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 *Зуя Олександра Васильовича*

академічної групи *125м-22-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка алгоритму запобіганню витоку інформації на підприємстві з вини персоналу*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Мацюк С.М.			
розділів:				
спеціальний	к.т.н., доц. Мацюк С.М.			
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 *Зую Олександру Васильовичу* **академічної групи** *125м-22-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка алгоритму запобіганню витоку інформації на підприємстві з вини персоналу*

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

Розділ	Зміст	Термін виконання
Розділ 1	Стан питання. Постановка задачі	02.11.2023
Розділ 2	Спеціальний розділ	16.11.2023
Розділ 3	Економічний розділ	30.11.2023

Завдання видано _____ Мацюк С.М.
(підпис керівника) (прізвище, ініціали)

Дата видачі: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ Зуй О.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 71 с., 5 рис., 3 табл., 5 додатків, 15 джерел.

Об’єкт дослідження: алгоритм запобіганню витоку інформації.

Мета кваліфікаційної роботи: забезпечення підвищення рівня безпеки підприємства на основі впровадження розробленого алгоритму запобіганню витоку конфіденційної інформації з вини персоналу.

У спеціальній частині наведений аналіз можливих загроз витоку конфіденційної інформації з вини персоналу; розглянуті етапи розробки, підстави для розробки, призначення розробки; розроблений алгоритм основних дій при роботі з персоналом, який має доступ до конфіденційної інформації підприємства.

В економічному розділі був виконаний розрахунок витрат на розробку і впровадження алгоритму на підприємстві. А також зроблений висновок щодо економічної ефективності впровадження створеного алгоритму.

Практичне значення полягає у підвищенні рівня безпеки розглянутого підприємства за рахунок зменшення ризику витоку конфіденційної інформації з вини персоналу підприємства.

Наукова новизна полягає в удосконаленні процесу роботи з персоналом з метою забезпечення інформаційної безпеки на підприємстві.

КОНФІДЕНЦІЙНА ІНФОРМАЦІЯ, ВИТІК ІНФОРМАЦІЇ, ЛЮДСЬКИЙ ФАКТОР, МОТИВАЦІЯ, АЛГОРИТМ, ПСИХОЛОГІЧНИЙ КЛІМАТ

THE ABSTRACT

Explanatory note: 71 p., 5 fig., 3 tab., 5 appendices, 15 sources.

The object of research: algorithm to prevent information leakage.

Purpose of qualification work: providing the increase of security level at enterprise by developing the algorithm to prevent leakage of the confidential information due to personnel fault.

The special part includes analysis of possible threats of confidential information leakage, the stages of development, the basis for development, assignment design. The algorithm of key actions for dealing with staff, who have access to confidential information at an enterprise, was developed.

The economic section includes calculation of costs for algorithm development and implementation at an enterprise. The conclusion as to the cost-effectiveness of the created algorithm implementation was made.

The practical significance of the qualification work consists in improving the security of an enterprise by reducing the risks of leakage of confidential information due to personnel fault at the enterprise.

The scientific novelty consists in the improvement of work process with the personnel to ensure the information security at an enterprise.

CONFIDENTIAL INFORMATION, INFORMATION LEAKAGE, HUMAN FACTORS, MOTIVATION, ALGORITHM, PSYCHOLOGICAL CLIMATE

Список умовних скорочень

АН – агентство нерухомості;

ВАТ – відкрите акціонерне товариство;

Д – доступність;

ЗІ – захист інформації;

ЗМІ – засоби масової інформації;

ІзОД – інформація з обмеженим доступом;

К – конфіденційність;

КЗ – контрольована зона;

НСД – несанкціонований доступ;

ОІД – об’єкт інформаційної діяльності;

ОС – операційна система;

ПЕОМ – персональна електронно-обчислювальна машина;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

Ц – цілісність.

ЗМІСТ

ВСТУП

Інформаційна безпека в даний час є основою будь-якого підприємства, що прагне до вдосконалення та розвитку. Проблема забезпечення інформаційної безпеки стає з кожним роком все більш актуальною і значущою в зв'язку з загальним переходом інформаційних технологій в управлінні на автоматизовану основу.

Ця кваліфікаційна робота присвячена розгляду проблеми витоку конфіденційної інформації з вини персоналу компанії. Актуальність даної теми полягає в тому, що на тлі досить серйозного ставлення до захисту державної і військової таємниці, проблема захисту конфіденційної інформації в комерційних організаціях не усвідомлюється поки ще повною мірою.

В даний час відомо безліч загроз конфіденційної інформації і відповідно до цього розроблені різні системи щодо захисту від них, проте, головною причиною більшої частини внутрішніх порушень залишається слабка підготовка співробітників організацій у питаннях інформаційної безпеки. Рішення даної проблеми є дуже важливим, так як навіть за наявності добре налагодженої системи захисту, «людський фактор» може бути найбільш слабкою ланкою, що зведе нанівець усі зусилля із захисту інформації.

Метою кваліфікаційної роботи є підвищення рівня безпеки підприємства на основі розробки алгоритму запобігання витоку конфіденційної інформації з вини персоналу. При досягненні поставленої мети галузь застосування є дуже великою. Це пов’язано з тим, що майже в кожній організації циркулює інформація з обмеженим доступом і у кожній є свій штат співробітників, який працює з нею, тому у керівників організацій завжди буде поставати питання захисту її від витоку.

Для досягнення поставленої мети вирішуються наступні завдання:

- проаналізувати об’єкт інформаційної діяльності;
- проаналізувати можливі загрози конфіденційної інформації для даного об’єкта інформаційної діяльності;

- дослідити загрози, які пов’язані з витоком інформації з вини персоналу;
- розробити алгоритм запобігання витоку конфіденційної інформації з вини персоналу;
- впровадити розроблений алгоритм на підприємство з подальшим контролем його функціонування.

Об'єктом дослідження є процес забезпечення інформаційної безпеки на підприємстві.

Базою дослідження виступає агентство нерухомості «Резидент».

Предметом дослідження у цій роботі виступає алгоритм запобігання витоку конфіденційної інформації з вини персоналу.

У роботі були використані наступні методи дослідження: аналітичний метод (опис, аналіз, спостереження, опитування); загальнонауковий метод (аналіз публікацій і статей по темі), а також вивчення нормативно-правової бази.

1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Канали розповсюдження і витоку конфіденційної інформації

Інформаційні джерела завжди розповсюджуються у зовнішнє середовище. Канали розповсюдження інформації носять об'єктивний характер та відрізняються активністю і включають у себе: ділові, управлінські, торгові, наукові, комунікативні регламентовані зв'язки; інформаційні мережі; природні технічні канали.

Канал розповсюдження інформації представляє собою шлях переміщення цінних відомостей з одного джерела в інший в санкціонованому режимі або в силу об'єктивних закономірностей.

Витік конфіденційної інформації являє собою неправомірний, тобто недозволений вихід цінної інформації за межі зони. Витік конфіденційної інформації означає не тільки отримання її особами, які не працюють на підприємстві, до витоку призводить і несанкціоноване ознайомлення з конфіденційною інформацією осіб даного підприємства.

Витік може відбутися при розголошенні конфіденційної інформації, в результаті втрати носія конфіденційної інформації, а також розкрадання носія інформації або відображеної у ньому інформації при схоронності носія у його власника. Розкрадання конфіденційної інформації також не завжди пов'язане з отриманням її особами, що не мають до неї доступу. Чимало прикладів, коли розкрадання носіїв конфіденційної інформації здійснювалося у колег по роботі, допущеним до цієї інформації, особами з метою заподіяння шкоди колезі. Але в будь-якому випадку втрата і розкрадання конфіденційної інформації, якщо і не призводять до її витоку, то завжди створюють загрозу витоку. Враховуючи велику кількість існуючих каналів розповсюдження і витоку конфіденційної інформації, в даній роботі головна увага була спрямована на вивчення і аналіз каналів витоку інформації через персонал.

1.2 Канали витоку конфіденційної інформації через персонал

Людина, як об'єкт впливу, більш схильна до неформальних впливів, ніж технічні засоби та інші носії конфіденційної інформації, в силу певної правової незахищеності в поточний момент своїх індивідуальних людських слабкостей і життєвих обставин.

Такий неформальний вплив має, як правило, прихований, нелегальний характер і може здійснюватися як індивідуально, так і групою осіб.

Особі, яка є носієм конфіденційної інформації, можуть зашкодити наступні види каналів витоку інформації: мовний канал, фізичний і технічний.

Мовний канал витоку - інформація передається від власника (носія) конфіденційної інформації за допомогою слів особисто об'єкту, зацікавленому в отриманні цієї інформації.

Фізичний канал витоку - інформація передається від власника конфіденційної інформації за допомогою паперових, електронних, магнітних (зашифрованих або відкритих) чи інших засобів об'єкту, зацікавленому в отриманні цієї інформації.

Технічний канал витоку - інформація передається за допомогою технічних засобів.

Форми впливу на особу, що являється носієм захищаємої інформації, можуть бути відкритими або прихованими.

Відкритий вплив на власника конфіденційної інформації передбачає безпосередній контакт.

Прихований вплив на власника конфіденційної інформації здійснюється опосередковано.

Засобом неформального впливу на власника конфіденційної інформації, для отримання від нього певних відомостей, через відкритий мовний канал є - людина або група людей, які взаємодіють за допомогою: обіцянок, прохання, натяків. У результаті цих дій власник конфіденційної інформації змушений змінити свою поведінку, свої службові зобов'язання і передати необхідну інформацію.

Прихований вплив за допомогою мовного каналу на власника конфіденційної інформації здійснюється за допомогою непрямого примусу, шантажу через третю особу, ненавмисного або навмисного прослуховування і т.ін.

Форми впливу на власника конфіденційної інформації через фізичний канал витоку може бути також відкритим або прихованим.

Відкритий вплив здійснюється за допомогою силового (фізичного) залякування (побоїв).

Прихований вплив є більш витонченим, з точки зору застосування засобів. Зацікавлений об'єкт впливає приховано на інтереси і потреби людини, що має доступ до конфіденційної інформації. Такий схований вплив може гуртуватися на: страху, шантажі, маніпулюванні фактами, хабарі, підкупі, корупції, переконанні, наданні послуг, завіренні про майбутнє особи, яка є носієм конфіденційної інформації.

Форма впливу на власника конфіденційної інформації технічними каналами також може бути відкритою чи прихованою.

Відкриті засоби - факсові, телефонні, Інтернет, радіозв'язок, телекомунікації, ЗМІ.

До прихованих засобів можна віднести: прослуховування з використанням технічних засобів, перегляд з екрана дисплея та інших засобів її відображення, несанкціонований доступ до ПЕОМ та програмно-технічних засобів.

Всі розглянуті засоби впливу незалежно від їх форм, роблять неформальний вплив на особу, що має доступ до конфіденційної інформації, і можуть бути пов'язані з протизаконними і кримінальними способами отримання конфіденційної інформації. Тому можливості маніпулювання індивідуальними особливостями людини, яка, відповідно до своєї посади, має доступ до конфіденційною інформацією, її соціальними потребами, з метою отримання потрібних даних, обов'язково необхідно враховувати при

розстановці, підборі кадрів і проведенні кадрової політики при організації робіт з конфіденційною інформацією.

Витік інформації може характеризуватися двома умовами:

- інформація переходить безпосередньо до зацікавленої в ній особі;
- інформація переходить до випадкової людини, третій особі.

Під третьою особою в даному випадку розуміється будь-яка стороння особа, що отримала інформацію в силу обставин, незалежних від цієї особи, чи безвідповідальності персоналу, що не має права доступу до неї, і, головне, ця особа не зацікавлена в даній інформації. Однак від третьої особи інформація може легко перейти до зловмисника.

Ненавмисний перехід інформації до третьої особи настає в результаті:

- втрати або неправильного знищення носія інформації;
- ігнорування або умисного невиконання працівником вимог щодо захисту інформації;
- зайвої балакучості працівників – з колегами по роботі, родичами, друзями, іншими особами в місцях загального користування;
- роботи з конфіденційною інформацією при сторонніх особах, або несанкціонованої передачі її іншому працівникові;
- використання конфіденційної інформації у відкритих документах, публікаціях, інтерв'ю, особистих записах, щоденниках тощо;
- самовільного розмноження працівником документів, в тому числі електронних, в службових або колекційних цілях.

На відміну від третьої особи зловмисник або його спільник цілеспрямовано видобувають конкретну інформацію і навмисно, незаконно встановлюють контакт з джерелом цієї інформації.

Організаційні канали витоку інформації відрізняються великою різноманітністю видів і засновані на встановленні різноманітних, в тому числі законних, взаємовідносин зловмисника з підприємством або співробітниками підприємства, для подальшого несанкціонованого доступу до інформації, що їх цікавить.

Основними видами організаційних каналів можуть бути: прихід на роботу зловмисника, як правило, на технічну або допоміжну посаду (оператором на комп'ютері, експедитором, кур'єром, прибиральницею, двірником, охоронцем, шофером і т.п.); участь в роботі підприємства в якості партнера, посередника, клієнта; пошук зловмисником спільника, що працює в організації, який може стати його співучасником; встановлення зловмисником довірчих взаємин з працівником організації або постійним відвідувачем; використання комунікативних зв'язків організації - участь у переговорах, нарадах, виставках, презентаціях, листуванні; використання помилкових дій персоналу або умисне провокування зловмисником цих дій; таємне або за фіктивними документами проникнення в будівлю підприємства та приміщення, кримінальний, силовий доступ до інформації, тобто крадіжка документів, жорстких дисків (вінчестерів) або самих комп'ютерів, шантаж і схиляння до співпраці окремих працівників, підкуп і шантаж працівників, створення екстремальних ситуацій і т.ін.; отримання потрібної інформації від третьої (випадкової) особи.

Організаційні канали відбираються або формуються зловмисником індивідуально відповідно до його професійного уміння, конкретної ситуації, і прогнозувати їх украй складно. Виявлення організаційних каналів вимагає проведення серйозної пошукової та аналітичної роботи.

1.3 Аналіз можливих загроз витоку конфіденційної інформації

Основною загрозою інформаційної безпеки є несанкціонований доступ зловмисника або сторонньої особи до конфіденційної інформації і, як результат, оволодіння інформацією і незаконне, протиправне її використання.

Найбільш частими загрозами конфіденційних документів є:

- несанкціонований доступ сторонньої особи до документів, справ і баз даних за рахунок його цікавості або обманних, провокуючих дій, а також випадкових або навмисних помилок персоналу підприємства;

- втрата документа або його окремих частин, носія чорнового варіанту документа або робочих записів за рахунок крадіжки, втрати, знищення;
- втрата конфіденційності інформації за рахунок її розголошення персоналом або витоку по технічних каналах, зчитування даних в чужих масивах, використання залишкової інформації на копіювальній стрічці, папері, дисках, помилкових дій персоналу;
- заміна документів, носіїв і їх окремих частин з метою фальсифікації, а також приховування факту втрати, викрадення;
- випадкове або навмисне знищення цінних документів і баз даних, несанкціонована модифікація і спотворення тексту, реквізитів, фальсифікація документів;
- втрата документів в умовах екстремальних ситуацій.

У відношенні конфіденційної інформації, що обробляється і зберігається в комп'ютерах, умови виникнення загроз, класифікуються за ступенем ризику наступним чином: ненавмисні помилки користувачів, які обслуговують інформаційні системи; крадіжки і підробки інформації; стихійні ситуації зовнішнього середовища; зараження вірусами.

Структура системи, склад і зміст комплексу частин забезпечення системи захисту інформації підприємства, їх взаємозв'язок залежать від цінності інформації, що захищається й охороняється, характеру виникаючих загроз інформаційної безпеки підприємства, необхідного захисту і вартості системи.

Одним з основних ознак захищеності інформації є обмеження, що вводяться власником інформації на її поширення і використання.

Ризик загрози витоку будь-яких інформаційних ресурсів (відкритих і з обмеженим доступом) створюють стихійні лиха, екстремальні ситуації, аварії технічних засобів і ліній електропостачання, зв'язку, інші об'єктивні обставини, а також зацікавлені і не зацікавлені у виникненні загрози особи.

Головним завданням захисту інформації – є організація захисту доступу (фізичного або програмного) до місця перебування конфіденційної інформації таким чином, щоб максимально ускладнити процес несанкціонованого доступу до даних, що захищаються.

1.4 Аналіз об’єкта інформаційної діяльності

1.4.1 Характеристика об’єкта інформаційної діяльності

В якості об'єкта інформаційної діяльності в даній роботі було розглянуто агентство нерухомості «Резидент». АН «Резидент» - це ріелторська фірма, що оперує на ринку нерухомості міста Дніпра.

АН "Резидент" має велику інформаційну базу об'єктів житлової і комерційної нерухомості по всіх районах міста Дніпра і передмістя.

Агентство надає послуги, до складу яких входять:

1) посередницькі послуги з питань купівлі-продажу, дарування, обміну, розміну об'єктів нерухомості;

2) перевірка та підготовка всіх необхідних документів;

3) інформаційно-посередницькі послуги з питань оренди об'єктів нерухомості;

4) підбір ексклюзивних варіантів;

5) ексклюзивне обслуговування клієнтів;

6) професійні консультації з питань, пов'язаних об'єктами нерухомості.

На підприємстві зберігається інформація про співробітників і клієнтів, звіти по фінансовій діяльності фірми, кредитні договори з банками, договори з клієнтами, інформаційна база даних, дані про вигідних партнерів.

Характеристика будівлі

Агентство нерухомості «Резидент» розташоване в одноповерховій будівлі. Займає площу 381 м.кв.

Контрольована зона знаходиться в межах стін будівлі.

Обстановка навколо будівлі:

південь: п'ятиповерхові житлові будинки, відстань до яких 200 м.

північ: лікарня, відстань до якої 150 м.

захід: двоповерхова будівля, відстань до якої 60 м;

схід: триповерхова адміністративна будівля, відстань до якого 90 м.

В офісі встановлено автономне опалення. Каналізаційний канал має вихід за межі контрольованої зони. Водопостачання від міського водоканалу також виходить за межі контрольованої зони. 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.

Технічні параметри будівлі:

- Матеріал зовнішніх стін - силікатна цегла, товщина - 450 мм.
- Матеріал внутрішніх стін - силікатна цегла, товщина - 200 мм.
- Вікна - потрійні металопластикові склопакети, ширина 1900 мм, висота 1300 мм, товщина скла 36 мм.
- Міжкімнатні двері - металопластикові, товщина 40 мм.
- Вхідні двері - дерев'яні, товщина 40 мм.
- Стеля товщиною 120 мм виготовлена із залізобетону.
- Дах побудований з дерев'яного каркасу, вкритого металочерепицею.
- Підлога - ламінат.

Штат співробітників: 30 чоловік

Посади по відділам:

1) Керівництво: директор; заступник директора;
2) Приймальна: секретар;
3) Рекламний відділ: менеджер з реклами;
4) Відділ по роботі з клієнтами: менеджери по роботі з клієнтами (ріелтори) - 15 осіб.
5) Відділ по роботі з персоналом: менеджер по роботі з персоналом;
6) Бухгалтерський відділ: головний бухгалтер;
7) Юридичний відділ: юрист;

8) Серверна: системний адміністратор;

9) Кімната охорони: охорона - 6 чоловік.

А також, прибиральниця.

Режим роботи:

- Організований 5-ти денний робочий тиждень;
- Робочий день з 9.00-18.00;
- Перерва з 12.00-13.00 ;
- Вихідний: субота, неділя;
- Прибирання здійснюється щодня в період з 7.00-9.00;
- Об'єкт охороняється цілодобово;
- Режим охорони: добу, через двоє. У зміні 2 людини.

1.4.2 Класифікація інформаційних об’єктів

Для всіх інформаційних об'єктів, виявлених у процесі обстеження АН «Резидент» була проведена класифікація за ознаками доступності (Д), цілісності (Ц), конфіденційності (К) – значення класифікації ДЦК [7] наведені в Додатку Б. Результати були занесені в таблицю 1.1.

Таблиця 1.1– Класифікація інформаційних об’єктів

№	Найменування	За доступністю	За цілісністю	За конфіденційністю
1	Фінансова інформація (звіти для податкової інспекції, фінансові звіти, бухгалтерський облік)	Д4	Ц3	К3
2	Інформація про клієнтів	Д4	Ц3	К4
3	Інформація про співробітників	Д1	Ц1	К1
4	Договори з клієнтами	Д1	Ц1	К2
5	Інформація про партнерів підприємства	Д2	Ц1	К2

1.4.3 Профіль захищеності для інформаційної системи

Згідно з НД ТЗІ 2.5-005-99 дана автоматизована система відноситься до класу «3» тому що це розподілений багатомашинний багатокористувачевий 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, ЦО-2, ЦВ-2,
ДР-2, ДС-1, ДЗ-1, ДВ-2,
НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, НВ-2 }

КД-2 (базова довірча конфіденційність);

КА -2 (базова адміністративна конфіденційність);

КО-1 (повторне використання об’єктів);

КК-1 (виявлення прихованих каналів);

КВ-3 (повна конфіденційність при обміні);

ЦД-1 (мінімальна довірча цілісність);

ЦА-3 (повна адміністративна цілісність);

ЦО-2 (повний відкат);

ЦВ-2 (базова цілісність при обміні);

ДР-2 (недопущення використання ресурсів);

ДС-1 (стійкість до відмов);

ДЗ-1 (модернізація);

ДВ-2 (відновлення після збоїв);

НР-3 (сигналізація про небезпеку);

НИ-2 (одинична ідентифікація и автентифікація);

НК-1 (достовірний канал);

НО-2 (розподіл обов’язків);

НЦ-3 (цілісність КЗЗ);

НТ-2 (самотестування при старті);

НВ-2 (автентифікація при обміні) [6].

1.4.4 Схема інформаційної системи

Інформаційна система підприємства забезпечує підтримку основних процесів управління підприємством і забезпечує безпечну роботу з цінною інформацією. На рисунку 1.1 наведений план приміщення АН «Резидент» з функціонуючою інформаційною системою.

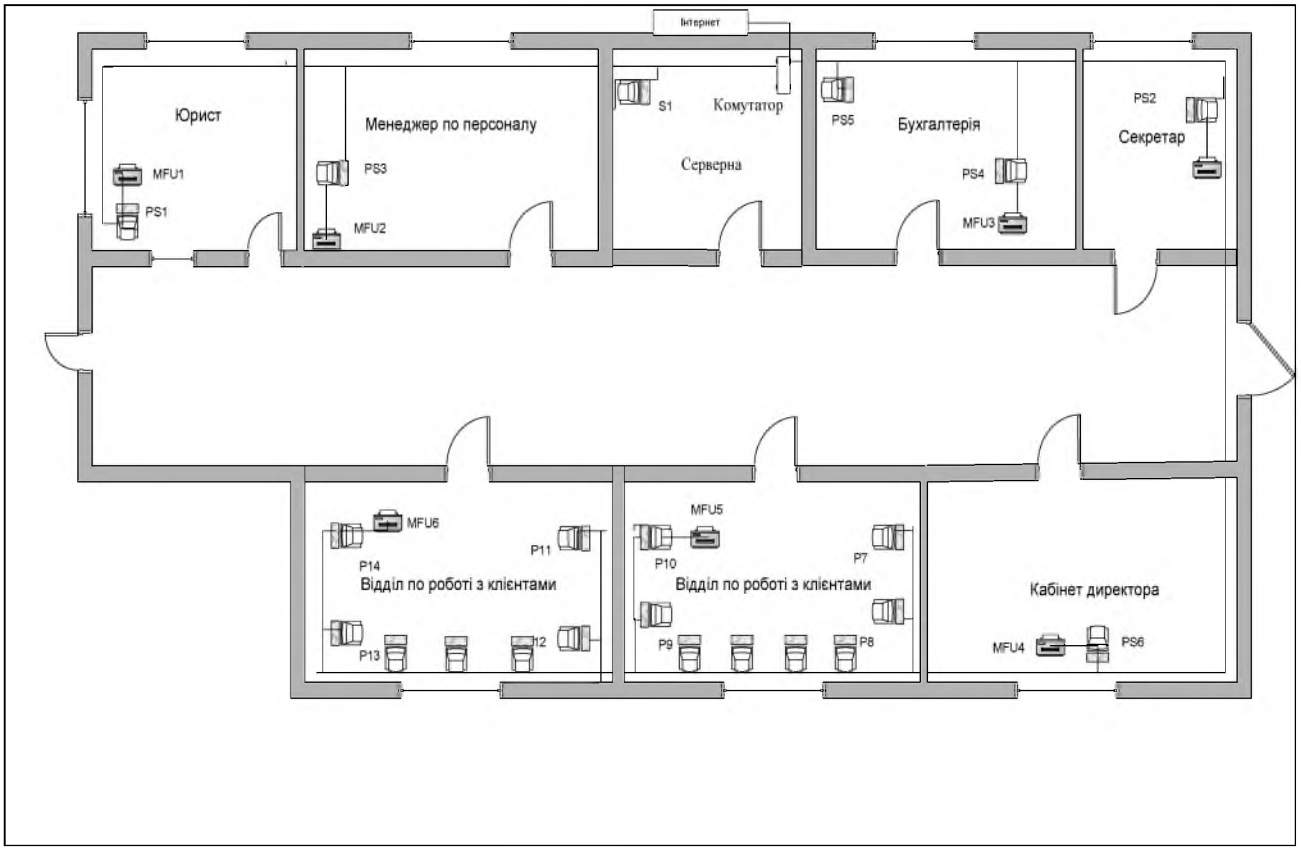
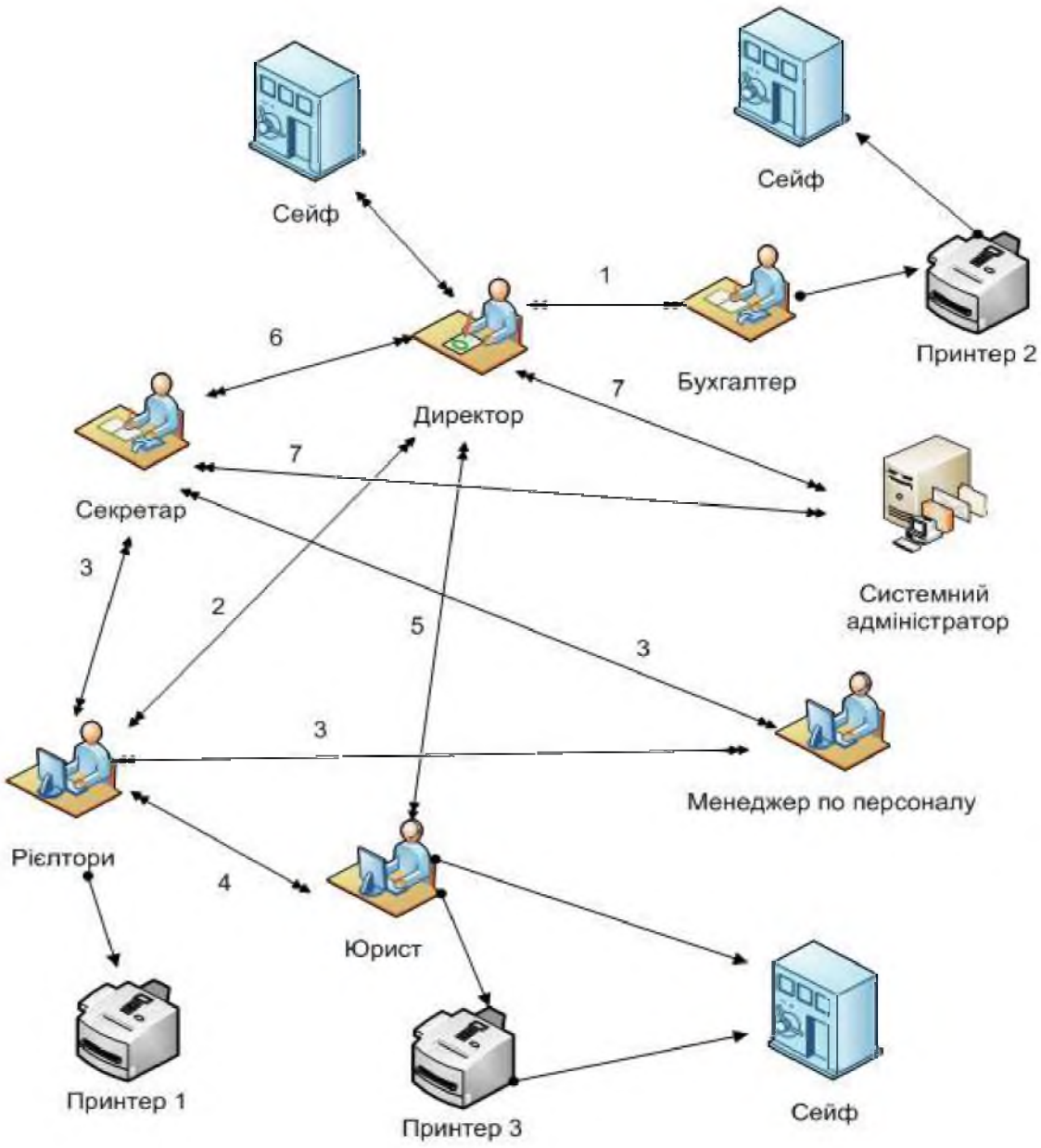


Рисунок 1.1 – Схема інформаційної системи

1.4.5 Схема інформаційних потоків

Внутрішні інформаційні потоки представляють собою фізичне переміщення інформації серед працівників підприємства. При організації інформаційних потоків, головною метою є оптимізація роботи підприємства. Схема інформаційних потоків АН «Резидент» наведена на рисунку 1.2.



1-фінансова інформація;

2-звіти про угоди;

3-організаційна інформація;

4-договори з клієнтами

5-договори з клієнтами, партнерами;

6- офісна інформація;

7- технічна інформація

Рисунок 1.2 – Схема інформаційних потоків

1.5 Постановка задачі

Актуальність даної роботи полягає в тому, що на сьогоднішній день існує досить серйозне ставлення до захисту державної і військової таємниці, а проблема захисту конфіденційної інформації в комерційних організаціях не усвідомлюється поки ще повною мірою. В даний час відомо безліч загроз конфіденційної інформації і відповідно до цього розроблені різні системи щодо захисту від них, проте, головною причиною більшості частини внутрішніх порушень залишається слабка підготовка співробітників організацій у питаннях інформаційної безпеки. Рішення даної проблеми є дуже важливим, так як, навіть за наявності добре налагодженої системи захисту, «людський фактор» може бути найбільш слабким місцем, що зведе нанівець усі зусилля по захисту інформації.

Для досягнення поставленої мети в даній роботі були поставлені наступні задачі:

1) провести аналіз об’єкта інформаційної діяльності;

2) проаналізувати можливі загрози конфіденційної інформації для даного об’єкта інформаційної діяльності;

3) дослідити загрози, які пов’язані з витоком інформації через персонал;

4) визначити та обґрунтувати методи по запобіганню витоку конфіденційної інформації через персонал;

5) впровадити розроблений алгоритм на підприємство, з подальшим контролем його функціонування.

2 СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Аналіз загроз витоку конфіденційної інформації з вини персоналу

Головною загрозою у системі захисту інформації є людина. За допомогою технічних, юридичних, організаційних складових люди захищають інформацію від людей. Саме людина, за допомогою технічних чи інших засобів, намагається отримати інформацію. Саме через недбале відношення до довірених людині даних, ці дані можуть бути втрачені. На сьогоднішній день існує все більше і більше можливостей отримання інформації, в тому числі й інформації з обмеженим доступом. З'являється все більше загроз витоку даних. А з розвитком новітніх технологій способи їх отримання постійно вдосконалюються. Отже, повинні існувати засоби, що здатні забезпечити захист інформації з обмеженим доступом.

Керівники підприємств дуже багато уваги приділяють забезпеченню захисту від технічного витоку інформації, проте вони забувають, що загроза витоку інформації може бути пов'язана з їхнім власним персоналом. Виходячи із даних антирейдерського союзу підприємців України:

1) 82% загроз реалізується власними співробітниками фірми або при їх прямій чи опосередкованій участі;

2) 17% загроз реалізується ззовні підприємства;

3) 1% загроз реалізується випадково.

Найпоширеніші фактори розголошення співробітниками інформації з обмеженим доступом наведені у таблиці 2.1.

Таблиця 2.1 – Фактори розголошення співробітниками інформації

№ п/п	Фактори	Частота появи фактора,%
1	Надмірна балакучість співробітників	32
2	Прагнення співробітників заробляти гроші будь-якими способами та за будь-яку ціну	24
3	Відсутність на фірмі служби безпеки	14
4	Звички співробітників фірми ділитися один з одним (традиційний обмін досвідом)	12
5	Безконтрольне використання інформаційних систем	10
6	Наявність можливостей виникнення серед співробітників конфліктних ситуацій	8

Як видно з таблиці, розголошення співробітниками інформації з обмеженим доступом найчастіше здійснюється через те, що керівництва компаній не приділяють уваги загрозам витоку інформації, пов’язаним з персоналом.

Для кращого розуміння можливостей витоку інформації та визначення способів його попередження були розглянуті декілька класифікацій самих порушників та класифікацію загроз, пов’язаних з персоналом.

Недбалі співробітники є найбільш поширеним типом внутрішніх порушників. Їх порушення у відношенні до конфіденційної інформації носить немотивований характер, не має конкретних цілей, наміру, користі.

Порушники, якими маніпулюють – це ті співробітники, яких обманним шляхом штовхають на порушення встановлених норм. Такі співробітники часто і не підозрюють про те, що їхні дії призводять до втрати конфіденційних даних.

Скривджені порушники – це співробітники, які прагнуть завдати шкоди компанії за особистими причинами. Найчастіше причиною такої поведінки може бути образа, що виникла із-за недостатньої оцінки їх ролі в компанії, недостатній розмір матеріальної компенсації, неналежне місце в корпоративній ієрархії, відсутність елементів моральної мотивації.

Наступний тип внутрішніх порушників — нелояльні порушники. Перш за все, це співробітники, що вирішили змінити місце роботи. Співробітники, що підробляють і впроваджені внутрішні порушники — це співробітники, мету яких визначає замовник викрадання інформації. У обох випадках співробітники прагнуть якомога надійніше замаскувати свої дії (принаймні, до моменту успішного розкрадання) [10].

Також сформована класифікація, що відображає зовнішні і внутрішні загрози підприємства, які пов'язані з персоналом.

Зовнішньою загрозою є така загроза, що знаходиться за межами підприємства, але саме через існування якої потрібно захищати інформацію і через яку існують загрози внутрішні. Адже, як би не було зацікавлених осіб в отриманні інформації підприємства, її не потрібно було б захищати. До зовнішніх загроз можна віднести протиправну діяльність кримінальних структур, конкурентів, фірм або приватних осіб, що займаються промисловим шпигунством та соціальною інженерією.

До внутрішніх загроз відносяться дії чи бездіяльність співробітників, що протидіють інтересам діяльності підприємства, наслідком яких може бути нанесення економічних збитків компанії, втрата інформаційних ресурсів, підрив ділового іміджу компанії, виникнення проблем у відносинах з реальними та потенційними партнерами тощо.

Розглянемо ці загрози більш детально. До зовнішніх належать:

а) промислове шпигунство – метою якого частіше всього буває: або перевірка ділового партнера на благонадійність, або ж знищення конкурента чи нанесення йому серйозних збитків. І, якщо в першому варіанті немає загроз підприємству, то в другому, якщо конфіденційна інформація потрапляє до рук

таких людей, це найчастіше призводить до дуже серйозних наслідків для підприємства, закінчуючи його банкрутством та ліквідацією.

І хоча існує багато технічних засобів для здобуття інформації, промисловим шпигунам інколи просто достатньо поговорити з працівниками, які, самі того не підозрюючи, можуть надати досить суттєву інформацію, якою конкуренти не втратять нагоди скористуватися. За оцінками фахівців, на частку людського фактору, тобто на балакучість співробітників, припадає до 60% всього витоку інформації. Інші 40% - це те, що вдається перехопити технічними засобами [9];

б) соціальна інженерія – це метод несанкціонованого доступу до інформації або систем зберігання інформації без використання технічних засобів [8]. Метод заснований на використанні слабкості людського чинника і вважається дуже руйнівним. Зловмисник отримує інформацію, наприклад, шляхом збору персональних даних про службовців об'єкту атаки, за допомогою звичайного телефонного дзвінка або шляхом проникнення в організацію під виглядом її службовця. Зловмисник може подзвонити працівникові компанії (під виглядом технічної служби) і вивідати пароль, пославшись на необхідність вирішення невеликої проблеми в комп'ютерній системі.

До внутрішніх загроз належать:

а) необережність персоналу. Дуже часто співробітники, хоч й не мають на меті розголосити конфіденційні відомості, роблять це, інколи навіть не розуміючи цього. Тож необережність можна поділити на дві категорії:

- дії чи бездіяльність співробітників, спричинені необізнаністю у сфері захисту інформації;
- дії чи бездіяльність співробітників у випадку, в яких співробітники знали або не знали, але повинні були знати про можливі негативні наслідки.

У першому випадку не можна казати про вину співробітника, скоріше це прорахунки вищого керівництва, яке не потурбувалося роз’яснити персоналу про важливість інформації і про її захист. Інколи керівники, як метод захисту

інформації, практикують не казати працівникам про важливість даних. У Кримінальному Кодексі України необережність поділяють саме на злочинну самовпевненість та злочинну недбалість.

Під злочинною самовпевненістю розуміють дії чи бездіяльність особи, коли вона знала про можливі негативні наслідки, передбачала їх настання, але зухвало розраховувала на їх відвернення.

Злочинною недбалістю є дії чи бездіяльність особи, коли вона не знала, але повинна була знати про можливі негативні наслідки свого діяння [11].

В усіх цих випадках метою співробітника не було розголошення конфіденційних відомостей, та саме до цього призвели його дії;

б) навмисні дії працівників по розголошенню інформації та мотиви цих дій. На відміну від необережності, навмисна дія передбачає, що метою дій співробітників було саме розголошення інформації, що є конфіденційною. Для того щоб виявити або попередити такі дії, потрібно визначитися, чому ж саме працівники пішли на них. Кожна людина є індивідуальною, в кожного своє життя та свої проблеми, через які він приймає ті чи інші рішення. Тож кожна ситуація має свої нюанси, але є декілька розповсюджених причин для розголошення інформації співробітниками.

До них відносяться: помста, матеріальна або інша вигода, самореалізація.

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

Тож загроза цілісності інформації йде від людини. Можна встановити найсучасніші системи технічного захисту, видати мільйони нормативних актів, які регулюють захист інформації, але поки буде ігноруватися людський фактор, доти юридичні, організаційні та технічні засоби будуть мало ефективними.

Проаналізувавши загрози конфіденційності даних, які пов'язані з персоналом, можна зробити висновок, що ігнорування цих загроз може призвести до серйозних збитків для підприємствах, в різних ситуаціях, мова може йти не тільки про фінансові втрати підприємства, але й про різке падіння його іміджу у зв'язку з тим, що воно не може захистити власну конфіденційну інформацію.

2.2 Порядок прийому співробітників на роботу

Один з найбільш важливих етапів у роботі з персоналом підприємства є процес відбору можливих кандидатів для призначення на посади, пов'язаних з роботою з конфіденційною інформацією. Тому що, якщо з самого початку посаду, яка передбачає доступ до конфіденційної інформації, займе недобросовісна або зі злочинними намірами людина, то всі інші заходи, які будуть проводитися, не зможуть запобігти витоку цінної інформації.

Пошук кандидата на знову створювану чи вакантну посаду на підприємстві не повинен носити безсистемний характер. Це пов'язано з тим, що випадкова людина, яка прийшла з вулиці, до певної міри таїть небезпеку для підприємства, як з точки зору його професійної придатності, так і особистих, моральних якостей.

Існує ряд ефективних напрямів активного пошуку кандидатів на вакантну посаду або робоче місце. До числа основних напрямків можна віднести:

1) пошук, кандидатів всередині підприємства, особливо якщо мова йде про керівника або фахівця високого рівня. Цей метод дає можливість просувати перспективних працівників по службових сходах і зацікавлювати їх

роботою, виховувати відданість справам фірми. Можна запрошувати на посаду особу, яка раніше працювала на підприємстві і добре себе зарекомендувала.

Перерозподіл персоналу відповідно до його схильностей і здібностей завжди дає великий позитивний ефект в покращенні роботи підприємства та забезпеченні її інформаційної безпеки. Але треба враховувати, що підтримується колективом тільки таке просування по службі, яке визначається високими діловими якостями працівника. Не може отримати схвалення персоналу висунення працівника, за принципом особистих зв'язків або знайомства.

Великою перевагою цього методу є те, що про кандидата досить багато відомо всьому колективу і судити про професійні, моральні та особисті якості, відповідність запропонованої посади можна на підставі досить великого досвіду. Однак метод має недолік, який полягає в тому, що без приходу нових людей колектив втрачає свої новаторські якості. Тим не менше цей метод є найкращим і найбільш надійним при підборі кандидата на посаду, пов'язану з доступом до цінною і конфіденційною інформацією;

2) пошук кандидатів серед студентів та випускників навчальних закладів, встановлення зв'язків з підрозділами вузів, зайнятими працевлаштуванням випускників. Можна мати достатньо повну інформацію про професійні та особисті якості студентів. Дуже ефективно вести пошук найбільш здібних студентів, залучати їх у процесі навчання до роботи в організації, відплачувати їх працю і, може навіть, фінансувати навчання у вузі;

3) звернення в державні і приватні бюро, агентства з найму робочої сили, біржі праці, організації з працевлаштування осіб, звільнених за скороченням штатів, працевлаштування молоді, колишніх військовослужбовців тощо.

Подібні агентства пропонують потрібний контингент працівників на наявні робочі місця, ведуть цілеспрямований пошук необхідного фахівця високої кваліфікації, організовують перепідготовку фахівців за індивідуальними замовленнями;

4) рекомендації працюючих у фірмі співробітників. Зазвичай такі рекомендації відрізняються виваженим характером, так як з рекомендованими людьми співробітникам доведеться працювати разом.

Зазначені напрями пошуку кандидатів на посади, які пов'язані з доступом до цінної для підприємства інформації, як правило, дозволяють вибрати необхідних працівників з ряду осіб, які виявили бажання зайняти вакантну посаду.

В даній роботі був розроблений алгоритм, який наглядно демонструє удосконалений процес прийому співробітників на роботах, яка пов'язана з отриманням доступу до конфіденційної інформації. Даний алгоритм представлений на рисунку 2.1. Він включає наступні етапи:

- відбір можливого кандидата для прийому на роботу;
- вивчення його резюме (і особової справи, якщо кандидат працює на підприємстві) керівництвом підприємства, службою персоналу, виклик для бесіди;
- інформування кандидатів, що працюють на підприємстві, про їхні майбутні посадові обов'язки, пов'язаних з таємницею підприємства;
- попередня співбесіда керівництва підприємства, уточнення окремих положень резюме; відповіді на питання про майбутню роботу; вивчення отриманих від кандидата рекомендаційних листів;
- заповнення кандидатом заяви про прийом, автобіографії, особового листка по обліку кадрів, копій документів про освіту, наявності вчених ступенів, вчених та почесних звань, передача до відділу кадрів рекомендаційних листів і за наявності характеристик;
- співбесіда кандидатів з працівником відділу кадрів за наданими документами, при необхідності підтвердження тих чи інших відомостей поданням додаткових документів;
- співбесіда з метою визначення його особистих і моральних якостей, а також професійних здібностей;
- за сукупністю зібраних матеріалів і їх аналізу прийняття рішення

керівництвом підприємства про відбір претендента та можливості запропонувати йому роботу, пов'язану з доступом до цінної інформації підприємства;

- заключна співбесіда з претендентом на посаду, отримання від нього принципової згоди на роботу з конфіденційною інформацією;
- у разі згоди - підписання претендентом зобов'язання про нерозголошення таємниці підприємства, зокрема, конфіденційних відомостей, що йому повідомляються; інформування претендента про характер конфіденційної інформації, з якою він буде працювати, наявності системи захисту цієї інформації і тих обмежень, які доведеться враховувати працівникові в службовій та неслужбової обстановці;
- ознайомлення претендента з посадовою інструкцією, робочими технологічними інструкціями, інструкцією щодо забезпечення інформаційної безпеки підприємства і іншими аналогічними матеріалами;
- складання проєкту контракту, що містить пункт про обов'язок працівника не розголошувати конфіденційні відомості підприємства;
- складання і підписання наказу про зарахування на роботу з випробувальним терміном (або на тимчасову роботу);
- створення особової справи на прийнятого працівника;
- заповнення на співробітника необхідних облікових форм;
- внесення прізвища співробітника в первинні облікові бухгалтерські документи;
- внесення відповідного запису до трудової книжки працівника;
- вивчення особистих, моральних і професійних якостей працівника протягом випробувального терміну;
- навчання співробітника правилами роботи з конфіденційною інформацією, інструктажі;
- аналіз результатів роботи працівника протягом випробувального терміну, складання нового контракту про тривалу роботу і видання

відповідного наказу або відмови співробітнику у роботі;

- оформлення допуску працівника до конфіденційної інформації.

Вивчення документів слід поєднувати з об'єктивним аналізом кількох кандидатів, які претендують на посаду, зіставленням результатів співбесід, тестування, опитувань і т.ін. Все це в сукупності дозволить на конкурсній або позаконкурсній основі правильно провести відбір саме того претендента на посаду, який найбільше відповідає складеним раніше вимогам.

Надані кандидатом персональні документи ретельно перевіряються на достовірність: відповідність прізвищ, імен та по батькові, інших персональних даних, наявність необхідних відміток і записів, ідентичність фотокартки і особи громадянина, відповідність форми бланка рокам їх використання , відсутність незавірених виправлень, спроб заміни листів, фотографій, відповідність і якість печаток і т.ін. При сумнівах кандидата просять представити дублікати зіпсованих документів або завірити виправлення. Відомості, включені до характеристики, рекомендаційні листи, списки наукових праць і винаходів, видані і засвідчені іншими установами, можуть бути перевірені шляхом звернення до цих закладів. Документи, явно недостовірні, можуть бути повернуті громадянину, і одночасно йому відмовляється у розгляді питання про прийом на роботу без пояснення причини відмови. Відомості, які зазначаються в резюме, не перевіряються.

При підборі персоналу для роботи з цінною чи конфіденційною інформацією слід в першу чергу звертати увагу на особисті і моральні якості кандидатів на посаду, їх порядність і лише потім - на їхні професійні знання, вміння і навички.

Важливо вже на перших етапах відбору виключити ті кандидатури, які за формальними ознаками явно не відповідають вимогам, що пред'являються до майбутнього співробітника.

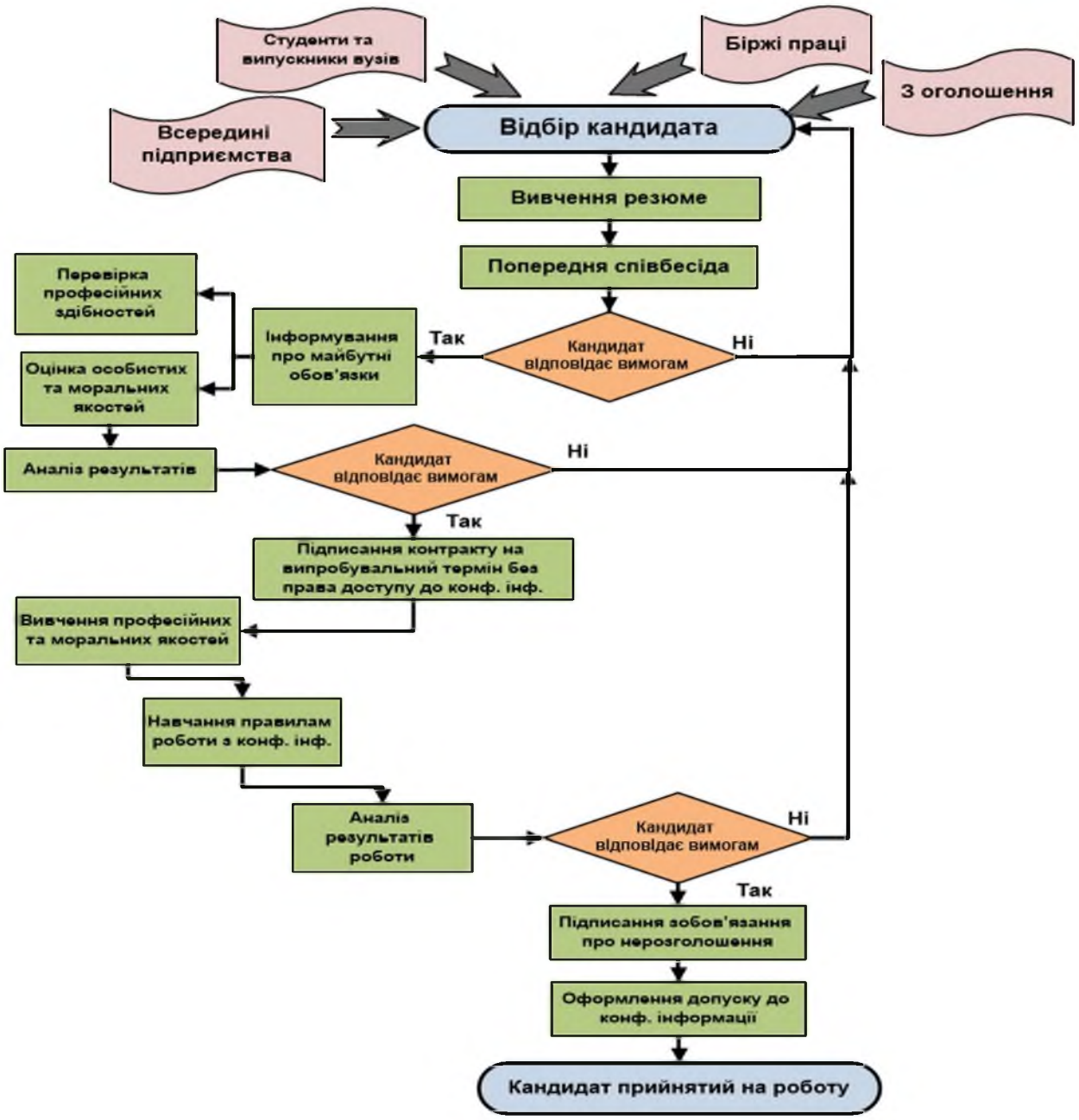


Рисунок 2.1 – Алгоритм прийому кандидатів на роботу, яка пов'язана з конфіденційною інформацією

Співбесіди з кандидатами на посаду переслідують такі цілі:

- виявити реальну причину бажання працювати в даному підприємстві;
- виявити можливих зловмисників або спробувати побачити слабкості кандидата як людини, які можуть провокувати злочинні дії;
- переконатися, що кандидат не має наміру використовувати в роботі секрети підприємства, в якому він раніше працював;
- переконатися у власній згоді кандидата дотримуватися правил захисту інформації та мати певні обмеження у професійному та

особистому житті.

Опитувальні листи для співбесіди складаються таким чином, щоб з'ясувати причини звільнення кандидата з попереднього місця роботи; чи працював кандидат раніше з конфіденційною інформацією, чи підписував зобов'язання про її нерозголошення.

Одним з головних завдань співбесіди є виявлення невідповідності мотивацій в різних логічних групах питань. Наприклад: хоче отримувати більшу заробітну плату, але раніше він одержував стільки ж, працював близько від дому, а хоче працювати у фірмі, що знаходиться на значній відстані, і т. ін.

З точки зору безпеки психологічний відбір переслідує такі цілі:

- виявлення судимості, злочинних зв'язків, кримінальних схильностей;
- визначення можливих злочинних схильностей, схильності кандидата до скоєння протиправних дій, зухвалих і необдуманих вчинків;
- встановлення чинників, що свідчать про морально-психологічну ненадійність, нестійкість, уразливість кандидата і т. ін.

При вмілому поєднанні традиційних і психологічних кадрових методів аналізу можна з певним ступенем вірогідності прогнозувати поведінку співробітників у різних, у тому числі екстремальних, ситуаціях.

Зазвичай відібраним для роботи вважається кандидат, у якого результати аналізу документів, співбесід, перевірок, тестів і психологічного вивчення не суперечать один одному, і не містять даних, які перешкоджали б прийому на роботу. Матеріали перевірок і аналізу кандидатів на посаду є суворо конфіденційною інформацією.

Зобов'язання про нерозголошення конфіденційної інформації і збереження таємниці фірми претендент підписує до того, як йому буде повідомлено склад цінних відомостей, з якими йому доведеться працювати, і порядок захисту цих відомостей.

Зобов'язання про нерозголошення конфіденційних відомостей являє

собою правовий документ, яким претендент добровільно і письмово дає згоду на обмеження його прав щодо використання конфіденційної інформації. Одночасно у зобов'язанні претендент попереджається про відповідальність за розголошення цієї інформації. Добре, якщо зобов'язання містить пункт про те що співробітник не буде використовувати у своїй діяльності інформацію, що належить на правах власності підприємства, в якому він раніше працював. Підписання зобов'язання про нерозголошення таємниці підприємства слід передбачити для службовців фірми, які не мають безпосереднього відношення до закритих відомостями, однак мають можливість ознайомитися з ними при виконанні службових обов'язків (шофери, двірники, прибиральниці, співробітники охорони і ін.).

Вважається, що зобов'язання про нерозголошення таємниці підприємства не дає повної гарантії збереження цих відомостей, однак, як показує практика, істотно знижують ризик розголошення персоналом або іншими особами цих відомостей, ризик незаконного їх використання, а також кількість спроб конкурентів впровадити на фірму свою агентуру.

Після підписання зобов'язання і проведення бесіди-інструктажу з претендентом укладається трудовий договір (контракт). У контракті повинен бути пункт про обов'язок працівника не розголошувати відомості, що становлять таємницю підприємства, а також конфіденційні відомості партнерів і клієнтів, про зобов'язання дотримуватися правил захисту конфіденційних відомостей. Може бути пункт про власність підприємства на результати роботи працівника, на зроблені ним винаходи і відкриття та згоду співробітника на публікацію цих досягнень тільки з дозволу керівництва підприємства. Часто міститься пункт про обов'язок співробітника повідомляти в службу безпеки про всі спроби сторонніх осіб отримати у нього конфіденційну інформацію. В обов'язковому порядку включається пункт про обов'язок співробітника негайно повідомляти безпосередньому керівнику і службі безпеки про втрату носіїв конфіденційної інформації.

У заключній частині вказується ступінь відповідальності за

розголошення таємниці підприємства або недотримання правил захисту інформації. Зазвичай це розірвання трудового договору, при необхідності - подальше судовий розгляд. Після підписання наказу про зарахування на роботу у відділі кадрів формується особова справа співробітника, що включає стандартний набір документів.

Отже, ускладнений алгоритм прийому на роботу, пов'язану з доступом до конфіденційної інформації, і перевірки достовірності відомостей, зазначених у документах, дає можливість всебічно оцінити кандидата на посаду. З іншого боку, він дає змогу керівництву підприємства і самому кандидату оцінити ситуацію і без поспіху прийняти правильне рішення. Методи психологічного аналізу, що проводяться одночасно з добре зарекомендованими прийомами аналізу документів претендента на посаду, дозволяють зробити досить обґрунтовані висновки про придатність даної особи для зайняття вакантної посади, пов'язаної з доступом до конфіденційної інформації.

2.3 Поточна робота з персоналом

Постійна робота з персоналом підприємства, що мають доступ до конфіденційної інформації є одним з найбільш актуальних і важливих напрямків у діяльності керівництва та посадових осіб підприємства. У вирішенні проблеми комплексного захисту інформації на підприємстві усе більш значне місце займає вибір ефективних способів і методів роботи з персоналом. Будучи генератором нових ідей і винаходів, що прискорюють науково-технічний прогрес, персонал направляє максимальні зусилля на підвищення добробуту підприємства в цілому і кожного його співробітника зокрема. Проте персонал часто стає і основним джерелом витоку конфіденційної інформації.

Від того наскільки працівник підприємства підготовлений професійно в області захисту інформації, до якої він має доступ цілком залежить його

здатність протистояти можливим спробам отримання зловмисниками або представниками організацій-конкурентів важливою для них інформації.

Високий рівень підготовки співробітників підприємства в питаннях захисту конфіденційної інформації дозволить також максимально знизити ймовірність появи ненавмисних помилок у поводженні з цією інформацією, наявність яких також потенційно створює передумови до її отримання недоброзичливцями. І навпаки, виявлення співробітниками підприємства, низьких професійних навичок і негативних морально-ділових якостей, значно знизить ефективність системи захисту конфіденційної інформації на підприємстві в цілому, оскільки ніякі заходи організаційного та технічного характеру не компенсують можливий витік інформації з боку співробітників підприємства.

На рисунку 2.2 представлено алгоритм, який ілюструє етапи поточної роботи з персоналом, що має доступ до конфіденційної інформації. За умовою дотримання представленої послідовності дій, значно знижується ризик втрати цінної інформації.

Даний алгоритм включає в себе наступні процеси:

- навчання і систематичне інструктування співробітників;
- проведення регулярної виховної роботи з персоналом, що працює з конфіденційними даними та документами;
- постійний контроль за виконанням персоналом вимог щодо захисту конфіденційної інформації;
- контрольну роботу з вивчення ступеня обізнаності персоналу в області конфіденційних робіт підприємства;
- проведення службових розслідувань за фактами витоку інформації і порушень персоналом вимог щодо захисту інформації.

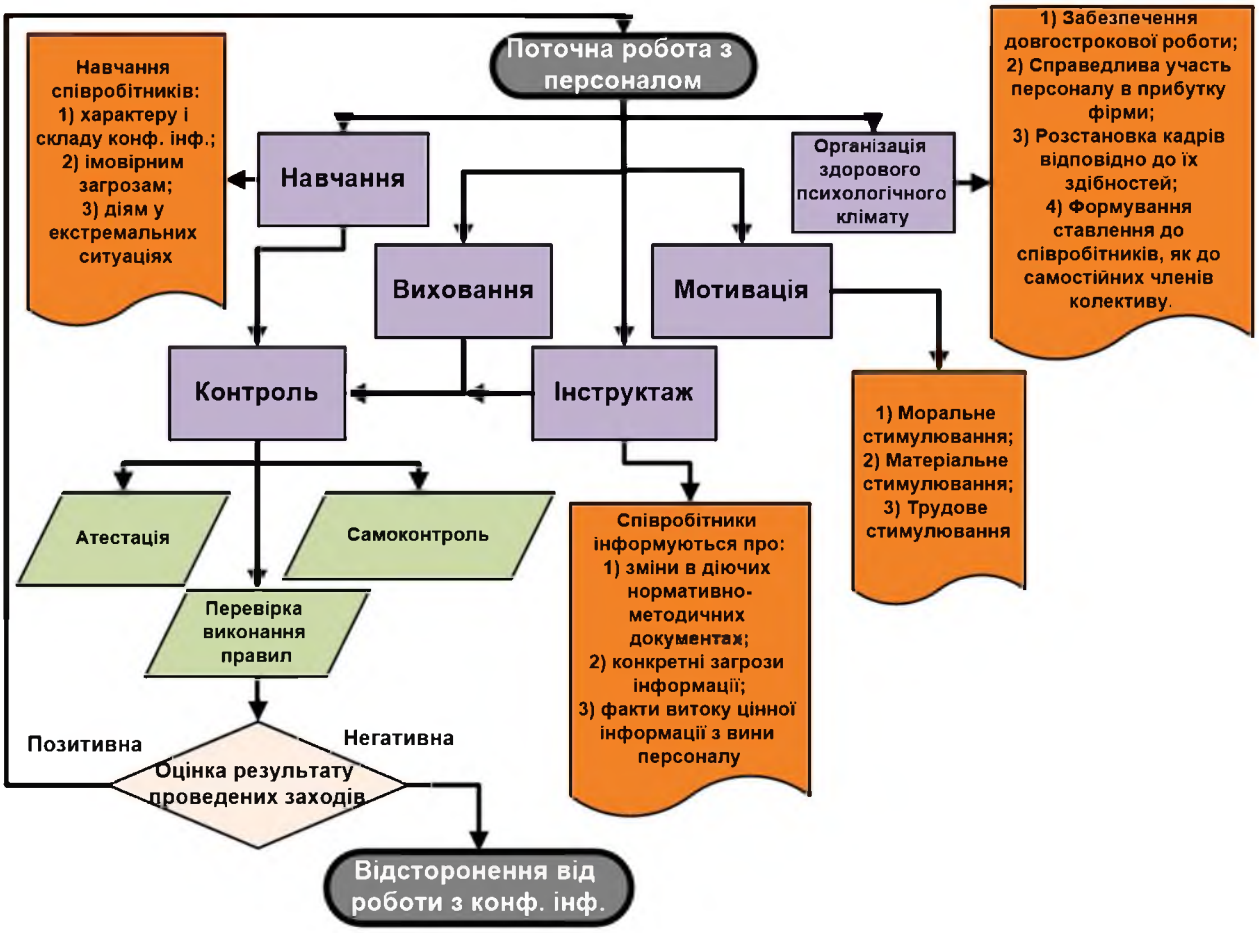


Рисунок 2.2 – Алгоритм поточної роботи з персоналом, який має доступ до конфіденційної інформації

2.3.1 Навчання та інструктаж співробітників

Метод навчання - першорядний метод роботи з персоналом підприємства, початковий етап у придбанні теоретичних знань і практичних навичок забезпечення захисту конфіденційної інформації в рамках виконання посадових обов'язків за основним фахом. Процес навчання співробітників підприємства повинен бути постійним і планомірним, так як система захисту цінної для підприємства інформації вимагає розвитку та вдосконалення.

Завдання навчання персоналу підприємства включає вивчення:

- нормативно-методичних документів по захисту використовуваних на підприємстві видів конфіденційної інформації;
- засобів системи захисту конфіденційної інформації підприємства;

- встановлених норм і правил захисту конфіденційної інформації на підприємстві, а також стандартів підприємства, положень про службу безпеки (режимно-секретний підрозділ);
- можливих загроз захисту конфіденційної інформації, їх характеру і можливих способів прояву;
- порядку роботи співробітників підприємства з носіями конфіденційної інформації з урахуванням встановлених вимог щодо режиму секретності.

Використовуються такі форми навчання:

- лекції, семінари та практичні заняття (тренажі) по діях персоналу в різних ситуаціях;
- тестування співробітників і оцінка рівня їх підготовленості;
- вирішення різних ситуаційних завдань, пов'язаних із захистом конфіденційної інформації;
- вирішення інтелектуальних завдань, спрямованих на отримання співробітниками підприємства навичок прогнозування різних ситуацій, пов'язаних з виникненням можливих каналів витоку інформації, загроз її безпеки;
- використання спеціалізованих програм навчання для забезпечення лекційних курсів і практичних занять.

Навчання персоналу підприємства з питань захисту конфіденційної інформації проводиться диференційовано, за категоріями посадових осіб - для керівників підрозділів, їх заступників, працівників підприємства. При виборі форм і методів навчання персоналу, враховують рівень професійної підготовленості співробітника, стаж роботи за конкретною спеціальністю, специфіку розв'язуваних їм завдань щодо захисту конфіденційної інформації, результати контролю діяльності співробітника з виконання встановлених вимог щодо захисту інформації на підприємстві.

Метод інструктажів застосовується керівництвом підприємства і керівниками структурних підрозділів для інформування співробітників, що

працюють з цінною інформацією, про положення знову прийнятих (затверджених) нормативно-методичних документів, а також вимог вищих органів державної влади. Під час інструктажів особлива увага повинна приділятися аналізу практичної роботи щодо виключення появи каналів витоку відомостей конфіденційного характеру і щодо запобігання виникнення загроз захисту інформації.

Метод індивідуальної та виховної роботи полягає в систематичному і цілеспрямованому впливі на процес формування та розвитку особистості співробітника підприємства та найбільш повного використання його професійних можливостей і здібностей, ділових, моральних та інших позитивних якостей для забезпечення схоронності довірених по роботі відомостей конфіденційного характеру .

Мета перевірки рівня знань - за допомогою оцінки знання співробітниками підприємства положень нормативно-методичних та внутрішніх організаційно-розпорядчих документів визначити ступінь підготовленості кожного працівника до виконання практичних завдань із захисту інформації. Перевірка рівня знань проводиться як керівництвом підприємства, так і співробітниками служби безпеки, підрозділи охорони.

2.3.2 Мотивація співробітників, їх заохочення і покарання

Особливе місце у діяльності керівництва підприємства і керівників структурних підрозділів по роботі з персоналом займають методи мотивації співробітників, які спрямовані на ефективне та якісне виконання покладених на них завдань на тлі суворого дотримання норм і правил захисту конфіденційної інформації.

Мотивація дій співробітників підприємства є основою загальної організаторської та управлінської функції керівника. При відсутності мотивації управлінська робота втрачає всякий сенс. У найзагальнішому вигляді мотивація - це процес спонукання співробітника підприємства до діяльності в ім'я досягнення певних цілей за допомогою внутрішньоособистих

і зовнішніх факторів. В основі спонукання лежить сукупність потреб, інтересів, бажань, цільових установок, ціннісних орієнтації, очікувань співробітника.

Основними факторами, що обумовлюють результативність праці персоналу являються готовність, можливість та умови для результативної діяльності.

Готовність до сумлінного виконання посадових обов'язків визначається тим, наскільки працівник схильний їх виконувати. Вона ґрунтується на мотиваційних складових особистості співробітника, а саме: на рівні потреб і інтересів; цільових установках; ціннісних орієнтаціях; бажання; задоволеності роботою; очікуванні винагороди залежно від результатів праці.

Відгуки всього одного співробітника можуть добре позначитися як на мотивації інших співробітників, так і на підвищенні якості роботи в цілому. Наприклад, працівнику після вправно виконаної роботи організовують відпустку, після повернення він ділиться враженнями і цим самим передає позитивні емоції іншим, а також стимул для вправної роботи.

Можливості співробітника, що дозволяють йому результативно виконувати його посадові обов'язки і поставлені завдання, визначаються як потенціал або сукупність його фізіологічних, інтелектуальних і професійних здібностей.

Потенціал співробітника залежить від рівня його знань, освіти, кваліфікації, вікових даних, стану здоров'я, витривалості, енергії і т.ін.

Умови являють собою сукупність зовнішніх стимулюючих факторів, що впливають на результативність праці персоналу і знаходяться поза його прямого контролю.

Виділяють три основні групи методів мотивації:

- методи безпосередньої мотивації праці;
- методи владної, примусової мотивації;
- методи стимулювання праці (морального, матеріального, трудового).

Методи безпосередньої мотивації праці характеризуються прямим впливом на особистість співробітника. До цієї групи належать методи переконання, навіювання та агітації.

Методи владної, примусової мотивації засновані на реальному примусі або потенційної можливості застосувати примус: виконання вказівок, наказів, розпоряджень та інших директивних рішень.

Методи стимулювання праці спрямовані на створення такої ситуації, яка спонукає співробітника діяти певним чином.

Моральне стимулювання – направлено на задоволення потреб співробітника в повазі і визнання з боку колективу, до найбільш поширених методів морального стимулювання відносяться заохочення, нагородження медалями, почесними знаками, присвоєння почесних звань;

Матеріальне стимулювання – спрямовано на підвищення рівня добробуту персоналу, реалізується в грошовій формі (виплата премій, різних надбавок, підвищення заробітної плати, залучення до участі в прибутках) і негрошовій формі (виділення путівок на відпочинок, надання житла, поїздки за місто і кемпінгові намети);

Трудове стимулювання – направлено на задоволення потреб співробітника в самовираженні і полягає в наданні йому можливості службового зростання, а також переведення (призначення) на посади, які більше відповідають його реальним можливостям, здібностям і інтересам.

Для підвищення ефективності праці персоналу, допущеного до конфіденційної інформації, необхідно комплексне використання перерахованих методів і засобів мотивації.

2.3.3 Контрольні заходи у роботі з персоналом

Метод контролю у роботі з персоналом підприємства має на меті оцінити ефективність роботи кожного співробітника підприємства по забезпеченню захисту конфіденційної інформації, використання сукупності

сил і засобів підприємства. Контроль може бути періодичним (плановим) і раптовим.

Проводиться співробітниками штатних підрозділів підприємства, що вирішують завдання з організації захисту інформації.

Основними формами контролю якості роботи персоналу підприємства, підвищення професіоналізму співробітників в області захисту конфіденційної інформації є:

- перевірки керівництвом підприємства або службою безпеки дотримання співробітниками положень нормативно-методичних документів по захисту інформації;
- звіти та доповіді керівників структурних підрозділів про результати роботи підлеглих співробітників;
- періодична атестація співробітників, допущених до конфіденційної інформації;
- самоконтроль співробітників.

Регулярні перевірки виконання співробітниками правил роботи з конфіденційною інформацією, документами і базами даних проводяться керівниками структурних підрозділів та напрямків діяльності підприємства, працівниками служби безпеки. Одночасно з дотриманням співробітником правил роботи з конфіденційними документами перевіряється наявність у цього співробітника зазначених за ним документів, носіїв інформації, справ, магнітних носіїв інформації; електронних масивів інформації, виробів та інших елементів, що складають таємницю підприємства. Перевірки можуть бути плановими та раптовими. Раптові перевірки проводяться при виникненні найменшої підозри про розголошення або витоку інформації.

Самоконтроль співробітників фірми полягає в перевірці самими керівниками і виконавцями повноти і правильності виконання ними діючих інструктивних положень, а також негайного інформування безпосереднього керівника і службу безпеки про факти втрати документів, втрати з якої-небудь причини цінної інформації, розголошення особисто або іншими

співробітниками відомостей, становлять таємницю фірми, порушення співробітниками порядку захисту інформації.

2.3.4 Атестація співробітників

Атестація співробітників представляється однією з найбільш ефективних форм контролю їх діяльності як у професійній сфері, так і у сфері дотримання інформаційної безпеки підприємства. Атестація персоналу - це колективна форма оцінки професійної придатності працівника, його відповідності займаній посаді. Атестація проводиться періодично: щокварталу, раз на рік та в інші терміни.

При проведенні атестації розглядаються наступні характеристики співробітника: трудова дисципліна, старанність, працьовитість, відповідальність, вимогливість і принциповість, організованість в роботі, якість і ефективність виконуваної роботи, самостійність і ініціатива, творча діяльність, прогресивність професійних рішень, професійний кругозір, вміння спілкуватися з людьми, організаторські здібності, відданість справі підприємства. У частині дотримання працівником вимог захисту інформації розглядаються такі характеристики, як знання нормативних та інструктивних документів щодо захисту інформації, вміння застосовувати вимоги цих документів у практичній діяльності, відсутність порушень у роботі з конфіденційними документами, вміння спілкуватися із сторонніми особами, не розкриваючи секрети підприємства, і т.ін. На основі вивчення цих характеристик формується уявлення про кожного співробітника, його ділових і людських якостях.

За результатами атестації видається наказ (розпорядження), в якому відображаються рішення атестаційної комісії про заохочення, переатестацію, підвищення на посаді або звільнення співробітників. Атестаційна комісія може також виносити рішення про відсторонення працівника від роботи з інформацією та документами, які складають таємницю підприємства.

2.3.5 Поліпшення психологічного клімату в колективі

Здоровий психологічний клімат у колективі підприємства створює важко переборний бар'єр на шляху будь-якого зловмисника, який намагається отримати конфіденційні відомості.

Для співробітника підприємства часто важливим являється не стільки оклад, який він отримує, скільки та доброзичлива обстановка, яка існує в колективі, впевненість в тому, що його поважають як фахівця, цінують його наполегливу працю і він може сподіватися на просування по службі. При формуванні здорового психологічного клімату вирішуються такі завдання:

- створення дієвої системи стимулювання праці персоналу;
- забезпечення довгострокової роботи на підприємстві кожного співробітника;
- формування ставлення до співробітників, як самостійним членам колективу, участь персоналу у виробленні рішень;
- справедливе участь персоналу в прибутках фірми;
- реалізація на практиці гнучкою, нетравматичної системи звільнень;
- розстановка кадрів відповідно до їх здібностей;
- верховенство у відносинах керівництва і співробітників духу колективізму.

При хорошому психологічному кліматі співробітники, доброзичливо ставляться до будь-яких обмежень, пов'язаних з функціонуванням системи захисту інформації, добровільно, з розумінням важливості виконують всі вимоги цієї системи.

Здоровий психологічний клімат має включати в себе наступні основні елементи:

- постійне вивчення і аналіз комплексу якостей кожного співробітника фірми, тобто знання кожного співробітника окремо, а не абстрактна виховна робота з колективом;
- суворе виконання пунктів і положень колективного договору;

- створення реальних умов для просування співробітників по службі або підвищення окладу з урахуванням їх трудових досягнень, а не з інших причин;
- оплата підприємством навчання або перепідготовка здатних і цінних для фірми співробітників;
- суворе виконання адміністрацією норм з техніки безпеки і охорони праці, створення найкращих умов для роботи співробітників та їх відпочинку;
- організація сприятливих умов для проведення відпусток і вихідних днів співробітників;
- своєчасне виявлення неформальних лідерів у колективі, висування їх на керівні посади або переведення в інші підрозділи. При виявленні їх негативний вплив на колектив - звільнення;
- охорона персоналу, гарантія юридичної та фізичного захисту у разі спроб кримінальних дій зловмисника по відношенню до них, їх родичам і близьким людям.

2.4 Порядок звільнення співробітників

У роботі з працівниками підприємства, допущеними до конфіденційної інформації, особливе місце займає етап їх звільнення (переведення на посади, не пов'язані з конфіденційною інформацією). Після прийняття керівництвом підприємства рішення про звільнення співробітника, допущеного до конфіденційної інформації, або про переведення його на посаду, не пов'язану з доступом до такого виду інформації, службою безпеки підприємства необхідно провести ряд заходів, спрямованих на запобігання можливого розголошення співробітником, що звільняється, цінної інформації про діяльність підприємства.

Алгоритм звільнення співробітника, робота якого пов’язана з конфіденційною інформацією зображено на рисунку 2.3. Він включає в себе наступні етапи:

- написання працівником заяви про звільнення з докладним розкриттям причини звільнення і бажано зазначенням місця передбачуваної роботи;
- передача заяви керівнику структурного підрозділу для оформлення і передачі до відділу кадрів;
- прийом службою від співробітника, що звільняється конфіденційної документації та всіх зазначених за ним документів, баз даних, носіїв інформації, виробів, матеріалів, з якими він працював, перевірка їх комплектності, повноти та оформлення їх прийому актом;
- здача співробітником пропуску для входу в робочу зону, всіх ключів і печаток, заборона співробітнику входити в робоче приміщення;
- проведення співробітником служби безпеки або служби персоналу бесіди із співробітником, що звільняється, з метою нагадування йому про зобов'язання збереження в таємниці тих відомостей, які йому були довірені по роботі на підприємстві, попередження співробітника про заборону використання цих відомостей в інтересах конкурента або в особистих цілях;
- підписання співробітником зобов'язання про нерозголошення їм конфіденційних відомостей після звільнення;
- документальне оформлення звільнення відповідно до загальних правил;
- прийом від співробітника пропуску для входу в будівлю підприємства, видача йому трудової книжки і розрахунку по заробітній платі.

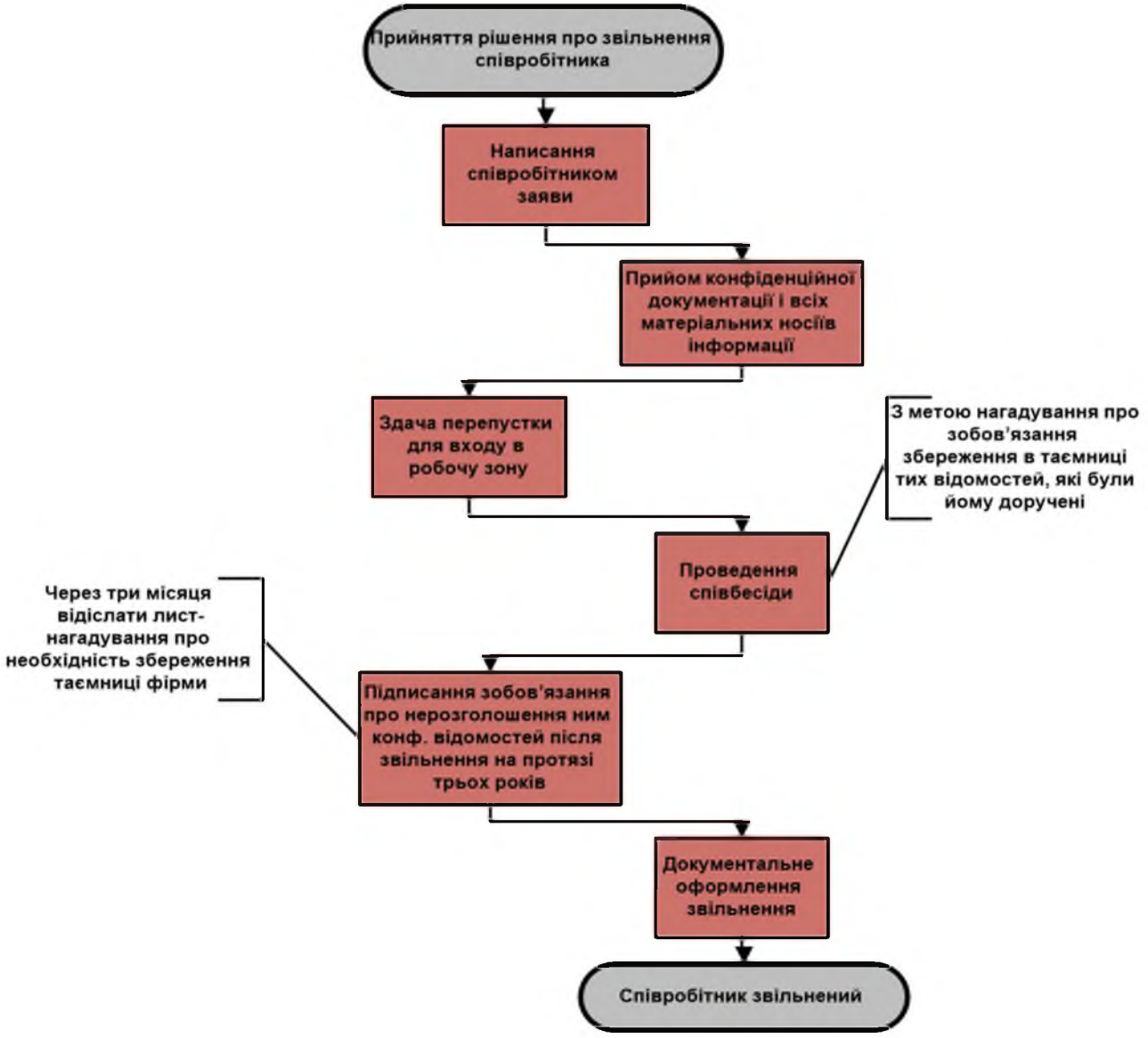


Рисунок 2.3 – Алгоритм звільнення співробітника, який має доступ до конфіденційної інформації

Основою проведення даних заходів є прийняття від співробітника, що звільняється, письмових зобов'язань про нерозголошення, що стали йому відомі в період роботи на підприємстві (в конкретній посаді) відомостей, що містять конфіденційну інформацію.

Ці зобов'язання повинні бути оформленими у вигляді розписки, яка після її оформлення залишається на підприємстві. У розписці вказуються прізвище, ім'я, по батькові співробітника і найменування останньої посади; перераховуються відомості конфіденційного характеру, заборонені до

розголошення протягом певного терміну, або наводиться посилання на пункти переліку відомостей, що містять конфіденційну інформацію.

Згода працівника з умовами нерозголошення перерахованих в розписці відомостей підтверджується підписом співробітника із зазначенням дати.

Оформлення розписки здійснюється в ході бесіди зі співробітником підприємства представника служби безпеки. Після оформлення розписки проводиться інструктаж із співробітником, що звільняється, про правила його поведінки після звільнення (переведення на іншу роботу) і про недопущення згадки цінних відомостей в ході спілкування з представниками організацій, що є конкурентами даного підприємства, родичам або випадковим знайомим.

Збиток від звільнення співробітника різко зменшується, якщо таємниця підприємства роздроблена і відома по частинам досить великому числу службовців. У цьому випадку не доводиться вдаватися до зазначених вище складних і часто мало ефективних способів захисту таємниці, відомої звільненим співробітникам.

У будь-якому випадку рекомендується після закінчення трьох місяців після звільнення направити колишньому співробітнику лист-нагадування про необхідність збереження таємниці підприємства.

Якщо керівництву фірми стали відомі випадки несанкціонованого використання колишнім співробітником конфіденційних відомостей підприємства, слід почати активну судовий розгляд виявлених фактів.

Розглянутий процес оформлення звільнення співробітників, які мають доступ до конфіденційної інформації, дозволить не тільки підвищити відповідальність усього персоналу за збереження довірених їм відомостей, але й запобігти факти крадіжки співробітниками, що звільняються, цінної інформації, обмежити можливість використання її в інших організаціях і фірмах.

2.5 Висновок

У спеціальній частині кваліфікаційної роботи були досліджені існуючі загрози витоку конфіденційної інформації, а також детально визначені

загрози, які пов’язані з витоком конфіденційної інформації з вини персоналу. На основі проведених аналізів були розроблені алгоритми, головна мета яких є запобігання витоку інформації з вини персоналу агентства нерухомості «Резидент» на усіх етапах роботи з персоналом, починаючи з прийому і закінчуючи звільненням. Розроблені алгоритми можуть бути застосовані і на інших комерційних підприємствах, де циркулює інформація з обмеженим доступом і відсутня інформація, що становить державну таємницю. Заключним етапом є впровадження створених алгоритмів на підприємство та здійснення перевірки їх подальшого функціонування.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Завданням даної роботи є підвищення безпеки підприємства за рахунок впровадження розробленого алгоритму запобіганню витоку конфіденційної інформації з вини персоналу. У даному розділі були виконані наступні розрахунки:

1) розрахунок капітальних витрат;
2) розрахунок поточних витрат;
3) визначена величина можливого збитку;
4) визначені та проаналізовані показники економічної ефективності системи інформаційної безпеки.

На підставі отриманих результатів було зроблено висновок щодо економічної ефективності створення цього алгоритму.

3.1 Визначення трудомісткості розробки алгоритму

Трудомісткість створення алгоритму визначається тривалістю кожної робочої операції, починаючи зі складання технічного завдання і закінчуючи оформленням документації.

$$t = tтз + tв + ta + tпр + tопр + tд, год.$$

Де tтз = 14 год. – тривалість складання технічного завдання на розробку алгоритму;

tв = 3 год. – тривалість вивчення технічного завдання, літературних джерел за темою тощо;

ta = 4 год. – тривалість розробки блок-схеми алгоритму;

tпр = 3 год. – тривалість програмування за готовою блок-схемою;

tопр = 16 год. – тривалість опрацювання алгоритму;

tд = 6 год. – тривалість підготовки технічної документації.

t = 14 год. + 3 год. + 4 год. + 3 год. + 16 год. + 6 год. = 46 год.

3.2 Розрахунок витрат на створення алгоритму

Витрати на створення алгоритму Крп складаються з витрат на заробітну плату виконавця розробки Ззп і вартості витрат машинного часу, що необхідний для опрацювання алгоритму на ПК Змч:

$$Крп = Ззп + Змч,$$

де Крп – витрати на створення алгоритму;

Ззп – заробітна плата спеціаліста з інформаційної безпеки;

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

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

$$Ззп = t * Зіб = 46 * 125 = 5750 \text{ грн.}$$

де t – загальна тривалість розробки алгоритму, год.;

Зіб – середньогодинна заробітна плата спеціаліста з інформаційної безпеки становить 125 грн/год.

Вартість машинного часу для розробки алгоритму на ПК визначається за формулою:

$$Змч = t * Смч, \text{грн.}$$

де t – трудомісткість розробки алгоритму на ПК, год.;

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

Вартість 1 години машинного часу ПК визначається за формулою:

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

$$= 0{,}4 * 1 * 1{,}68 + \frac{(4000 * 0{,}5)}{1920} + \frac{4500 * 0{,}5}{1920} =$$

$$= 0{,}67 + 1{,}04 + 1{,}17 = 2{,}88 \text{ грн/год,}$$

Де Р- встановлена потужність апаратури інформаційної безпеки, 0,4 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, 4000 грн.;

На – річна норма амортизації на ПК, 0.5 частки одиниці;

Напз – річна норма амортизації на ліцензійне програмне забезпечення, 0,5 частки одиниці;

Клпз – вартість ліцензійного програмного забезпечення, 4500 грн.;

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

$$Змч = t * Смч = 46 * 2{,}88 = 132{,}48 \text{ грн.}$$

Визначена таким чином вартість створення алгоритму Крп є частиною одноразових капітальних витрат разом з витратами на придбання і налагодження апаратури системи інформаційної безпеки.

$$Крп = Ззп + Змч = 5750 + 132{,}48 = 5882{,}48 \text{ грн.}$$

3.3 Розрахунок (фіксованих) капітальних витрат

Капітальні (фіксовані) витрати на проєктування та впровадження проєктного варіанта системи інформаційної безпеки складають:

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

де Кпр – вартість розробки проєкту інформаційної безпеки та залучення для цього зовнішніх консультантів, 28000 грн.;

Кзпз – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), 115000 грн.;

Крп – вартість розробки політики безпеки інформації, 5882,48 грн.;

Каз – вартість закупівель апаратного забезпечення та допоміжних матеріалів відсутня, 28000 грн.;

Кнавч - витрати на навчання технічних фахівців і обслуговуючого персоналу, 32000 грн.;

Кн – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, 32000 грн.

Відповідно до заданих даних розраховуємо капітальні витрати

$$К = Кпр + Кзпз + Крп + Каз + Кнавч + Кн =$$
$$= 28000 + 115500 + 5882{,}48 + 28000 + 32000 + 32000 = 241382{,}48 \text{ грн.}$$

3.4 Розрахунок поточних (експлуатаційних) витрат

Поточні витрати включають:

- 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:

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

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

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 (0,4 кВт*24 комп'ютери = 9,6 кВт)

Fр = 12 міс * 20 робочих діб/міс * 8 робочих годин * 24 комп'ютери = 46080 год – річний фонд робочого часу системи інформаційної безпеки;

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

$$Се = 9,6 * 46080 * 1,68 = 743178,24 \text{ грн.}$$

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

$$Стос = К * 0,02 = 35382,48 * 0,02 = 707,65 \text{ грн.}$$

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

$$С = Со + Сз + Се + Стос =$$
$$= 15000 + 30000 + 743178,24 + 707,65 = 788885,89 \text{ грн.}$$

3.5 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
Директор	25000	1	25000
Заступник директора	20000	1	20000
Секретар	15000	1	15000
Менеджер з реклами	15000	1	15000
Менеджер по роботі з клієнтам (ріелтор)	15000	15	225000
Менеджер по роботі з персоналом	15000	1	15000
Головний бухгалтер	20000	1	20000
Юрист	20000	1	20000
Системний адміністратор	20000	1	20000
Охоронець	10000	6	60000
Прибиральниця	8000	1	8000
		Сума	443000

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

$$Пп = \left(\frac{Зс}{Fр}\right) * tв = \left(\frac{443000}{160}\right) * 4 = 11075 \text{ грн.}$$

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.:

$$Пви = (443000/160) * 8 = 22150 \text{ грн.}$$

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

$$Ппв = (20000/125) * 4 = 640 \text{ грн.}$$

Витрати на відновлення працездатності системи:

$$Пв = Пви + Ппв + Пзч = 22150 + 640 + 5000 = 27790 \text{ грн.}$$

Пзч = 5000 грн. - вартість для витрат на заміну частин;

О = 15000000 грн. - обсяг чистого прибутку за рік.

Втрати від зниження працездатності атакованої системи:

$$V = \frac{О}{Fр} * (tп + tв + tви) = \frac{15000000}{1920} * (3 + 4 + 8) = 117187{,}5 \text{ грн.}$$

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 інформаційну систему при реалізації загрози складе:

$$U = Пп + Пв + V = 11075 + 27790 + 117187{,}5 = 156052{,}5 \text{ грн.}$$

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

$$В = \sum_{i}\sum_{n} * U = 24 * 4 * 156052{,}5 = 14981040 \text{ грн.}$$

де: i- число атакованих вузлів, 24 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:

$$E = B * R - C = 14981040 * 0{,}25 - 788885{,}89 = 2956374{,}11 \text{ грн.}$$

Визначення та аналіз показників економічної ефективності системи інформаційної безпеки:

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині кваліфікаційної роботи, 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 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.

$$ROSI = E/K = 2956374{,}11 / 241382{,}48 = 12{,}25$$

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

$$To = K/E = 1/ROSI = 1 / 12{,}25 = 0{,}08 \text{ років} = 1 \text{ місяць.}$$

3.6 Висновок

У даному розділі були проведені розрахунки витрат на проєкт системи захисту інформації. Також була визначена економічна ефективність розробки і впровадження алгоритму запобіганню витоку конфіденційної інформації з вини персоналу на розглянуте в даній кваліфікаційній роботі підприємство АН «Резидент». Відповідно до розрахунків, виконаних в даному розділі, проєкт системи інформаційної безпеки є доцільним і економічно вигідним. Термін окупності капітальних інвестицій складає один місяць. Тому можна зробити висновок, що розглянуті переваги є основною економічною ефективністю розробки та показують необхідність застосування на практиці.

ВИСНОВКИ

Практично будь-яка діяльність в нинішньому суспільстві тісно пов'язана з отриманням, накопиченням, зберіганням, обробкою і використанням різноманітних інформаційних потоків. У зв'язку з цим виникає маса проблем, пов'язаних із забезпеченням збереження конфіденційної інформації.

В умовах ринку і конкуренції конфіденційна інформація різних комерційних організацій виступає, як спосіб збільшення прибутку підприємства або як спосіб нанесення шкоди конкурентам. Витік комерційних секретів може призвести до зниження доходів підприємства або його банкрутства.

У процесі виконання даної кваліфікаційної роботи, були вирішені поставлені задачі і винесені відповідні висновки. У розглянутому в даній роботі агентстві нерухомості «Резидент» цінність представляє інформація, що містить відомості, які не відносяться до державної таємниці і становлять інтелектуальну власність фізичної особи. У процесі даного дослідження була проаналізована система захисту інформаційних потоків підприємства. Основну загрозу інформаційній безпеці становить незаконний доступ конкурентів до конфіденційної інформації та використання її для нанесення шкоди підприємству.

Для врегулювання процесів забезпечення безпеки інформації, і головним чином при роботі персоналу з конфіденційною інформацією, документами, договорами і базами даних був розроблений алгоритм системи захисту конфіденційної інформації підприємства при роботі з персоналом, який встановлює принципи та способи запобігання витоку цінної інформації, який можуть виникнути з вини персоналу.

Таким чином, в роботі досліджені та проаналізовані сучасні вимоги до організації захисту конфіденційної інформації при роботі з персоналом. На основі аналізу теоретичного матеріалу був розроблений алгоритм, що дозволяє запобігти витоку конфіденційної інформації з вини персоналу.

В економічному розділі було виконано розрахунок капітальних та експлуатаційних витрат на створення та підтримку розробленого алгоритму. На підставі отриманих розрахунків, був зроблений аналіз економічної ефективності впровадження розробки на підприємство.

Поставлені в роботі завдання можна вважати досягнутими.

ПЕРЕЛІК ПОСИЛАНЬ

1 Національна електронна бібліотека (Електрон. ресурс) / Спосіб доступу: URL: http://padonak.biz/gos/41.html.- Назва з екрана.

2 Національна електронна бібліотека (Електрон. ресурс) / Спосіб доступу: URL: http://all-ib.ru/content/index_info.- Назва з екрана.

3 НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

4 Національна електронна бібліотека (Електрон. ресурс) / Спосіб доступу: URL: http://hack-expo.void.ru/groups/suz/html/7.htm.- Назва з екрана.

5 Національна електронна бібліотека (Електрон. ресурс) / Спосіб доступу: URL: http://www.vuzlib.net/beta3/html/1/13257/13348/.-Назва з екрана.

6 Національна електронна бібліотека (Електрон. ресурс) / Спосіб доступу: URL: http://zakon.rada.gov.ua /.-Назва з екрана.

7 Wozencraft J. M. and Jacobs I. M. Principles of Communication Engineering. John Wiley &. Sons, Inc.. New York. 2001.

8 Національна електронна бібліотека (Електрон. ресурс) / Спосіб доступу: URL: http://sevendays.com.ua//informacionnaja_predprijatija.html.- Назва з екрана.

9 Національна електронна бібліотека (Електрон. ресурс) / Спосіб доступу: URL: http://www.warning.dp.ua/comp7.htm.-Назва з екрана.

10 Національна електронна бібліотека (Електрон. ресурс) / Спосіб доступу: URL: http://www.bre.ru/security/20864.html.-Назва з екрана.

11 Національна електронна бібліотека (Електрон. ресурс) / Спосіб доступу: URL: http://www.elitarium.ru/2007/11/14/klimat_v_kollektive.html.- Назва з екрана.

12 Національна електронна бібліотека (Електрон. ресурс) / Спосіб доступу: URL: http://www.ua.all.biz/buy/service/?group=13189.-Назва з екрана.

13 Національна електронна бібліотека (Електрон. ресурс) / Спосіб доступу: URL: http://www.infopulse.com.ua/rus/about/qms/qms-development-ISMS.-Назва з екрана.

14 Національна електронна бібліотека (Електрон. ресурс) / Спосіб доступу: URL: http://www.superjob.ru/community/security/11694/.-Назва з екрана.

15 Національна електронна бібліотека (Електрон. ресурс) / Спосіб доступу: URL: http://www.hrliga.com/index.php=profession&op=545&print=true.-Назва з екрана.

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	1	
4	А4	Вступ	2	
5	А4	Розділ 1	14	
6	А4	Розділ 2	28	
7	А4	Розділ 3	10	
8	А4	Висновки	2	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	2	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Ґ	2	

ДОДАТОК Б. Класифікація інформаційних об’єктів

1. За доступністю або наявності:

Д5 – критична інформація (робота суб'єкта буде зупинена);

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 викоривувана, що не впливає на роботу суб'єктів інформація);

Д0 – шкідлива інформація (наявність такої інформації вимагає обробки, а обробка веде до перевитрат ресурсів).1. По доступності або наявності:

2. За несанкціонованої модифікації або цілісності:

Ц4 – критична інформація (несанкціонована зміна призведе до неправильної роботи всього підприємства або значної його частини; наслідки такої модифікації незворотні);

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

Ц2 – важлива інформація (несанкціонована зміна призводить до неправильної роботи підприємства через деякий час, якщо не будуть зроблені деякі дії; наслідки такої модифікації зворотні);

Ц1 – значуща інформація (несанкціонована зміна позначиться через деякий час, але не призведе до збою в системі; наслідки такої модифікації зворотні);

Ц0 – незначна інформація (несанкціонована зміна не позначиться на роботі системи).

3. За розголошенням чи конфіденційністю:

К5 – критична інформація (розголошення інформації призведе до краху підприємства або дуже значних матеріальних втрат);

К4 – дуже важлива інформація (розголошення призведе до значних матеріальних втрат, якщо не будуть прийняті певні 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 рідких випадках);

К0 – незначна інформація (не впливає на роботу суб'єкта).

ДОДАТОК В. Перелік документів на оптичному носії

1 Презентація_Зуй.ppt

2 Кваліфікаційна робота_Зуй.doc

ДОДАТОК Г. Відгук керівника економічного розділу

Керівник розділу _____ _____

(підпис) (прізвище, ініціали)

ДОДАТОК Ґ. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125м-22-2 Зуя О.В.

на тему: «Розробка алгоритму запобіганню витоку інформації на підприємстві з вини персоналу»

Пояснювальна записка: 71 с., 5 рис., 3 табл., 5 додатків, 15 джерел.

Об'єктом дослідження кваліфікаційної роботи є алгоритм запобіганню витоку інформації.

Мета кваліфікаційної роботи: забезпечення підвищення рівня безпеки підприємства на основі впровадження розробленого алгоритму запобіганню витоку конфіденційної інформації з вини персоналу.

У роботі наведено аналіз можливих загроз витоку конфіденційної інформації з вини персоналу; розроблено алгоритм основних дій при роботі з персоналом, який має доступ до конфіденційної інформації підприємства.

В економічному розділі виконано розрахунок витрат на розробку і впровадження алгоритму на підприємстві. Також зроблений висновок щодо економічної ефективності впровадження створеного алгоритму.

Практичне значення полягає у підвищенні рівня безпеки розглянутого підприємства за рахунок зменшення ризику витоку конфіденційної інформації з вини персоналу підприємства.

Наукова новизна полягає в удосконаленні процесу роботи з персоналом з метою забезпечення інформаційної безпеки на підприємстві.

До недоліків слід віднести недостатню обґрунтованість отриманих результатів та неточність окремих положень.

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

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

Керівник роботи,
к.т.н., доц. Мацюк С.М.