з виконанням професійних обов'язків. Таке зобов'язання чинне після припинення ним діяльності, пов'язаної з персональними даними, крім випадків, установлених Законом України «Про

захист персональних даних».

До пункту 4.Відповідальність внести такі пункти

4.4. За навмисне оголошення персональних даних клієнтів банку третім особам у власних корисливих цілях.

Повна посадова інструкція головного бухгалтера банку приведена в додатку.

2.6.3 Рекомендації щодо розробки посадової інструкції бухгалтера банку

До пункту 2. Функціональні обов'язки вести такі пункти

2.2.1. Виконує роботу з ведення бухгалтерського обліку по залученню внесків грошових коштів фізичних і юридичних осіб, з розміщення залучених коштів від свого імені і за свій рахунок, з відкриття і ведення банківських рахунків фізичних та юридичних осіб, по здійсненню розрахунків за дорученням фізичних і юридичних осіб, занесенням персональних даних фізичних та юридичних осіб до баз персональних даних банку.

2.2.3. Розробляє форми первинних документів, що застосовуються для оформлення господарських операцій, по яких не передбачені типові форми, а також форми документів для внутрішньої бухгалтерської звітності, бере участь у визначенні змісту основних прийомів і методів ведення обліку і технології персональних даних клієнтів.

2.2.6. Виконує роботи з формування, ведення і зберігання бази персональних даних клієнтів банку, вносить зміни до довідкової та

нормативної інформації, що використовується при обробці цих даних.

До пункту 4. Відповідальність вести такі пункти

4.1.4 Розповсюдження персональних даних клієнтів банку без згоди суб'єкта персональних даних.

4.1.5 Використання персональних даних клієнтів банку у власних цілях

4.1.6 Передачу третій особі персональних даних клієнтів банку без

згоди володільця бази персональних даних.

4.1.8 Порушення заборони розголошення відомостей стосовно суб'єктів персональних даних, доступ до персональних даних яких надається іншим суб'єктам відносин, пов'язаних з такими даними.

Повна посадова інструкція бухгалтера банку приведена в додатку.

2.6.4 Рекомендації щодо розробки посадової інструкції касира-операціоніста банку

До пункту 2. Функціональні обов’язки вести такий пункти

2.8 Вносить персональні дані клієнтів банку до баз персональних даних.

До пункту 3. Права вести такі пункти

3.2. Вносити на розгляд керівництва пропозиції щодо вдосконалення роботи, пов'язаної з обробкою персональних даних клієнтів в базах персональних даних.

До пункту 4. Відповідальність вести такі пункти

4.4. Поширення персональних даних про фізичну особу з баз персональних даних без згоди суб'єкта персональних даних (дозволяється тільки у випадках, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини).

4.5. Збирання персональних даних з порушенням вимог Закону України «Про захист персональних даних». Такі дані підлягають негайному знищенню в базах персональних даних у встановленому законодавством порядку.

2.7 Охорона праці

2.7.1 Загальні положення при роботі з ПК

При виконанні робіт на комп'ютерах необхідно дотримуватись вимог загальної та даної інструкції з охорони праці.

До самостійної роботи на комп'ютерах допускаються особи, які пройшли медичний огляд, навчання по професії, вступний інструктаж з охорони праці та первинний інструктаж з охорони праці на робочому місці. В подальшому вони проходять повторні інструктажі з охорони праці на робочому місці один раз на півріччя, періодичні медичні огляди один раз на два роки.

Під час роботи на комп'ютерах можуть діяти такі небезпечні та шкідливі фактори, як:

- фізичні;
- психофізіологічні.

Основним обладнанням робочого місця користувача комп'ютера є монітор, системний блок та клавіатура.

Робочі місця мають бути розташовані на відстані не менше 1,5 м від стіни з вікнами, від інших стін на відстані 1м, між собою на відстані не менше 1,5 м. Відносно вікон робоче місце доцільно розташовувати таким чином, щоб природне світло падало на нього збоку, переважно зліва.

Робочі місця слід розташовувати так, щоб уникнути попадання в очі прямого світла. Джерела освітлення рекомендується розташовувати з обох боків екрану паралельно напрямку погляду. Для уникнення світлових відблисків екрану, клавіатури в напрямку очей користувача, від світильників загального освітлення або сонячних променів, необхідно використовувати спеціальні фільтри для екранів, захисні козирки, на вікнах — жалюзі. Фільтри з металевої або нейлонової сітки використовувати не рекомендується, тому що сітка спотворює зображення через інтерференцію світла. Найкращу якість зображення забезпечують скляні поляризаційні фільтри. Вони усувають практично всі відблиски, роблять зображення чітким і контрастним.

При роботі з текстовою інформацією (в режимі введення даних та редагування тексту, читання з екрану) найбільш фізіологічним правильним є зображення чорних знаків на світлому фоні.

Монітор повинен бути розташований на робочому місці так, щоб поверхня екрана знаходилася в центрі поля зору на відстані 400-700 мм від очей користувача. Рекомендується розміщувати елементи робочого місця так, щоб витримувалася однакова відстань очей від екрана, клавіатури, тексту.

Зручна робоча поза при роботі з комп'ютером забезпечується регулюванням висоти робочого столу, крісла та підставки для ніг. Раціональною робочою позою може вважатися таке положення, при якому ступні працівника розташовані горизонтально на підлозі або підставці для ніг, стегна зорієнтовані у горизонтальній площині, верхні частини рук - вертикальні. Кут ліктьового суглоба коливається в межах 70-90°, зап'ястя зігнуті під кутом не більше ніж 20°, нахил голови 15-20°.

Для нейтралізації зарядів статичної електрики в приміщенні, де виконується робота на комп'ютерах, в тому числі на лазерних та світлодіодних принтерах, рекомендується збільшувати вологість повітря за допомогою кімнатних зволожувачів. Не рекомендується носити одяг з синтетичних матеріалів.

Згідно статті 18 Закону України ”Про охорону праці” працівник зобов'язаний:

а) знати і виконувати вимоги нормативних актів про охорону праці, правила поводження з устаткуванням та іншими засобами виробництва, користуватися засобами колективного та індивідуального захисту;

б) дотримуватись зобов'язань щодо охорони праці, передбачених колективним договором та правилами внутрішнього трудового розпорядку підприємства;

в) співробітничати з власником у справі організації безпечних і нешкідливих умов праці, особисто вживати посильних заходів щодо усунення будь-якої виробничої ситуації, яка створює загрозу його життю чи здоров'ю, або людей, які його оточують, повідомляти про небезпеку свого безпосереднього керівника або іншу посадову особу.

Вимоги безпеки перед початком роботи:

- увімкнути систему кондиціювання в приміщенні;
- перевірити надійність встановлення апаратури на робочому столі. Повернути монітор так, щоб було зручно дивитися на екран - під прямим кутом (а не збоку) і трохи зверху вниз, при цьому екран має бути трохи нахиленим, нижній його край ближче до оператора;
- перевірити загальний стан апаратури, перевірити справність електропроводки, з'єднувальних шнурів, штепсельних вилок, розеток, заземлення захисного екрана;
- відрегулювати освітленість робочого місця;
- відрегулювати та зафіксувати висоту крісла, зручний для користувача нахил його спинки;

- приєднати до системного блоку необхідну апаратуру. Усі кабелі, що з'єднують системний блок з іншими пристроями, слід вставляти та виймати при вимкненому комп'ютері;
- ввімкнути апаратуру комп'ютера вимикачами на корпусах в послідовності: монітор, системний блок, принтер (якщо передбачається друкування);
- відрегулювати яскравість свічення монітора, мінімальний розмір світної точки, фокусування, контрастність. Не слід робити зображення надто яскравим, щоб не втомлювати очей.

Рекомендується:

- яскравість свічення екрана - не менше 100Kg/M2;
- відношення яскравості монітора до яскравості оточуючих його поверхонь в робочій зоні - не більше 3:1;
- мінімальний розмір точки свічення не більше 0,4 мм для монохромного монітора і не менше 0,6 мм для кольорового, контрастність зображення знаку - не менше 0,8.

При виявленні будь-яких несправностей роботу не розпочинати, повідомити про це керівника.

Вимоги безпеки під час виконання роботи:

- необхідно стійко розташовувати клавіатуру на робочому столі, не опускати її хитання. Під час роботи на клавіатурі сидіти прямо, не напружуватися;
- для забезпечення несприятливого впливу на користувача пристроїв типу "миша" належить забезпечувати вільну велику поверхню столу для переміщення "миші" і зручного упору ліктьового суглоба;
- не дозволяються сторонні розмови, подразнюючі шуми;
- періодично при вимкненому комп'ютері прибирати ледь змоченою мильним розчином бавовняною ганчіркою порох з поверхонь апаратури. Екран ВДТ та захисний екран протирають ганчіркою, змоченою у спирті. Не дозволяється використовувати рідинні або аерозольні засоби

чищення поверхонь комп'ютера.

Забороняється:

- самостійно ремонтувати апаратуру. Ремонт апаратури здійснюється
- спеціалістами з технічного обслуговування комп'ютера, 1 раз на
- півроку повинні відкривати процесор і вилучати пилососом пил і бруд, що накопичилися;
- класти будь-яку предмети на апаратуру комп'ютера;
- закривати будь-чим вентиляційні отвори апаратури, що може призвести до її перегрівання і виходу з ладу.

Для зняття статичної електрики рекомендується час від часу доторкатися до металевих поверхонь.

Розташувати принтер необхідно поруч з системним блоком таким чином, щоб з'єднувальний шнур не був натягнутий. Забороняється ставити принтери на системний блок.

Для досягнення найбільш чистих, з високою роздільністю зображень і щоб не зіпсувати апарат, має використовуватися папір, вказаний в інструкції до принтера. При зминанні паперу потрібно відкрити кришку і обережно витягнути лоток з папером.

Згідно з інструкцією фірми-виробника потрібно дотримуватися правил зберігання картриджа.

Забороняється:

- зберігати картриджі без упаковки;
- ставити картриджі вертикально;
- перевертати картридж етикеткою донизу;
- відкривати кришку валика і доторкатися до нього;
- самому заповнювати використаний картридж.

Вимоги безпеки після закінчення роботи:

- закінчити та записати у пам'ять комп'ютера файл, що знаходиться в роботі;
- вимкнути принтер та інші периферійні пристрої. Штепсельні вилки

витягнути з розеток. Накрити клавіатуру кришкою запобігання попаданню в неї пилу;

- прибрати робоче місце;
- ретельно вимити руки теплою водою з милом;
- вимкнути кондиціонер, освітлення і загальне електроживлення;
- пройти в спеціально обладнаному приміщенні сеанс психофізіологічного розвантаження і зняття втоми з виконанням спеціальних вправ аутогенного тренування.

2.7.2 Інженерно-технічні заходи. Розрахунок штучного освітлення.

Штучне освітлення поділяється в залежності від призначення на робоче, аварійне, евакуаційне та охоронне. Розрізняють такі системи штучного освітлення: загальне, місцеве та комбіноване.

Система загального освітлення призначена для освітлення всього приміщення, вона може бути рівномірною та локалізованою.

Загальне рівномірне освітлення встановлюють у цехах, де виконуються однотипні роботи невисокої точності по усій площі приміщення при великій щільності робочих місць. Загальне локалізоване освітлення встановлюють на поточних лініях, при виконанні робіт, різноманітних за характером, на певних робочих місцях, при наявності стаціонарного затемнюючого обладнання, та якщо треба створити спрямованість світлового потоку.

Місцеве освітлення призначається для освітлення тільки робочих поверхонь, воно може бути стаціонарним (наприклад, для контролю за якістю продукції на поточних лініях) та переносним (для тимчасового збільшення освітленості окремих місць або зміни напрямку світлового потоку при огляді, контролі параметрів, ремонті).

Світильники місцевого освітлення повинні бути зручними у користуванні, а, головне, безпечними при експлуатації.

Категорично забороняється застосовувати лише місцеве освітлення, оскільки воно створює значну нерівномірність освітленості, яка підвищує

втомленість зору та призводить до розладу нервової системи. Таке освітлення на виробництві є допоміжним до загального. Комбіноване освітлення складається з загального та місцевого. Його передбачають для робіт I—VIII розрядів точності за зоровими параметрами, та коли необхідно створити концентроване освітлення без утворення різких тіней. Необхідно розрахувати потужність освітлювальної установки і визначити схему розташування світильників для штучного освітлення в приміщенні.

Обчислення будуть вироблятися по методу коефіцієнта використання світлового потоку, призначеного для розрахунку освітленості загального рівномірного освітлення горизонтальних поверхонь. Для освітлення приміщення проектом передбачено використання люмінесцентних ламп, у яких висока світловіддача, тривалий термін праці, мала яскравість світної поверхні, близький до природного світла спектральний склад випромінювання. Для виключення появи зон затемнення в середині приміщення, а також для більш рівномірної освітленості робочих місць світильники розташовуємо перпендикулярно лінії зору оператора ЕОМ.

Відповідно до галузевих норм освітленості рівень робочої поверхні над підлогою (hрп) для приміщень складає 0,8 м, а норма освітленості Е=400 $Л_к$.

Розрахункова висота (h) підвісу світильників над робочою поверхнею:

$h = H - h_{св} - h_{рп} = 3,5 - 0,5 - 0,8 = 2,2$ (м), де (4.1)

H - висота приміщення,

$h_{св}$ - висота звису світильників від перекриття.

Відстань між рядами світильників:

$L = \lambda \cdot h = 0,9 \cdot 2,2 = 1,98$ (м). (4.2)

Розрахунок необхідного числа світильників у приміщенні зробимо по формулі:

$N = S / L^2 = 24 / 3,92 \approx 6$ шт., де (4.3)

$S = 6 \cdot 4 = 24$ м^2- площа приміщення.

Для визначення коефіцієнта використання світлового потоку знайдемо індекс приміщення:

$i = A \cdot B / h \cdot (A+B) = 6 \cdot 4 / 2{,}2 \cdot (6+4) = 1{,}09.$ (4.4)

Розрахуємо світловий потік ламп у світильнику:

$\Phi = (E \cdot k \cdot S \cdot z) / (N \cdot \eta)$, де (4.5)

Е=400 лк – нормована мінімальна освітленість приміщення;

k=1,4 – коефіцієнт запасу, що враховує запилення світильників і знос джерел світла в процесі експлуатації;

$S = 6 \cdot 4 = 24$ м2 - площа приміщення;

z = 1,1 – коефіцієнт нерівномірності висвітлення;

$N = 6$ – число світильників;

$\eta = 0{,}52$ – коефіцієнт використання світлового потоку.

Світловий потік $\Phi = (400 \cdot 1{,}4 \cdot 24 \cdot 1{,}1) / (6 \cdot 0{,}52) = 4738{,}46$ лм

Щоб забезпечити світловий потік Φ = 4738,46 лм, необхідна люмінесцентна лампа ЛБ80-4, що має наступні технічні дані:

потужність лампи дорівнює 80 Вт;

світловий потік після 100 годин горіння - 4960 лм.

Загальна потужність, споживана світильниками, складе

$P = 80 \cdot 6 = 480$ Вт.

Відхилення фактичної освітленості від заданої дорівнює:

$\Delta = (4738{,}46 - 4960) \cdot 100\% / 4738{,}46 = -4{,}67\%$

При розрахунку освітленості припустима величина відхилень від нормованої складає -10%…+20%.

2.8 Висновок

В спеціальній частині кваліфікаційної роботи в кінцевому результаті були розроблені рекомендації щодо захисту інформації, яка обробляється в інформаційній комп'ютерній системі. На основі Закону України «Про захист персональних даних», були розглянуті питання підвищення обізнаності працівників Кам'янського відділення ПАТ КБ «Правекс-банк» в області захисту персональних даних, було розроблено та реалізовано пункти безпеки

при обробці персональних даних до посадових інструкцій працівників відділення. В пункті «Охорона праці» було проаналізовано шкідливі фактори які впливають на користувачів під час роботи за персональним комп'ютером. Також, було розраховано штучне освітлення для приміщення, де знаходяться користувачі ПК.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Необхідність обґрунтування витрат на реалізацію політики безпеки

Метою виконання економічного розділу кваліфікаційної роботи є економічне обґрунтування доцільності впровадження політики безпеки відділенням комерційного банку.

Для цього визначено економічну ефективність використання основних результатів, що отримані в результаті виконання роботи.

Економічна доцільність визначається розрахунками:

- капітальних витрат, що потребує розроблена політика безпеки;
- експлуатаційних витрат;
- річного економічного ефекту від впровадження інформаційної політики безпеки.

Запропонована політика інформаційної безпеки передбачає необхідність витрат на її реалізацію. Заходами, що потребують витрат, є:

- оновлення ліцензій програмного забезпечення;
- навчання персоналу в питаннях інформаційної безпеки;

3.2 Визначення трудомісткості розробки політики безпеки інформації

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}, \text{ год.} \quad (3.2)$$

Де $t_{тз}$ = 6 год. - тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_{в}$ = 5 год. - тривалість розробки концепції безпеки інформації у організації;

$t_{а}$ = 4 год. – тривалість процесу аналізу ризиків;

$t_{вз}$ = 4 год. – тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{озб}$ = 4 год. – тривалість вибору основних рішень з забезпечення безпеки інформації;

tовр = 2 год. – тривалість організації виконання відновлювальних робіт забезпечення неперервного функціонування організації;

tд = 4 год.– тривалість документального оформлення політики безпеки.

t = 6 год. + 5 год. + 4 год. + 4 год. + 4 год. + 2 год. + 4 год. = 29 год.

3.3 Розрахунок витрат на створення політики безпеки

$$Крп = Ззп + Змч, \quad (3.3)$$

де Крп – витрати на створення політики безпеки;

Ззп – заробітна плата спеціаліста з інформаційної безпеки;

Змч – вартість витрат машинного часу, що необхідні для створення політики безпеки.

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$Ззп = t * Зіб = 29 * 200 = 5800 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, год;

Зіб – средньогодинна заробітна плата спеціаліста з інформаційної безпеки становить 200 грн/год.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$Змч = t * Смч, \text{грн.}$$

де t – трудомісткість розробки політики безпеки інформації на ПК, год;

Смч – вартість 1 години машинного часу ПК, грн/год.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = Р * tнал * Се + \frac{Фзал * На}{Fp} + \frac{Клпз * Напз}{Fp} =$$

$$= 0{,}2 * 2 * 1{,}68 + \frac{(12000 * 0{,}2)}{1920} + \frac{15000 * 0{,}2}{1920} =$$

$$= 0{,}67 + 1{,}25 + 1{,}56 = 3{,}48 \text{ грн/год,}$$

Де Р- встановлена потужність апаратури інформаційної безпеки, 0.3 кВт - середня потужність одного комп'ютера;

tнал – кількість машин на яких розроблюється політика безпеки;

Се – тариф на електричну енергію, 1,68 грн/кВт·год;

Фзал – залишкова вартість ПК на поточний рік, 12000 грн.;

На – річна норма амортизації на ПК, 0.2 частки одиниці;

Напз – річна норма амортизації на ліцензійне програмне забезпечення, 0,2 частки одиниці;

Клпз – вартість ліцензійного програмного забезпечення, 15000 грн.;

Fp – річний фонд робочого часу (за 40-годинного робочого тижня Fp = 1920 год.)

$$Змч = t * Смч = 29 * 3{,}48 = 100{,}92 \text{ грн.}$$

$$Крп = Ззп + Змч = 5800 + 100{,}92 = 5900{,}92 \text{ грн.}$$

3.4 Розрахунок (фіксованих) капітальних витрат:

Оновлення ліцензії системного, прикладного і спеціалізованого ПЗ: Avast Antivirus Pro Plus - 525 грн. (вартість ліцензії для одного ПК на рік), Windows 11 Pro — 1150 грн. на рік, MS Office 2019 – 2210 грн. на рік, Онлайн-бухгалтерія Dilovod – 510 грн. на рік. Необхідно оновлення ПЗ для 15 комп'ютерів.

Загальна вартість закупівель ліцензійного ПЗ:

$$Кзпз = 15 * 4395 \text{ грн} = 65925 \text{ грн.} \qquad (3.4)$$

Таким чином, капітальні (фіксовані) витрати на впровадження системи інформаційної безпеки складають:

$$К = Кпр + Кзпз + Крп + Каз + Кнавч + Кн,$$

де Кпр – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, 15000 тис. грн;

Кзпз – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), 65925 тис. грн;

Каз – вартість закупівель апаратного забезпечення та допоміжних матеріалів відсутня, оскільки за розробленими політики безпеки закупівля апаратного забезпечення не є необхідною.

Кнавч - витрати на навчання адміністратора безпеки, становлять 5000 грн.

Крп – вартість розробки політики безпеки інформації, 5900,92 тис. грн;

Кн – витрати на встановлення обладнання та налагодження системи інформаційної безпеки відсутні, оскільки не закуповується апаратне забезпечення.

$$К = Кпр + Кзпз + Крп + Каз + Кнавч + Кн =$$
$$= 15000 + 65925 + 5000 + 5900,92 = 91825,92 \text{ грн.}$$

3.5 Розрахунок поточних (експлуатаційних) витрат:

- навчання персоналу в питаннях інформаційної безпеки;
- витрати на керування системою інформаційної безпеки.

1. Витрати на навчання персоналу в питаннях інформаційної безпеки включають в себе послуги сторонніх організацій, що створюють політику безпеки інформації та відповідно до неї розробляють інструкції для персоналу,

що є користувачами системи. Вартість навчання адміністративного персоналу й кінцевих користувачів розглянутої системи:

Со = 15000 грн. – витрати на навчання персоналу.

2. Обов'язки з керування системою інформаційної безпеки виконує керівник та адміністратор безпеки (за відсутності керівника), тому річний фонд заробітної плати складає додаткову заробітну плату директора та системного адміністратора за рік:

$$Сз = Зк + Заб = 1500 + 1000 = 2500 \text{ грн. (за 1 місяць)} \qquad (3.5)$$

$$Сз = 2500 * 12 = 30000 \text{ грн. (за 1 рік)}$$

де Зк – додаткова заробітна плата керівника, 18000 грн. на рік.

Заб – додаткова заробітна плата адміністратора безпеки, 12000 грн. на рік.

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року (Се), визначається за формулою:

$$Се = Р * Fp * Це$$

де Р – встановлена потужність апаратури інформаційної безпеки (0,3 кВт*15 комп'ютерів = 4,5 кВт)

Fр = 12 міс * 20 робочих діб/міс * 8 робочих годин * 15 комп'ютерів = 28800 год – річний фонд робочого часу системи інформаційної безпеки;

Це = 1,68 грн за 1 кВт/год. – тариф на електроенергію на 01.01.2023 року.

$$Се = 4{,}5 * 28800 * 1{,}68 = 217728 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки (Стос) визначаються у відсотках від вартості капітальних витрат (2%).

$$\text{Стос} = \text{К} * 0{,}02 = 91825{,}92 * 0{,}02 = 1836{,}52 \text{ грн.}$$

Отже, річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$\text{С} = \text{Со} + \text{Сз} + \text{Се} + \text{Стос} =$$
$$= 15000 + 30000 + 217728 + 1836{,}52 = 264564{,}52$$

Розрахунок оцінки величини збитку:

Втрати від зниження продуктивності співробітників атакованої системи мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки (Пп).

Таблиця 3.1 Заробітні плати працівників за місяць

Посада	**Розмір зар. плати**	**Кількість співробітників**	**Витрати на зар. плату на міс., грн**
Керівник відділенням	27000	1	27000
Заступник керівника відділенням	21000	1	21000
Адміністратор безпеки	20000	1	20000
Системний адміністратор	15000	1	15000
Головний бухгалтер	16000	1	16000
Бухгалтер	13000	1	13000
Головний економіст	16000	1	16000

Продовження таблиці 3.1

Посада	**Розмір зар. плати**	**Кількість співробітників**	**Витрати на зар. плату на міс., грн.**
Економіст	13000	1	13000
Юрисконсульт	15000	1	14000
Операціоніст	13000	4	52000
Менеджер по роботі з клієнтами	13000	4	52000
		Сума	1546000

Місячний фонд робочого часу складає 160 годин. Річний – 1920 годин. Час простою внаслідок атаки tп = 4 год.

$$Пп = \left(\frac{Зс}{Fр}\right) * tв = \left(\frac{1546000}{160}\right) * 4 = 38650 \text{ грн.}$$

Витрати на відновлення працездатності системи включають кілька складових:

Пви – витрати на повторне введення інформації, грн.;

Ппв – витрати на відновлення системи, грн.;

Пзч – вартість заміни частин системи, грн.

Витрати на повторне введення інформації розраховуються виходячи з розміру заробітної плати співробітників системи Зс, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу tви = 8 год.:

$$Пви = (1546000/160) * 8 = 77300 \text{ грн.}$$

Витрати на відновлення системи визначаються часом відновлення після атаки tв = 4 год. і розміром середньогодинної заробітної плати адміністратора безпеки:

$$Ппв = (20000/200) * 4 = 400$$

Витрати на відновлення працездатності системи:

$$Пв = Пви + Ппв + Пзч = 77300 + 400 + 5500 = 83200 \text{ грн.}$$

Пзч = 5500 грн - вартість для витрат на заміну частин;

О = 9000000 грн - обсяг чистого прибутку за рік.

Втрати від зниження працездатності атакованої системи:

$$V = \frac{О}{Fр} * (tп + tв + tви) = \frac{9000000}{1920} * (3 + 4 + 8) = 70312{,}5 \text{ грн.}$$

Fr – це річний фонд часу роботи відділення, 1920 годин;

tп – 4 годин простою після атаки;

tв – 4 годин відновлення після атаки;

tви – 8 годин повторного введення загубленої інформації під час атаки;

Таким чином, загальний збиток від атаки на ІТС відділення при реалізації загрози складе:

$$U = Пп + Пв + V = 38650 + 83200 + 70312{,}15 = 192162{,}5 \text{ грн.}$$

Таким чином, загальний збиток від атак на вузол або сегмент корпоративної мережі організації складе:

$$B = \sum_i \sum_n * U = 3 * 4 * 192162{,}5 = 2305950 \text{ грн.}$$

де: і- число атакованих вузлів, 3 комп'ютери;

n – середнє число атак на рік, 4 рази.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням В – загального збитку від атаки; R – очікуваної ймовірності атаки на систему; С – щорічних витрат на експлуатацію системи інформаційної безпеки.

Ймовірність R (0…1). Якщо реалізація загроз найймовірніша 1 раз на 3 місяці, тобто 4 рази на рік, то R=0,25.

Загальний ефект від впровадження політики безпеки:

$$E = B * R - C = 2305950 * 0{,}25 - 264564{,}52 = 311922{,}98 \text{ грн.}$$

Визначення та аналіз показників економічної ефективності системи інформаційної безпеки:

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині дипломного проекту, здійснюється на основі визначення та аналізу наступних показників:

- коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);
- термін окупності капітальних інвестицій То.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі.

Коефіцієнт ROSI розраховують за допомогою показників:

Е – загальний ефект від впровадження системи інформаційної безпеки тис. грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. грн.

$$ROSI = E/K = 311922{,}98 / 91825{,}92 = 3{,}4$$

Термін окупності капітальних інвестицій показує, за скільки років інвестиції окупляться за рахунок загального ефекту від впровадження ПБ.

$$To = K/E = 1/ROSI = 1 / 3{,}4 = 0{,}29 \text{ років} = 3{,}5 \text{ місяців.}$$

3.6 Висновки

Розробка і впровадження політики інформаційної безпеки для Кам'янського відділення ПАТ КБ «Правекс-Банк» можна назвати економічно доцільними, так як витрати на її створення значно менші за суму збитків, завдяки невеликій вартості комплектуючих, необхідних для відновлення системи та її інформаційних ресурсів у разі успішних атак порушників.

Тому в результаті:

- капітальні витрати на впровадження інформаційної політики безпеки становлять 91825,92 грн.;
- експлуатаційні витрати на впровадження інформаційної політики безпеки становлять 264564,52 грн.;
- загальний збиток від атаки на вузол складає 2305950 грн.;
- ефект від впровадження системи інформаційної безпеки становить 311922,98 грн.;
- термін окупності капітальних інвестицій складатиме 3,5 місяців.

Отже, економічна доцільність обґрунтована і впровадження інформаційної політики безпеки може бути ефективною та успішною.

ВИСНОВКИ

У кваліфікаційній роботі було проаналізовано нормативну базу України в сфері захисту персональних даних, виявлено загрози банківських установ. Розроблена типова політика безпеки для автоматизованих систем обробки персональних даних в банку. Розроблені рекомендації до посадових інструкцій працівників відділення, які мають справу з обробкою персональних даних клієнтів банку.

Щодо охорони праці було проаналізовано шкідливі фактори, які впливають на працівників відділення банку під час роботи за персональним комп'ютером. Також, було розраховано штучне освітлення для приміщення, де знаходяться користувачі ПК.

В економічному розділі було показано економічну доцільність впровадження політики безпеки в інформаційну комп’ютерну систему обробки інформації шляхом розрахунку:

- капітальних витрат;
- розрахунку витрат на розмежування доступу;
- розрахунку поточних витрат;
- розрахунку оцінки величини збитку;

В результаті виконаних розрахунків можна зробити висновок, що впровадження даної політики є економічно ефективним.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1 Міжнародний стандарт ISO/IEC 27005:2011 «Інформаційна технологія. Методи і засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки» [Електронний ресурс] - Режим доступу: www/ URL: https://exebit.files.wordpress.com/2013/11/iso-27005-2011-ru-v1.pdf.

2 Закон України «Про інформацію» [Електронний ресурс] / Київ, Верховна Рада України - Режим доступу : www/ URL: http://zakon5.rada.gov.ua/laws/show/2657-12 - 21.05.2015 г. - Загл. з екрану.

3 Загрози інформаційній безпеці у банківських установах [Електронний ресурс] - Режим доступу: www/ URL: http://essuir.sumdu.edu.ua/bitstream/123456789/34067/1/Borysova_banking%20establishment.pdf.

4 Операційний менеджмент [Електронний ресурс] - Режим доступу: www/ URL: http://library.if.ua/book/145/9626.html.

5 Загальна декларація прав людини (1948 р.)

6 Європейська конвенція про захист прав людини і основоположних свобод (1953 р.)

7 Несистематичний моніторинг законодавства України. / Спосіб доступу: URL: http://newlaw.com.ua/2011/01/zaxist-personalnix-danix/#more-1560.

8 2010 ТЗІ – Технічний захист інформації / Спосіб доступу: URL: http://search.ligazakon.ua/l_doc2.nsf/link1/TM039203.html– Загол. з екрана.

9 Закон України «Про інформацію».

10 Закон України «Про захист персональних даних» від 01.06.2010 р. № 2297-VI.

11 Домарев В.В. Організація захисту електронних документів / Спосіб доступу: URL: http://www.security.ukrnet.net/modules/sections/index.php?op=viewarticle&artid=568 – Загол. з екрана.

12 Левадний С.М., Оцінка інформаційних ризиків [Електронний ресурс] - Режим доступу: www/ URL: http://www.rusnauka.com/21_SEN_2014/Informatica/4_174674.doc.htm.

13 Методи та засоби оцінювання ризиків безпеки інформації в системах електронної комерції [Електронний ресурс] - Режим доступу: www/ URL: http://www.nbuv.gov.ua/old_jrn/natural/Vnulp/ISM/2008_610/03.pdf.

14 An introduction to Risk Management [Електронний ресурс] - Режим доступу: www/ URL: http://www.dphu.org/uploads/attachements/books/books_3632_0.pdf

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	3	
4	А4	Вступ	1	
5	А4	Розділ 1	19	
6	А4	Розділ 2	44	
7	А4	Розділ 3	11	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	2	
14	А4	Додаток Ґ	12	
15	А4	Додаток Д	5	
16	А4	Додаток Е	5	
17	А4	Додаток Є	5	
18	А4	Додаток Ж	4	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Презентація_Полєв.ppt

2 Кваліфікаційна робота_Полєв.doc

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ _____

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125м-22-2 Полєва М.Д.

на тему: «Розробка рекомендацій та політики безпеки щодо обробки персональних даних в ІКС банківської установи»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 122 сторінках.

Метою кваліфікаційної роботи є розробка рекомендацій та політики безпеки щодо обробки персональних даних в інформаційних комп'ютерних системах банківських установ з розробкою типової політики безпеки відділення банку, а також посадових інструкцій.

У ході виконання роботи були вирішені наступні завдання: проаналізовано нормативну базу; проаналізовано загрози ІКС банківських установ, розроблено рекомендації щодо захисту персональних даних в ІКС банківських установ. Щодо охорони праці було проаналізовано шкідливі фактори, які впливають на працівників відділення банку під час роботи за персональним комп'ютером, розраховано штучне освітлення для приміщення банку.

В економічному розділі розраховано економічну доцільність впровадження політики безпеки в ІКС для відділення банку.

Розроблені в роботі типова політика безпеки та посадові інструкції можуть бути впроваджені та використані на практиці у банківських установах.

До недоліків роботи слід віднести недостатню проробку окремих питань.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Полєв М.Д. заслуговує на оцінку « » та присвоєння кваліфікації «Магістр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
к.т.н., доц. **Ковальова Ю.В.**

ДОДАТОК Ґ. Політика безпеки в інформаційній комп'ютерній системі обробки персональних даних підприємства

ЗАТВЕРДЖУЮ

Директор
Кам'янського відділення
ПАТ АКБ «Правекс-Банк»
_____ А. В. Бондаренко

Політика безпеки в інформаційних комп'ютерних системах обробки персональних даних АКБ «ПРАВЕКС-БАНК» (далі - Політика) визначає загальні правила забезпечення інформаційної безпеки в інформаційних системах (далі - Системи) організації. Процедури і правила використання тих чи інших Систем можуть бути встановлені додатковими внутрішніми документами організації (порядки, політики, положення, інструкції тощо).

1. Загальні положення

Інформаційна безпека передбачає захист усіх форм і засобів обробки інформації з метою гарантованого забезпечення її цілісності, конфіденційності та доступності.

2. Мета і завдання Політики

Інформація та Системи є одним з життєво важливих ресурсів організації, що забезпечують його ефективну роботу. Несанкціонований доступ і несанкціоноване використання Систем та інформації може стати причиною матеріальних збитків для організації і його клієнтів, завдати шкоди його репутації, не дозволить гарантувати таємницю про операції клієнтів. Виходячи з цього, цілі і завдання Політики полягають у наступному:

- Забезпечити цілісність, конфіденційність і доступність інформації і Систем підприємства;

- Забезпечити безперервність бізнесу і мінімізувати збиток підприємства шляхом запобігання можливих інцидентів інформаційної безпеки;

- Забезпечити відповідність заходів, що вживаються в області захисту інформації, бізнес-цілям організації;

- Надати співробітникам підприємства рекомендації і сприяння в галузі інформації.

3. Розробка, впровадження та перегляд Політики

Відповідальним за розробку, впровадження, документування, перегляд і зміна Політики є адміністратор інформаційної безпеки організації.

Положення Політики підлягають перегляду в разі зміни організаційної або технологічної інфраструктури підприємства, серйозних інцидентів безпеки, виявлення нових загроз, вразливостей, інших значущих змін.

Власник бази персональних даних може встановлювати додаткові процедури забезпечення безпеки, що регулюють надання прав доступу до довірених їм ресурсів. Ці процедури можуть бути більш деталізовані, передбачати додаткові обмеження, але не можуть суперечити Політиці.

Політика обов'язкова до використання всіма співробітниками організації.

Контроль за дотриманням співробітниками організації вимог цієї Політики здійснюють директор, адміністратор безпеки та мережі.

4. Терміни та визначення

Конфіденційність - забезпечення доступу до інформації тільки для авторизованих користувачів.

Цілісність - забезпечення повноти і точності інформації та методів її обробки.

Доступність - забезпечення доступу до інформації та суміжних ресурсів авторизованих користувачів тоді, коли їм це необхідно.

Інформаційна система - засоби обчислювальної техніки та програмне забезпечення призначені для вирішення якої-небудь задачі.

Інформаційні ресурси - різні види підприємницької інформації а наступних фазах її життєвого циклу: генерація (створення), обробка, зберігання, передача, знищення.

Адміністратор системи - привілейований користувач, що виконує функції супроводу і адміністрування Системи.

Користувач - суб'єкт, який здійснює роботу в Системі.

5. Використання носіїв комп'ютерної інформації

5.1 При необхідності запису конфіденційної інформації на флеш-карти, дискети або інші носії співробітник повинен отримати відповідний дозвіл начальника структурного підрозділу, в якому він працює, якщо інше не визначено його службовими обов'язками.

5.2 Користувач зобов'язаний своєчасно знищувати втратили актуальність копії документів, що містять конфіденційну інформацію. Знищення інформації на магнітних носіях виконується тільки шляхом повного форматування останніх.

5.3 Використання флеш-карт або інших магнітних носіїв інформації можливе тільки після обов'язкової перевірки їх на наявність вірусів. У разі виявлення вірусів на магнітному носії або в пам'яті комп'ютера робота з цими пристроями припиняється до знищення вірусів.

6. Логічний доступ до інформаційних ресурсів

6.1 Інформаційні ресурси можуть використовуватися співробітниками організації тільки в службових цілях.

6.2 Вся інформація, що зберігається в системах, є конфіденційною, за винятком інформації, доступ до якої не обмежується.

6.3 Необхідною умовою доступу до інформаційних ресурсів підприємства є ознайомлення співробітника з цією політикою.

6.4 Співробітникам організації надаються права доступу до інформаційних ресурсів відповідно до їх службовими обов'язками та встановленим Порядком надання прав доступу до інформаційних ресурсів організації (далі - Порядок).

6.5 Кожному користувачеві Системи Адміністратор мережі і безпеки організації призначає унікальний ідентифікатор (обліковий запис).

6.6 При обробці критичної інформації повинна забезпечуватися можливість визначення авторства (протоколювання) кожної виконаної операції на основі ідентифікаторів користувачів.

6.7 Забороняється використання ресурсів, до яких у співробітника немає прав доступу. Можливість доступу користувача до ресурсів, не передбачених його службовими обов'язками, не означає право на їх використання.

6.8 Забороняється робота в Системах під іменами інших користувачів і з використанням чужих паролів доступу.

6.9 Забороняється передача прав доступу до інформаційних ресурсів.

6.10 Співробітники організації мають виконувати тільки ті операції і з тими даними, які визначаються їх службовими обов'язками. Будь-які інші операції вважаються забороненими.

6.11 Основним засобом доступу до інформаційних ресурсів організації є персональний комп'ютер. За кожним комп'ютером закріплюється відповідальний користувач, який визначається керівником структурного підрозділу при установці комп'ютера.

6.12 Відповідальний користувач не повинен допускати роботи інших користувачів на своєму ПК. Така робота можлива тільки у разі службової необхідності з дозволу керівника структурного підрозділу.

6.13 При передачі ПК іншому користувачеві локальний диск комп'ютера може бути переформатований на розсуд керівника структурного підрозділу, в якому цей комп'ютер експлуатується. Форматування диска повинно здійснюється за згодою і під контролем даного керівника структурного підрозділу.

6.14 Установка додаткового програмного забезпечення виконується в установленому порядку. Користувачам забороняється:

- Самостійно змінювати конфігурацію програмних та апаратних засобів ПК, здійснювати установку і видалення прикладних програм, зміна системних параметрів, знищувати або додавати файли в системні директорії;

- Змінювати встановлену адміністратором стан розділення дискових ресурсів комп'ютера, тобто створювати або видаляти колективні ресурси, а також змінювати права і паролі доступу до них;

- Змінювати будь-які налаштування доступу до мережі.

6.15 Відповідальний користувач відповідає за відсутність на локальному диску свого комп'ютера сторонніх програм.

6.16 Відповідальний користувач відповідає за конфіденційність інформації на екрані свого монітора. При тимчасовій відсутності на робочому місці (більше 2-х хвилин) або присутності сторонніх мають можливість бачити конфіденційну інформацію на екрані монітора, користувач повинен вимкнути екран або заблокувати його за допомогою одночасного натискання клавіш клавіша Windows + L, або використовувати заставку (screensaver), захищену паролем, для відновлення роботи слід використовувати пароль користувача екрану.

6.17 Користувач зобов'язаний своєчасно забирати з принтера, сканера або копіювального апарату, видрукувані, відскановані або ксерокопійовані документи.

6.18 Для пересилання електронних документів, що містять конфіденційну інформацію, всередині організації користувач зобов'язаний використовувати тільки систему корпоративної електронної пошти.

6.19 При віддаленому підключенні до інформаційних ресурсів організації повинна бути забезпечена достатня захист, спрямована на мінімізацію ризиків крадіжки обладнання та інформації, несанкціонованого розкриття інформації, несанкціонованого віддаленого доступу до систем організації, зловживання наданими ресурсами.

7. Паролі

7.1 У момент надання співробітнику прав у Системі, адміністратор повідомляє користувачеві тимчасовий пароль, який користувач зобов'язаний змінити при першому вході в Систему.

7.2 Користувач зобов'язаний забезпечити конфіденційність своїх особистих паролів. Забороняється розголошувати і передавати іншим співробітниками паролі, а також розміщувати пароль у електронному вигляді на магнітних носіях.

7.3 Користувач зобов'язаний регулярно (протягом 45 днів) змінювати свої паролі. Зміна пароля в обов'язковому порядку проводиться також у разі порушення його конфіденційності або за вказівкою адміністратора відповідної системи.

7.4 У якості особистого пароля користувач повинен самостійно вибирати послідовність символів довжиною не менше 7 (семи) знаків. Рекомендується використання в паролі поєднання літер верхнього та нижнього регістрів, цифр і знаків пунктуації. При виборі пароля забороняється повторне або «циклічне» використання старих паролів. Новий пароль повинен відрізнятися від попереднього не менш, ніж у чотирьох позиціях.

7.5 У якості особистого паролів співробітникові підприємства забороняється використовувати:

- Послідовності символів, що складаються з одних цифр (у тому числі дати, номери телефонів і т.д.);

- Послідовності повторюваних літер;

- Поспіль йдуть у розкладці клавіатури або в алфавіті літери;

- Імена та прізвища;

- Ім'я користувача в Системі (ідентифікатор) і загальновживані скорочення;

- Осмислені англійські й українські слова;

- Асоційовану зі співробітником інформацію, яку легко впізнати (адреса, марка автомобіля тощо).

7.6 У випадку якщо користувач забув свій пароль і не може отримати доступ до інформаційних ресурсів, він повинен звернутися до адміністратора мережі і безпеки.

7.7 Користувачу дозволяється використовувати один і той самий пароль для входу в мережу, в систему корпоративної електронної пошти.

7.8 Паролі встановлені за умовчанням в додатках і операційних системах (під час інсталяції), підлягають негайній заміні після початку використання системи (програми).

8. Забезпечення доступності інформаційних систем

8.1 Для систем, що забезпечують критичну інформацію, має забезпечуватися збереження їх працездатності при втраті, знищенні, несанкціонованої модифікації даних, програмного забезпечення, вихід з ладу устаткування і т.д.

8.2 Супровід робіт апаратного та програмного забезпечення передбачає:

• Контроль за несанкціонованої установкою апаратного та програмного забезпечення;

• Контроль за несанкціонованим зміна програм і прав доступу до них;

• Зберігання еталонних копій, вихідних текстів програмного забезпечення, у тому числі і попередніх версій, у спеціальних бібліотеках програмного забезпечення;

• Поділ технологічних процесів розробки, тестування, переносу в промислову середовище і експлуатації програмного забезпечення;

• Контроль і документування будь-яких змін апаратної і програмної частин системи, відображення змін в прикладному програмному забезпеченні в номері версії, системної документації та документації користувачів.

8.3 Резервне копіювання інформації має відповідати таким вимогам:

• Забезпечувати можливість відновлення програм і даних у разі виникнення аварійних ситуацій;

• Копії програмного забезпечення та даних повинні розташовуватися в безпечному місці, захищеному від пожеж та інших загроз;

• Періодично повинна перевірятися можливість відновлення інформації з копій.

8.4 Процедури резервного копіювання даних повинні бути суворо регламентовані. Періодичність резервного копіювання повинна дозволяти відновити роботу Систем без істотних втрат для підприємства в найкоротший час.

8.5 Мінімальний рівень копійованої інформації, разом з точними і повними переліками резервних копій і документованими процедурами відновлення повинен зберігатися віддалено і на достатній відстані з метою уникнення збитків у разі аварії на основному майданчику.

8.6 Резервування підлягає:

• Серверне та мережеве обладнання;

• Програмне забезпечення;

• Канали зв'язку;

• Інформаційні бази даних.

9. Антивірусний захист

9.1 Антивірусний захист інформаційних ресурсів організації повинна забезпечувати контроль:

• Інформації, що входить з глобальних мереж у внутрішню мережу організації;

• Інформації, що зберігається на файлових серверах організації;

• Інформації, що зберігається на персональних комп'ютерах співробітників.

9.2 Повинна проводитися перевірка на віруси всієї вхідної з глобальної мережі електронної пошти і файлів.

9.3 На всіх файлових серверах в корпоративній мережі організації повинно бути встановлене антивірусне програмне забезпечення.

9.4 Повинна проводитися щоденна перевірка на віруси всіх програм і файлів даних на файлових серверах.

9.5 Робочі станції користувачів повинні мати резидентні антивірусні програми, що забезпечують перевірку на віруси всіх файлів при їх завантаження в комп'ютер, а також антивірусні сканери для повної перевірки жорстких дисків.

9.6 Антивірусні програми і бази вірусних сигнатур повинні щодня централізовано оновлюватись.

9.7 Користувачі зобов'язані інформувати системного адміністратора про будь-якому виявленому вірус, зміну конфігурації, незвичну поведінку комп'ютера або програми.

9.8 При виявленні вірусу повинні бути вжиті наступні заходи:

• Будь-який комп'ютер, який підозрюється в зараженні вірусом, негайно відключається від мережі;

• Заражений комп'ютер не підключається до мережі до тих пір, поки адміністратор мережі і безпеки не засвідчуватися в успішному результаті лікування (видалення) вірусу;

• Якщо вірус видалити не вдається, всі програми, в комп'ютері видаляються, включаючи, при необхідності, операційну систему, жорсткий диск формується;

• Віддалені програми повторно встановлюються з надійних джерел і повторно перевіряється на наявність вірусів;

• Проводиться аналіз причин зараження вірусом, і приймаються необхідні заходи безпеки.

10. Вимоги до захисту приміщень

10.1 Приміщення організації, в яких розташовуються засоби обчислювальної техніки, повинні обладнуватися охоронно-пожежною сигналізацією, необхідними засобами інженерного захисту та контролю доступу.

10.2 Приміщення з серверним обладнанням, на якому обробляється критична інформація, повинні бути обладнані достатніми засобами кондиціонування, вимірювання та контролю температури і вологості повітря,

засобами охоронної сигналізації, системою контролю доступу та автоматизованою системою пожежогасіння, системою контролю стану електропостачання, при необхідності - засобами відео спостереження. Доступ у ці приміщення надається строго певним особам у відповідності зі службовими обов'язками, час входу і виходу з приміщення повинен фіксуватися в спеціальній базі даних.

11. Функції щодо забезпечення інформаційної безпеки

Правління

11.1 У рамках організації та здійснення загального керівництва поточною діяльністю підприємства, визначає стратегію і програму забезпечення інформаційної безпеки організації.

11.2 Стверджує політику і процедури інформаційної безпеки.

Підрозділ інформаційної безпеки організації:

11.3 Грає лідируючу роль у розробці стратегії інформаційної безпеки організації.

11.4 Готує положення щодо формування бюджету, спрямованого на забезпечення інформаційної безпеки організації.

11.5 Фахівці підрозділу в рамках своїх повноважень розробляють політики та процедури інформаційної безпеки організації.

11.6 Розробляють технічні, організаційні та адміністративні плани забезпечення реалізації політики інформаційної безпеки організації.

11.7 Забезпечують штатний функціонування комплексу засобів інформаційної безпеки організації.

11.8 Забезпечують виконання вимог інформаційної безпеки, викладених у даній політиці та інших внутрішніх документах організації.

11.9 Забезпечують моніторинг функціонування системи управління інформаційної безпеки організації.

11.10 Оцінюю ризики інформаційної безпеки.

11.11 Контролюють дії користувачів.

11.12 Забезпечують вибір засобів і механізмів контролю, управління і забезпечення інформаційної безпеки організації.

11.13 Проводять розслідування подій, пов'язаних з порушеннями інформаційної безпеки організації.

11.14 Забезпечує цілісність і доступність.

Управління внутрішнього аудиту та контролю:

11.15 Оцінює відповідність операцій, додатків і Систем прийнятим політикам безпеки.

11.16 Оцінює стратегію інформаційної безпеки організації і вносить пропозиції щодо її зміни.

11.17 Оцінює стан інформаційної безпеки організації.

11.18 Інформує керівництво підприємства про стан інформаційної безпеки.

11.19 Розробляє плани заходів щодо вдосконалення системи інформаційної безпеки за результатами аудиторських перевірок.

Управління по роботі з персоналом:

11.20 Забезпечує ознайомлення працівників організації з Політикою і правилами інформаційної безпеки організації.

11.21 Забезпечує накладення на співробітників дисциплінарних стягнень у разі порушення Політики та правил інформаційної безпеки організації.

Співробітники організації:

11.22 Виконують вимоги інформаційної безпеки, викладені в даній Політиці та інших внутрішніх документів організації.

11.23 Забезпечуються виконання вимог інформаційної безпеки, викладені в даній Політиці та інших внутрішніх документів організації, третіми особами, з якими вони контактують у рамках своїх посадових обов'язків, у тому числі шляхом наявності зазначених вимог у контрактах, угодах, договорах з третіми особами.

12. Відповідальність

12.1 Адміністратор мережі і безпеки організації несе відповідальність за стан інформаційної безпеки організації.

12.2 Співробітник організації несе відповідальність за всі дії, виконувані ним в Системах організації відповідно до внутрішніми нормативними документами організації.

Додаток Д. Посадова інструкція начальника відділу банку

ЗАТВЕРДЖУЮ

_____ _____

(назва установи, організації) (уповноважена особа)

_____

(ПІБ, підпис)

"___" _____ 20__ р.

ПОСАДОВА ІНСТРУКЦІЯ НАЧАЛЬНИКА ВІДДІЛУ БАНКУ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1 Дана посадова інструкція визначає функціональні обов'язки, права і відповідальність начальника відділу банку.

1.2 Начальник відділу банку відноситься до категорії керівників.

1.3 Начальник відділу банку призначається на посаду і звільняється з посади в установленому чинним трудовим законодавством порядку наказом директора банку.

1.4 Взаємовідносини за посадою:

1.4.1 Пряме підпорядкування Директору банку

1.4.2. Додаткове підпорядкування

1.4.3 Віддає розпорядження співробітникам відділу банку

1.4.4 Працівника заміщає Заступник начальника відділу банку

1.4.5 Працівник заміщає

2. КВАЛІФІКАЦІЙНІ ВИМОГИ ДО НАЧАЛЬНИКА ВІДДІЛУ БАНКУ:

2.1 Освіта вища професійна освіта

2.2 Досвід роботи не менше 3 років

2.3 Знання Законів, інших нормативно правових актів України, що відносяться до діяльності фінансово-банківських установ. Накази, відомчі інструкції і нормативні документи, що стосуються роботи відділу. Основи економіки. Перспективи розвитку фінансово-банківської системи і стратегічні напрямки діяльності банку. Основи наукової організації праці. Правила і норми охорони праці, техніки безпеки і протипожежного захисту.

2.4 Навички роботи за фахом

3. ДОКУМЕНТИ, ЯКІ РЕГЛАМЕНТУЮТЬ ДІЯЛЬНІСТЬ

3.1 Зовнішні документи:

Законодавчі та нормативні акти, що стосуються виконуваної роботи.

3.2 Внутрішні документи:

Статут банку, Накази і розпорядження директора банку; Положення про відділ, Посадова інструкція начальника відділу банку, Правила внутрішнього трудового розпорядку.

2. ФУНКЦІОНАЛЬНІ ОБОВ'ЯЗКИ

Начальник відділу банку:

4.1. Здійснює керівництво діяльністю відділу банку і несе персональну відповідальність за якість виконуваних відділом робіт і результати його діяльності.

4.2. Забезпечує підготовку проектів поточних і перспективних планів робіт та здійснює контроль за виконанням завдань які стоять перед відділом банку.

4.3. Організує систематичний аналіз діяльності відділу банку і на його основі готує необхідні проекти документів з питань, що входять у його компетенцію.

4.4. Готує проекти положення про відділ банку та посадових інструкцій працівників відділу.

4.5. Очолює розробку проектів нормативних, методичних та інструктивних матеріалів за напрямками діяльності відділу банку.

4.6. Вивчає ефективність діючих правил та інструкцій, що стосуються діяльності банку і одночасно стосуються роботи відділу банку. На основі аналізу специфіки ринку банківських послуг у різних регіонах вносить пропозиції щодо вдосконалення зазначених документів.

4.7. Вживає заходів до впровадження в роботу відділу банку найбільш ефективних методів і технологій банківської діяльності.

4.8. Сприяє створенню необхідних умов праці та сприятливого морально-психологічного клімату в колективі.

4.9. Забезпечує дотримання працівниками відділу банку трудової дисципліни.

4.10. Дозволяє оперативні питання, готує довідки, проекти відповідей на заяви, листи і скарги громадян, що стосуються роботи відділу банку.

4.11. Здійснює контроль, надає практичну і методичну допомогу відповідним структурним підрозділам банку, у тому числі з виїздом на місце.

4.12. Забезпечує збереження комерційної таємниці про діяльність банку і його клієнтів.

4.13. Забезпечує правильне застосування в роботі відділу банку чинного законодавства та ведення діловодства в установленому порядку.

4.14. Забезпечує збереження персональних даних клієнтів банку.

5. ПРАВА

Начальник відділу банку має право:

5.1. Знайомитися з проектами рішень Ради директорів банку (правління банку), Голови банку, що стосуються діяльності відділення банку.

5.2. Брати участь в обговоренні питань, що стосуються виконання ним посадових обов'язків.

5.3. Підписувати і візувати документи в межах своєї компетенції.

6. ВІДПОВІДАЛЬНІСТЬ

Начальник відділу банку несе відповідальність:

6.1. За неналежне виконання або невиконання своїх посадових обов'язків, передбачених цією посадовою інструкцією, - в межах, визначених чинним трудовим законодавством України.

6.2. За правопорушення, скоєні в процесі здійснення своєї діяльності - в межах, визначених чинним адміністративним, кримінальним та цивільним законодавством України.

6.3. За завдання матеріальної шкоди - в межах, визначених чинним трудовим і цивільним законодавством України.

6.4 За використання персональних даних фізичних або юридичних осіб, а також надання третім особам часткового або повного права обробки баз персональних даних цих осіб іншим суб'єктам відносин, без надання згоди суб'єкта персональних даних.

7. УМОВИ РОБОТИ

7.1. Режим роботи начальника відділу банку визначається відповідно до Правил внутрішнього трудового розпорядку, встановленими в банку.

8. УМОВИ ОПЛАТИ ПРАЦІ

Умови оплати праці начальника відділу банку визначаються відповідно до Положення про оплату праці персоналу.

9 ПРИКІНЦЕВІ ПОЛОЖЕННЯ

9.1 Дана Посадова інструкція складена в двох примірниках, один з яких зберігається у Банку, інший - у працівника.

9.2 Задачі, Обов'язки, Права і Відповідальність можуть бути уточнені відповідно до зміни Структури, Задач і Функцій структурного підрозділу і робочого місця.

9.3 Зміни та доповнення до даної Посадової інструкції вносяться наказом директора банку.

Керівник структурного підрозділу (ініціали, прізвище) _____

(Підпис)

"" _____ 20__р.

ПОГОДЖЕНО:

Начальник юридичного відділу

(Ініціали, прізвище)

_____

(Підпис)

"" _____ 20__р.

З інструкцією ознайомлений: (ініціали, прізвище) _____

(Підпис)

"" _____20__ р.

ДОДАТОК Е. Посадова інструкція головного бухгалтера банку

ЗАТВЕРДЖУЮ

_____ _____

(назва установи, організації) (уповноважена особа)

_____

(ПІБ, підпис)

"___" _____ 200_ р.

ПОСАДОВА ІНСТРУКЦІЯ ГОЛОВНОГО БУХГАЛТЕРА БАНКУ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Головний бухгалтер банку відноситься до категорії керівників.

1.2. На посаду головного бухгалтера банку призначається особа, має вищу професійну освіту за профілем, робочий стаж фінансово-банківської чи аналогічної роботи на керівних посадах не менше 5 років.

1.3. Головний бухгалтер банку призначається на посаду і звільняється від неї головою банку і підпорядковується безпосередньо:_____

1.4. Головний бухгалтер банку повинен знати:

1.4.1 Закони, інші нормативні правові акти, що відносяться до діяльності банку;

1.4.2 Бухгалтерський облік, накази, відомчі інструкції і нормативні документи, що стосуються діяльності структурних підрозділів банку, що займаються бухгалтерським обліком та звітністю;

1.4.3 Сучасні засоби обчислювальної техніки;

1.4.3 Основи економіки, цивільне право, фінансове, податкове і господарське законодавство;

1.4.4 Перспективи розвитку фінансово-банківської системи;

1.4.5 Специфіку діяльності філій банку;

1.4.6 Основи наукової організації праці;

1.4.7 Правила і норми охорони праці, техніки безпеки і протипожежного захисту;

2. ПОСАДОВІ ОБОВ'ЯЗКИ

Головний бухгалтер банку:

2.1. Здійснює організацію бухгалтерського обліку господарсько-фінансової діяльності та контролю за економічним використанням матеріальних, трудових і фінансових ресурсів, збереженням довірених банку коштів відповідно до встановленого в банку порядком ведення бухгалтерського обліку та звітності.

2.2. Забезпечує організацію обліку та звітності на основі впровадження в практичну роботу прогресивних форм і методів бухгалтерського обліку та контролю.

2.3. Керує працівниками бухгалтерії.

2.4. Готує проекти положень про відповідні структурних підрозділах банку, забезпечує виконання покладених на них завдань.

2.5. Несе відповідальність за всіма напрямками діяльності цих підрозділів.

2.6. Розглядає і затверджує посадові інструкції працівників, займаються бухгалтерським обліком та звітністю.

2.7. Організує облік грошових коштів та інших цінностей, бухгалтерський облік здійснюваних операцій, пов'язаний з їх рухом, а також виконанням кошторисів витрат фінансової діяльності банку.

2.8. Забезпечує облік фінансових, розрахункових, кредитних операцій і контроль за законним та своєчасним їх оформленням.

2.9. Організовує своєчасне проведення розрахунків по заробітній плати працівників, правильне нарахування та перерахування платежів зацікавленим органам та організаціям у рамках чинного законодавства.

2.10. Здійснює контроль за дотриманням порядку ведення бухгалтерського обліку та контролю.

2.11. Вживає заходів щодо запобігання випадків заподіяння банку збитку, порушень фінансового, податкового та господарського законодавства.

2.12. У необхідних випадках вживає заходів до погашення виникли збитків, забезпечує своєчасну передачу необхідних документів у правоохоронні органи.

2.13. Веде роботу по забезпеченню дотримання штатної, фінансової та розрахунково-касової дисципліни, кошторисів адміністративно-господарських та інших витрат.

2.14. Забезпечує законність списання з бухгалтерських балансів недостач, дебіторської заборгованості та інших втрат, безнадійних до стягненню.

2.15. Забезпечує збереження бухгалтерських документів, що містять персональні дані фізичних та юридичних осі, оформлення і здачу їх в установленому порядку в архів.

2.16. Очолює роботу з розробки нових та уніфікації чинних документів з бухгалтерського обліку, впровадження ефективних засобів механізації обліково-обчислювальних робіт.

2.17. Забезпечує своєчасне складання бухгалтерської звітності, подання її в установленому порядку до відповідних органи.

2.18. Надає методичну допомогу структурним підрозділам банку з питань бухгалтерського обліку, контролю, звітності й економічного аналізу.

2.19. Забезпечує контроль за виконанням договірних зобов'язань.

2.20. Виконує представницькі функції і забезпечує взаємодія з різними структурними підрозділами банку.

2.21. Забезпечує збереження комерційної таємниці про діяльність банку, його клієнтів та їх персональних даних.

2.22. Зобов'язаний не допускати розголошення у будь-який спосіб персональних даних, які було довірено банку фізичною або юридичною особою, які стали відомі у зв'язку з виконанням професійних обов'язків. Таке зобов'язання чинне після припинення ним діяльності, пов'язаної з персональними даними, крім випадків, установлених Законом України «Про захист персональних даних»

3. ПРАВА

Головний бухгалтер банку має право:

3.1. Діяти від імені банку.

3.2. Представляти його інтереси у взаєминах з органами державної влади, юридичними особами, громадянами.

3.3. Підписувати і візувати документи в межах своєї компетенції.

3.4. Представляти на розгляд голови банку пропозиції щодо поліпшення діяльності банку, пропозиції щодо призначення, переміщення, звільнення, заохочення та притягнення до дисциплінарної та матеріальної відповідальності працівників бухгалтерії.

3.5. Вимагати від керівництва підприємства сприяння у виконанні своїх посадових обов'язків.

4. ВІДПОВІДАЛЬНІСТЬ

Головний бухгалтер банку несе відповідальність:

4.1. За неналежне виконання або невиконання своїх посадових обов'язків, передбачених цією посадовою інструкцією, в межах, визначених чинним законодавством України.

4.2. За правопорушення, скоєні в процесі здійснення своєї діяльності - в межах, визначених чинним адміністративним, кримінальним та цивільним законодавством України.

4.3. За наслідки прийнятих рішень, збереження та ефективне використання майна підприємства, а також фінансово-господарські

результати його діяльності - відповідно до статуту підприємства і чинним законодавством України;

4.4. За навмисне оголошення персональних даних клієнтів банку третім особам у власних корисливих цілях.

Керівник структурного підрозділу (ініціали, прізвище) _____

(Підпис)

"" _____ 20__р.

ПОГОДЖЕНО:

Начальник юридичного відділу

(Ініціали, прізвище)

_____

(Підпис)

"" _____ 20__р.

З інструкцією ознайомлений: (ініціали, прізвище) _____

(Підпис)

"" _____20__ р.

ДОДАТОК Є. Посадова інструкція бухгалтера банку

ЗАТВЕРДЖУЮ

_____ _____

(назва установи, організації) (уповноважена особа)

_____

(ПІБ, підпис)

"___" _____ 20__ р.

ПОСАДОВА ІНСТРУКЦІЯ БУХГАЛТЕРА БАНКУ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Дана посадова інструкція визначає функціональні обов'язки, права і відповідальність бухгалтера щодо банківських операцій.

1.2. Бухгалтер за банківськими операціями призначається на посаду і звільняється з посади в установленому чинним трудовим законодавством порядку наказом директора.

1.3. Бухгалтер за банківськими операціями підпорядковується безпосередньо _____(П.І.Б.).

1.4. На посаду бухгалтера за банківськими операціями призначається особа, що має вищу професійну (економічну) освіту без пред'явлення вимог до стажу роботи або середня професійна (економічна) освіта і стаж роботи на посаді бухгалтера за банківськими операціями не менше 3 років.

1.5. Бухгалтер за банківськими операціями повинен знати:

- Законодавчі акти, постанови, розпорядження, накази, керівні, методичні та нормативні матеріали з організації бухгалтерського обліку за банківськими операціями та складання звітності;

- Форми і методи бухгалтерського обліку на даній ділянці;

- План та кореспонденцію рахунків;

- Організацію документообігу по обліку банківських операцій;

- Порядок документального оформлення і відображення на рахунках бухгалтерського обліку операцій, пов'язаних із залученням вкладів грошових коштів фізичних і юридичних осіб, розміщення зазначених коштів від свого імені і за свій рахунок на умовах повернення, платності, строковості; відкриттям і веденням банківських рахунків фізичних та юридичних осіб ; методи економічного аналізу господарсько-фінансової діяльності;

- Правила експлуатації обчислювальної техніки;

- Економіку, організацію праці та управління;

- Ринкові методи господарювання;

- Законодавство про працю;

- Правила і норми охорони праці.

1.6. У період тимчасової відсутності Бухгалтера за банківськими операціями його обов'язки покладаються на _____(П.І.Б.)

2. ФУНКЦІОНАЛЬНІ ОБОВ'ЯЗКИ

2.1. Функціональні обов'язки бухгалтера з обліку касових операцій визначені на основі й у обсязі кваліфікаційної характеристики з даної посади і можуть бути доповнені, уточнені при підготовці посадової інструкції, виходячи з конкретних обставин.

2.2. Бухгалтер за банківськими операціями:

2.2.1. Виконує роботу з ведення бухгалтерського обліку по залученню внесків грошових коштів фізичних і юридичних осіб, з розміщення залучених коштів від свого імені і за свій рахунок, з відкриття і ведення банківських рахунків фізичних та юридичних осіб, по здійсненню розрахунків за дорученням фізичних і юридичних осіб, занесенням персональних даних фізичних та юридичних осіб до баз персональних даних банку.

2.2.2. Забезпечує керівників, кредиторів, інвесторів, аудиторів та інших користувачів бухгалтерської звітності порівнянною і достовірною бухгалтерською інформацією по даному напрямку обліку.

2.2.3. Розробляє форми первинних документів, що застосовуються для оформлення господарських операцій, по яких не передбачені типові форми, а також форми документів для внутрішньої бухгалтерської звітності, бере участь у визначенні змісту основних прийомів і методів ведення обліку і технології персональних даних клієнтів.

2.2.4. Бере участь у проведенні економічного аналізу господарсько-фінансової діяльності філії за даними бухгалтерського обліку і звітності з метою виявлення внутрішньогосподарських резервів, здійснення режиму економії і заходів щодо вдосконалення документообігу, у розробці та впровадженні прогресивних форм і методів бухгалтерського обліку на основі застосування сучасних засобів обчислювальної техніки, в проведення інвентаризацій грошових коштів і товарно-матеріальних цінностей.

2.2.5. Готує дані по відповідних ділянках бухгалтерського обліку для складання звітності, стежить за збереженням бухгалтерських документів, оформляє їх відповідно до встановленого порядку для передачі в архів.

2.2.6. Виконує роботи з формування, ведення і зберігання бази персональних даних клієнтів банку, вносить зміни до довідкової та нормативної інформації, що використовується при обробці цих даних.

2.2.7. Бере участь у формулюванні економічної постановки завдань або окремих їх етапів, що вирішуються за допомогою обчислювальної техніки, визначає можливість використання готових проектів, алгоритмів, пакетів прикладних програм, що дозволяють створювати економічно обґрунтовані системи обробки економічної інформації.

3. ПРАВА

3.1. Бухгалтер за банківськими операціями має право:

3.1.1. Приймати участь в обговоренні питань, що входять в його функціональні обов'язки.

3.1.2. Вносити пропозиції та зауваження з питань поліпшення діяльності на дорученій ділянці роботи.

4. ВІДПОВІДАЛЬНІСТЬ

4.1. Бухгалтер несе відповідальність за:

4.1.1. Невиконання своїх функціональних обов'язків.

4.1.2. Недостовірну інформацію про стан виконання отриманих завдань і доручень, порушення термінів їх виконання.

4.1.3. Невиконання наказів, розпоряджень директора, доручень та завдань від головного бухгалтера та директора.

4.1.4 Розповсюдження персональних даних клієнтів банку без згоди суб'єкта персональних даних.

4.1.5 Використання персональних даних клієнтів банку у власних цілях

4.1.6 Передачу третій особі персональних даних клієнтів банку без згоди володільця бази персональних даних.

4.1.7. Порушення Правил внутрішнього трудового розпорядку.

4.1.8 Порушення заборони розголошення відомостей стосовно суб'єктів персональних даних, доступ до персональних даних яких надається іншим суб'єктам відносин, пов'язаних з такими даними.

5. УМОВИ РОБОТИ

5.1. Режим роботи бухгалтера за банківськими операціями визначається відповідно до Правил внутрішнього трудового розпорядку.

8. УМОВИ ОПЛАТИ ПРАЦІ

Умови оплати праці визначаються відповідно до Положення про оплату праці персоналу.

Керівник структурного підрозділу (ініціали, прізвище) _____

(Підпис)

"" _____ 20__р.

ПОГОДЖЕНО:

Начальник юридичного відділу

(Ініціали, прізвище)

_____

(Підпис)

"" _____ 20__р.

З інструкцією ознайомлений: (ініціали, прізвище) _____

(Підпис)

"" _____20__ р.

ДОДАТОК Ж. Посадова інструкція касира-операціоніста банку

ЗАТВЕРДЖУЮ

_____ _____

(назва установи, організації) (уповноважена особа)

_____

(ПІБ, підпис)

"___" _____ 20__ р.

ПОСАДОВА ІНСТРУКЦІЯ КАСИРА-ОПЕРАЦІОНІСТА БАНКУ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Касир-операціоніст банку відноситься до категорії технічних фахівців.

1.2. Призначення на посаду касира-операціоніста банку та звільнення з неї здійснюється наказом керівника банком.

1.3. Касир-операціоніст банку підпорядковується безпосередньо начальнику зміни або керівнику відділу.

1.4. На час відсутності касира-операціоніста банку його права та обов'язки переходять до іншої службової особи, яке набуває відповідних прав і несе відповідальність за належне виконання покладених на нього обов'язків.

1.5. На посаду касира-операціоніста банку призначається особа, яка має початкову професійну освіту без пред'явлення вимог до стажу роботи або середня (повна) загальна освіта та спеціальну підготовку за встановленою програмою без пред'явлення вимог до стажу роботи.

1.6. Касир-операціоніст банку повинен знати:

1.6.1 Нормативні правові акти, положення, інструкції, інші керівні матеріали і документи з ведення касових операцій;

1.6.2 Форми касових і банківських документів;

1.6.3 Правила прийому, видачі, обліку і зберігання грошових коштів і цінних паперів;

1.6.4 Порядок оформлення прибуткових і витратних документів;

1.6.5 Ліміти залишків касової готівки, встановленої для підприємства, правила забезпечення їх збереження;

1.6.6 Порядок ведення касової книги, складання касової звітності;

1.6.7 Основи організації праці;

1.6.8 Правила експлуатації обчислювальної техніки;

1.6.9 Основи законодавства про працю;

1.6.10 Правила внутрішнього трудового розпорядку;

1.6.11 Правила і норми охорони праці.

1.7. Касир-операціоніст банку керується у своїй діяльності:

1.7.1 Законодавчими актами України;

1.7.2 Статутом банку, правилами внутрішнього трудового розпорядку, іншими нормативними актами банку;

1.7.3 Наказами та розпорядженнями керівництва;

1.7.4 Цією посадовою інструкцією.

2. ФУНКЦІОНАЛЬНІ ОБОВ'ЯЗКИ

Касир-операціоніст банку виконує такі посадові обов'язки:

2.1. Здійснює операції з приймання, обліку, видачі і зберіганню грошових коштів і цінних паперів з обов'язковим дотриманням правил, що забезпечують їх збереження.

2.2. Обслуговує клієнтів по рахунках, вкладах, переказів, банківських картках.

2.3. Веде валютно-обмінні операції.

2.4. Здійснює розрахунки з клієнтами, продаж банківських продуктів.

2.5. Веде на основі прибуткових і витратних документів касову книгу, звіряє фактичну наявність грошових сум і цінних паперів з книжковим залишком.

2.6. Складає описи старих купюр, а також відповідні документи з метою заміни на нові.

2.7. Складає касову звітність.

2.8 Вносить персональні дані клієнтів банку до баз персональних даних.

3. ПРАВА

Касир-операціоніст банку має право:

3.1. Знайомитися з проектами рішень керівництва банку, що стосуються його діяльності.

3.2. Вносити на розгляд керівництва пропозиції щодо вдосконалення роботи, пов'язаної з обробкою персональних даних клієнтів в базах персональних даних.

3.3. У межах своєї компетенції повідомляти безпосередньому керівнику про всі виявлені недоліки в діяльності підприємства та вносити пропозиції щодо їх усунення.

3.4. Отримувати від структурних підрозділів та фахівців інформацію та документи, необхідні для виконання його посадових обов'язків.

3.5. Вимагати від керівництва установи сприяння у виконанні своїх посадових обов'язків і прав.

4. ВІДПОВІДАЛЬНІСТЬ

Касир-операціоніст банку несе відповідальність за:

4.1. Невиконання або неналежне виконання своїх посадових обов'язків, передбачених цією посадовою інструкцією, - в межах, визначених чинним трудовим законодавством України.

4.2. Заподіяння матеріального збитку роботодавцеві - в межах, визначених чинним трудовим і цивільним законодавством України.

4.3. Правопорушення, скоєні в процесі здійснення своєї діяльності, - в межах, визначених чинним адміністративним, кримінальним, цивільним законодавством України

4.4. Поширення персональних даних про фізичну особу з баз персональних даних без згоди суб'єкта персональних даних (дозволяється

тільки у випадках, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини).

4.5. Збирання персональних даних з порушенням вимог Закону України «Про захист персональних даних». Такі дані підлягають негайному знищенню в базах персональних даних у встановленому законодавством порядку.

5. УМОВИ РОБОТИ

5.1. Режим роботи бухгалтера за банківськими операціями визначається відповідно до Правил внутрішнього трудового розпорядку.

8. УМОВИ ОПЛАТИ ПРАЦІ

Умови оплати праці визначаються відповідно до Положення про оплату праці персоналу.

Керівник структурного підрозділу (ініціали, прізвище) _____

(Підпис)

"" _____ 20__р.

ПОГОДЖЕНО:

Начальник юридичного відділу

(Ініціали, прізвище)

_____

(Підпис)

"" _____ 20__р.

З інструкцією ознайомлений: (ініціали, прізвище) _____

(Підпис)

"" _____20__ р.