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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістр

студентки *Білової Юлії Олексіївни*

академічної групи *125м-21-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка моделі управління інформаційною безпекою готельного підприємства*

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

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістр

студенту ***Біловій Юлії Олексіївні*** **академічної групи** ***125м-21-1***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка моделі управління інформаційною безпекою готельного підприємства***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 31.10.22р. № 1200-с

Розділ	Зміст	Термін виконання
Розділ 1	Проаналізувати державні стандарти у сфері інформаційної безпеки України. Міжнародні стандарти управління ризиками інформаційної безпеки.	20.10.2022
Розділ 2	У спеціальній частині визначити найбільш небезпечні загрози які з'являються при функціонуванні підприємства та його ІС, де оброблюється конфіденційна інформація. Розробити типову модель управління інформаційною безпекою, для цього типу підприємства.	16.11.2022
Розділ 3	В економічному розділі виконати розрахунок витрат на проєктування та експлуатацію системи інформаційної безпеки.	05.12.2022

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 05.09.2022 р.

Дата подання до екзаменаційної комісії: 12.12.2022 р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 123 с., 13 рис., 27 табл., 4 додатка, 18 джерел.

Об’єкт дослідження: особливості управління інформаційною безпекою підприємств готельного бізнесу України.

Мета роботи: визначення особливостей аналізу та управління інформаційною безпекою підприємств готельного бізнесу України, дослідження існуючих методів та особливостей їх використання на практиці.

У роботі проаналізовано державні стандарти у сфері інформаційної безпеки України. Міжнародні стандарти управління ризиками інформаційної безпеки.

У спеціальній частині визначено найбільш небезпечних загроз які з’являються при функціонуванні підприємства та його ІС, де оброблюється конфіденційна інформація. Після аналізу була побудована типова модель загроз та модель порушника, для цього типу підприємства.

В економічному розділі проведено розрахунок витрат на проєктування та експлуатацію системи інформаційної безпеки.

Наукова новизна полягає у отримання моделі аналізу та управління інформаційною безпекою на підприємствах готельного бізнесу.

МОДЕЛЬ УПРАВЛІННЯ, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ТИПОВА МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ГОТЕЛЬ

ABSTRACT

Explanatory note: 123 p., 13 pic., 27 tabl., 4 app., 18 sources.

Object of study: features of information security management of hotel business enterprises in Ukraine.

Purpose: to determine the peculiarities of analysis and management of information security of hotel business enterprises in Ukraine, to study existing methods and features of their use in practice.

The work analyzes the state standards in the field of information security of Ukraine. International standards of information security risk management.

The special part identifies the most dangerous threats that appear in the functioning of the enterprise and its IS, where confidential information is processed. After the analysis, a typical threat model and an offender model were built for this type of enterprise.

In the economic section, the costs of designing and operating an information security system were calculated.

The scientific novelty is to obtain a method of analysis and management of information security in the hotel business.

MANAGEMENT MODEL, INFORMATION SECURITY MANAGEMENT, TYPICAL THREAT MODEL, OFFENDER MODEL, HOTEL

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ВВБ – високий вплив на бізнес;

ДСТУ – Державний стандарт України;

ЗБД – загроза безпеки даних;

ІБ – інформаційна безпека;

ІС – інформаційна система;

ІТ – інформаційні технології;

КЗЗ- комплекс запобіжних заходів;

КС- комп'ютерна система;

МПБ- мандатна політика безпеки;

НСД – несанкціонований доступ;

ОІБ- основи інформаційної безпеки;

ОРаЗ – очікуваний разовий збиток;

ОРіЗ – очікуваний річний збиток;

ОС – операційна система;

ПБ – політика безпеки;

ПД – персональні дані;

ПЗ – програмне забезпечення;

РПБ- рольова політика безпеки;

СЗІ – система захисту інформації;

СКБД- система керування баз даних;

СУІБ – система управління інформаційною безпекою;

ТЗІ – технічний захист інформації;

ЩЧВ – щорічна частота виникнення;

ITIL – Information Technology Infrastructure Library;

MMS – Military Message System;

NPV – Net Present Value;

SMF – Service Management Function.

ЗМІСТ

с.

ВСТУП

Бурхливий розвиток підприємств готельного бізнесу в Україні, вимагає від них для задоволення вимог клієнтів, постійно розвивати свої служби. Одним з важливих підрозділів готельного бізнесу є обслуговування абонентів, які виступають в якості провідника між готелем, його послугами та клієнтами. В кожному готелі, які надають свої послуги є власні ЦОА.

З урахуванням особливостей ведення бізнесу в Україні, в готелях постійно виникають загрози інформаційної безпеки, які можуть суттєво вплинути на бізнес компанії, як великої так і незначної за розмірами. Інформація, яка оброблюється в ІС, потребує значного рівня захищеності, тому що містить персональні дані клієнтів, як фізичних так і юридичних осіб. Для забезпечення достатнього рівня захисту потрібно не реагувати на виникаючи інциденти, а запобігати їм. Тобто потрібно діяти продуктивно. Можливість спрогнозувати загрози ІБ та своєчасно запобігти виникнення порушень безпеки, надається велике значення.

Існує багато різноманітних методик управління інформаційною безпекою, які базуються на різних підходах. Кожний з цих підходів має свої переваги та недоліки, але всі вони дозволяють в тій чи інший мірі визначити рівень захищеності циркулюючої інформації.

В роботі буде розглянуто основні особливості функціонування підприємств готельного бізнесу, загрози які притаманні організаціям цього типу. Будуть розглянуті декілька методик управління інформаційною безпекою, з метою вибору найбільш оптимальної методики для впровадження на підприємстві.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

1.1.1 Актуальність питання управління інформаційною безпекою на підприємствах готельного бізнесу

Більшість організацій усвідомлює, наскільки висока роль IT в досягненні поставлених бізнес-цілей. Однак сучасні IT-інфраструктури тісно пов'язані між собою і працюють в середовищі з постійно зростаючим рівнем небезпеки, що характеризується безперервним збільшенням частоти атак і постійного посилення щодо вимог до часу реакції. Найчастіше організації нездатні реагувати на нову загрозу безпеці раніше, ніж вона вплине на їх бізнес. Управління безпекою інфраструктури організації (і створюваної завдяки цій інфраструктурі бізнес-цінності) стало одним з головних завдань IT-підрозділів.

Крім того, нові закони, пов'язані з корпоративним управлінням, зберігання конфіденційності та виконання фінансових зобов'язань, примушують організації приділяти більше уваги управлінню IT-інфраструктурами і підвищувати ефективність управління. Формальний процес управління інформаційною безпекою дозволяє готелям домогтися поєднання максимальної економічної ефективності з відомим і прийнятним рівнем бізнес-ризику і надає користувачам зрозумілий і не суперечливий метод організації та пріоритизації обмежених ресурсів для реалізації управління ризиками. Реалізація управління інформаційною безпекою дозволяє організаціям запровадити економічно ефективний контроль, що знижує ризик до прийнятного рівня.

Визначення прийнятного ризику і підхід до управління інформаційною безпекою залежать від конкретної організації, оскільки не існує універсального рішення, а різні організації використовують різні моделі управління ризиками. Кожна модель пропонує власне поєднання точності, ресурсів, часу, складності та суб'єктивності. Інвестиції в процес управління ризиками, заснований на перевіреній концепції і чіткому визначенні ролей та обов'язків, готують організацію до визначення пріоритетів, планування нейтралізації загроз та

зв'язку загроз та вразливостей з бізнесом. Крім того, ефективна програма управління ризиками допоможе компанії забезпечити дотримання законодавчих вимог, які постійно посилюються. Потрібен системний підхід до менеджменту ризиків інформаційної безпеки, щоб ідентифікувати організаційні потреби щодо відповідності вимогам інформаційної безпеки та створити ефективну систему менеджменту інформаційної безпеки. Цей підхід повинен бути виправданим для середовища організації і, зокрема, повинен бути урівноваженим підходом повного менеджменту ризиків підприємства. Всі зусилля з безпеки повинні ефективним і своєчасним способом звернутися до ризиків, де і коли вони необхідні.

В даний час готельна індустрія являє собою галузь з дуже високим рівнем конкуренції. Будь-який сучасний готель - це складний комплекс функціональних ланок. Від злагодженості роботи цього комплексу залежить успішність існування підприємства на ринку. При зростанні обсягу продажів, з одного боку, і зростаючої конкуренції, з іншого, підвищується значення оперативності в роботі персоналу. Гостро постає необхідність автоматизації більшості робочих місць готельного персоналу. Вирішенням цієї проблеми може стати комплексна автоматизація готельного комплексу, що досягається застосуванням автоматизованих систем управління (АСУ). У зв'язку з вищевикладеним метою роботи є створення ефективної моделі безпеки подібної системи.

Розробка моделі. Основною функцією таких систем автоматизації готелів є подання стану номерного фонду, інформація про занятість кожного конкретного номера, що дозволяє здійснювати планування продажу номерів в майбутньому(Бронювання) і поточний контроль діяльності засобів розміщення. Крім іншого, необхідно позбутися від паперової тяганини і виключити або максимально зменшити можливість помилок, в результаті дії так званого людського фактора, що є причиною додаткових незручностей і матеріальних витрат. Така система управління, по можливості, повинна забезпечувати інтелектуальну обробку даних. Завданням будь якої АСУ виступають ефективне зберігання, обробка та аналіз даних. Дані в систему можуть заноситися як

вручну, так і автоматично. При цьому інформаційно-аналітична система середнього та великого підприємства або організації повинна забезпечувати користувачам доступ до аналітичної інформації, захищеної від несанкціонованого використання. Захист даних від несанкціонованого доступу є одним із пріоритетних завдань при проєктуванні будь-якої інформаційної системи.

При розробці моделі безпеки інформаційної системи необхідно враховувати такі основні аспекти інформаційної безпеки, як конфіденційність, цілісність і доступність. Розробка складних, розподілених інформаційних систем тягне за собою необхідність враховувати ряд специфічних вимог щодо забезпечення безпеки функціонування. Зокрема, архітектура системи повинна бути достатньо гнучкою і допускати відносно простий розвиток конфігурації використовуваних засобів і нарощування функцій і ресурсів інформаційної системи. При цьому необхідно забезпечувати безпеку функціонування системи при різних видах загроз, а також надійний захист даних від помилок проєктування, від руйнування або втрати інформації. Необхідно також пам'ятати і про користувачів. У процесі проєктування і розробки інформаційної системи необхідно забезпечити авторизацію користувачів простий та комфортний доступ до управління і як результат функціонування інформаційної системи, наглядний інтерфейс[1]. Структура моделі безпеки повинна надавати наступний базовий функціонал:

- перевірка прав доступу користувачів до конкретних об'єктів і на конкретні дії;

- ведення історії операцій з об'єктами: додавання, зміна, видалення;

- адміністративні операції: ведення списку користувачів, установка прав на об'єкти та групи об'єктів, установка дозволів для користувача профілів.

Наш підхід до побудови систем управління ІБ, включаючи розробку процесів забезпечення ІБ, базується на наступних методичних

рекомендаціях та директивах:

– рекомендації ITIL (Information Technology Infrastructure Library, кращий світовий досвід у сфері організації роботи IT-служби), а також моделі управління IT-ресурсами та IT-сервісами Microsoft Operations Framework (MOF);

– рекомендації Microsoft service management function (SMF).

Доцільність використання рекомендацій з управління IT-ресурсами та IT-послугами (і в першу чергу процесів управління інцидентами, змінами) при побудові СУІБ обумовлена тим , що процеси забезпечення інформаційної безпеки нерозривно пов'язані з процесами захисту, а значить, і управління інформаційними системами і повинні бути тісно інтегровані з процесами управління IT.

1.1.2 Визначення загроз інформаційній безпеці

Під загрозою (взагалі) зазвичай розуміють потенційно можливу подію, дію (вплив), процес або явище, яке може привести до нанесення шкоди будь-чиїм інтересам. Згідно з визначенням в законодавстві України, загроза — будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків ІС [2]. Надалі загрозою інформаційної безпеки ІС будемо називати можливість реалізації впливу на інформацію, оброблювану в ІС, що призводить до спотворення, знищення, копіювання, блокування доступу до інформації, а також можливість впливу на компоненти ІС, що призводить до втрати, знищення або збою функціонування носія інформації, засобу взаємодії з носієм або засоби його управління. В даний час розглядають досить великий перелік загроз інформаційної безпеки ІС, що нараховує сотні пунктів. Найбільш характерні і часто реалізуються з них перераховані нижче:

– несанкціоноване копіювання носіїв інформації;

– необережні дії, що призводять до розголошення конфіденційної інформації, або роблять її загальнодоступною;

– ігнорування організаційних обмежень (встановлених правил) при визначенні рангу системи.

Завдання можливих загроз інформаційної безпеки проводиться з метою визначення повного переліку вимог до розроблюваної системі захисту. Перелік загроз, оцінки ймовірності їх реалізації, а також модель порушника є основою для аналізу ризику реалізацій загроз і формулювання вимог до системи захисту ІС. Крім виявлення можливих загроз повинен бути проведений аналіз цих загроз на основі їх класифікації за низкою ознак. Кожна з ознак класифікації відображає одну з узагальнених вимог до системи захисту. При цьому – загрози, що відповідають кожній ознаці класифікації, дозволяють деталізувати вимогу, яка відображається цією ознакою.

Необхідність класифікації загроз інформаційної безпеки ІС обумовлена [2] тим, що архітектура сучасних засобів автоматизованої обробки інформації, організаційна, структурна і функціональна побудова інформаційно-обчислювальних систем і мереж, технології та умови автоматизованої обробки інформації такі, що накопичується, зберігається та обробляється інформація схильна випадковим впливам надзвичайно великого числа факторів, через що стає неможливим формалізувати задачу повного опису безлічі загроз. Як наслідок, для системи, яка підлягає захисту визначають не повний перелік загроз, а перелік класів загроз.

Класифікація всіх можливих загроз інформаційної безпеки ІС може бути проведена по ряду базових ознак.

Незалежно від конкретних видів загроз або їх проблемно-орієнтованої класифікації ІС задовольняє потреби організації, якщо забезпечуються наступні властивості інформації і систем її обробки.

Конфіденційність інформації – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом [2]. Або інакше це суб'єктивно визначена (приписувана) характеристика (властивість) інформації, яка вказує на необхідність введення обмежень на коло суб'єктів, що мають доступ до цієї інформації, і забезпечувана здатністю системи (середовища) зберігати вказану інформацію в таємниці від суб'єктів, які не мають повноважень доступу до неї. Об'єктивні передумови

подібного обмеження доступності інформації для одних суб'єктів укладені в необхідності захисту їх законних інтересів від інших суб'єктів інформаційних відносин.

Цілісність інформації – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом [3]. Інакше це можливо трактувати, як існування інформації в неспотвореному вигляді (незмінному по відношенню до деякого фіксованого її стану). Точніше кажучи, суб'єктів цікавить забезпечення більш широкої властивості достовірності інформації, яка складається з адекватності (повноти і точності) відображення стану предметної області і безпосередньо цілісності інформації, тобто те що вона неспотворена.

Доступність інформації – властивість, яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний [2]. Також це можливо розглянути, як властивість системи (середовища, засобів і технології обробки), в якій циркулює інформація, що характеризується здатністю забезпечувати своєчасний безперешкодний доступ суб'єктів до інформації, яка їх цікавить і готовність відповідних автоматизованих служб до обслуговування запитів, які надходять від суб'єктів, завжди, коли в них виникає необхідність. Таким чином, у відповідності з існуючими підходами, прийнято вважати, що інформаційна безпека ІС забезпечена у випадку, якщо для будь-яких інформаційних ресурсів у системі підтримується певний рівень конфіденційності (неможливості несанкціонованого отримання будь-якої інформації), цілісності (неможливості несанкціонованої або випадкової її модифікації) та доступності (можливості за розумний час отримати необхідну інформацію). Відповідно для інформаційних систем було запропоновано розглядати три основних типа загроз.

Загроза порушення конфіденційності полягає в тому, що інформація стає відомою тому, хто не має повноважень доступу до неї. У термінах комп'ютерної безпеки загроза порушення конфіденційності має місце кожного разу, коли отримано доступ до деякої секретної інформації, що зберігається в обчислювальній системі чи передається від однієї системи до іншої. Іноді, у зв'язку з загрозою порушення конфіденційності, використовується термін "витік". Загроза порушення цілісності включає в себе будь-яке навмисне змінення інформації, що зберігається в обчислювальній системі чи передається з однієї системи в іншу. Цілісність також буде порушена, якщо до несанкціонованого зміни призводить випадкова помилка програмного або апаратного забезпечення. Санкціонованими змінами є ті, які зроблені уповноваженими особами з обгрунтованою метою так кваліфікацією Загроза відмови служб виникає кожного разу, коли в результаті навмисних дій, що вживаються іншим користувачем або зловмисником, блокується доступ до деякого ресурсу обчислювальної системи. Реально блокування може бути постійним – запитуваний ресурс ніколи не буде отриманий, або воно може викликати тільки затримку запрошуваного ресурсу, достатньо довгу для того, щоб він став марним.

1.2 Система управління інформаційною безпекою. Основні типи інформаційних систем.

Вважається, що система управління ризиками організації повинна мінімізувати можливі негативні наслідки, пов'язані з використанням інформаційних технологій, та забезпечити виконання основних бізнес-цілей підприємства.

Побудова ефективної системи управління ризиками IT-безпеки – це не разовий проєкт, а комплексний процес, направлений на мінімізацію зовнішніх і внутрішніх загроз при обліку обмежень на ресурси і час. Для побудови ефективної системи IT-безпеки необхідно спочатку узагальнено описати процеси діяльності і виділити ризики. Потім слід визначити поріг ризиків. Перевищення подібного порогу означає, що даним ризиком необхідно

управляти. Потрібно побудувати таку систему ІТ-безпеки, яка забезпечить мінімізацію ризиків з високим рівнем небезпеки. Причому ризики, що мають рівень нижче критичного, можна взагалі виключити з аналізу. В таблиці 1.1 наведені основні стадії управління ризиками.

Таблиця 1.1– Управління інформаційною безпекою на різних стадіях життєвого циклу ІС

Фаза життєвого циклу інформаційних систем	Відповідність фазі управління ризиками
1 Передпроєктна стадія	Виявлення основних класів ризиків для даної ІС.
2 Проєктування ІС	Виявлення ризиків, специфічних для даної ІС (що випливають з особливостей архітектури ІС)
3 Створення ІС: постачання елементів, монтаж, налагодження та конфігурування	До початку функціонування ІС повинні бути ідентифіковані і взяті до уваги всі класи ризиків
4 Функціонування ІС	Періодична переоцінка ризиків, пов'язана зі змінами зовнішніх умов і в конфігурації ІС
5 Припинення функціонування ІС (інформаційні та обчислювальні ресурси більше не використовуються за призначенням і утилізуються)	Дотримання вимог інформаційної безпеки за відношенню до виведеним інформаційних ресурсів

Стосовно основних типів ІС складаються типові моделі загроз безпеки, що характеризують настання різних видів наслідків в результаті несанкціонованого або випадкового доступу.

1.3 Загальний опис методик управління інформаційною безпекою

Формальне визначення політики безпеки називають *м*атематичною моделлю безпеки. Згідно з вимогами нормативних документів у сфері захисту інформації в інформаційних системах, системи захисту інформації будують на основі математичних моделей захисту інформації. Використання цих моделей дає змогу теоретично обґрунтувати відповідність системи захисту інформації вимогам заданої політики безпеки.

Існує велика кількість методик ІБ,які ґрунтуються на математичних моделях та на моделях, які розроблені провідними компаніями у галузі комп'ютерних технологій таких ,як Microsoft . На рисунку 1.1 наведено деякі з моделей.

Нижче розглянемо данні моделі в більш розгорнутому виді та проведемо загально порівняльний аналіз.

1.3.1 Дискреційна політика безпеки

Дискреційна політика безпеки - політика безпеки здійснювана на підставі заданого адміністратором безлічі дозволених відносин доступу.

Основою дискреційної (дискретної) політики безпеки являється дискреційне управління доступом (Discretionary Access Control - DAC), яке визначається двома властивостями:

– всі суб'єкти та об'єкти повинні бути ідентифіковані;

– права доступу суб'єкта до об'єкта системи визначаються на підставі деякого зовнішнього по відношенню до системи правила (заздалегідь не закладається в систему).

До переваг дискреційної політики безпеки можна віднести відносно просту реалізацію відповідних механізмів захисту. Цим обумовлений той факт, що більшість поширених в даний час АС забезпечують виконання положень саме даної політики безпеки.

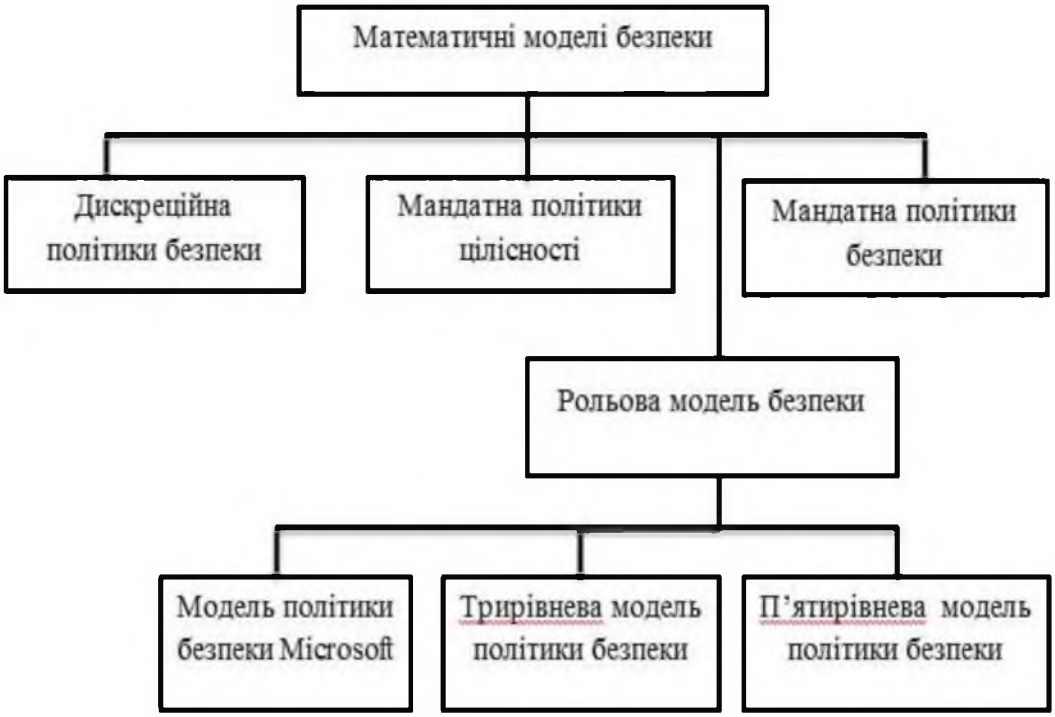

Рисунок 1.1 – Основні в моделі безпеки

Недолік - статична система.

Як приклад реалізацій дискреційної політики безпеки в АС можна привести матрицю доступів, рядки якої відповідають суб'єктам системи, а стовпці - об'єктам; елементи матриці характеризують права доступу. До недоліків відноситься статичність моделі. Це означає, що дана політика безпеки не враховує динаміку змін стану АС, не накладає обмежень на стану системи.

Крім цього, при використанні дискреційної політики безпеки виникає питання визначення правил поширення прав доступу та аналізу їх впливу на безпеку автоматизовану систему. У загальному випадку при використанні даної політики безпеки перед МБО (монітором безпеки об'єктів), який при санкціонуванні доступу суб'єкта до об'єкта керується деяким набором правил, варто алгоритмічно нерозв'язна завдання: перевірити призведуть його дії до порушення безпеки чи ні.

У той же час є моделі автоматизованої системи, що реалізують дискреційну політику безпеки (наприклад, модель Take-Grant), які надають алгоритми перевірки безпеки.

Так чи інакше, матриця доступів не є тим механізмом, який би дозволив реалізувати ясну і чітку систему захисту інформації в автоматизованій системі. Цим обумовлюється пошук інших більш досконалих політик безпеки.

1.3.2 Мандатна політика безпеки

Мандатна політика безпеки - політика безпеки заснована на сукупності надання доступу, визначеного на безлічі атрибутів безпеки суб'єкта та об'єкта.

Основу мандатної (повноважної) політики безпеки випадках становить мандатне управління доступом (Mandatory Access Control - MAC), яке передбачає, що:

- всі суб'єкти та об'єкти системи повинні бути однозначно ідентифіковані;
- заданий лінійно упорядкований набір міток секретності;
- кожному об'єкту системи привласнена мітка секретності, яка визначає цінність міститься в ньому інформації - його рівень секретності в АС;
- кожному суб'єкту системи присвоєна мітка секретності, яка визначає рівень довіри до нього в АС - максимальне значення мітки секретності об'єктів, до яких суб'єкт має доступ; мітка секретності суб'єкта називається його рівнем доступу;

Основна мета мандатної політики безпеки - запобігання витоку інформації від об'єктів з високим рівнем доступу до об'єктів з низьким рівнем доступу, тобто протидія виникненню в АС інформаційних каналів зверху вниз.

Перевага МПБ - більш високий ступінь надійності, правила ясні і зрозумілі.

Це пов'язано з тим, що МБО такої системи повинен відслідковувати не тільки правила доступу суб'єктів системи до об'єктів, а й стану самої АС. Таким чином, канали витоку в системах даного типу не закладені в неї безпосередньо (що ми спостерігаємо в положеннях попередньої політики безпеки), а можуть з'явитися тільки при практичній реалізації системи внаслідок помилок розробника.

Недоліки - реалізація систем з політикоюбезпеки даного типу досить складна і вимагає значних ресурсів обчислювальної системи.

Як приклад моделі АС, що реалізують мандатну політику безпеки можна привести - модель Белла-Лапалуда. В рамках даної моделі доводиться важливе твердження, яке вказує на принципову відмінність систем, що реалізують мандатну захист, від систем з дискреційної захистом: якщо початковий стан системи безпечно, і всі переходи системи зі стану в стан не порушують обмежень, сформульованих політикою безпеки, то будь-який стан системи безпечно.

1.3.4 Мандатна політика цілісності (Абстрактна модель захисту інформації)

Однією з перших моделей була опублікована в 1977 модель Біба. Відповідно до неї всі суб'єкти та об'єкти попередньо поділяються за кількома рівнями доступу, а потім на їх взаємодії накладаються наступні обмеження:

– суб'єкт не може викликати на виконання суб'єкти з більш низьким рівнем доступу;

– суб'єкт не може модифікувати об'єкти з більш високим рівнем доступу.

Як бачимо, ця модель дуже нагадує обмеження, наведені в моделі ЛаПадула.

1.3.5 Рольова політика безпеки

В основі розглянутих раніше політик безпеки лежать ставлення між окремим користувачем (суб'єктом) і об'єктом доступу, визначається яким зовнішнім фактором (дискреційний доступ), або рівні безпеки (мандатний доступ). Разом з тим, аналіз різних організаційно-управлінських і організаційно-технологічних схем, показує, що в реальному житті співробітники підприємств, установ виконують певні функціональні обов'язки не від свого особистого імені, а в рамках певної посади. Посада, яку можна трактувати як певну роль, представляє деяку абстрактну, точніше узагальнену сутність, яка має певний тип функцій і тип положення робітника (підпорядкованість, права і повноваження).

Таким чином, в реальному житті в більшості організаційно-технологічних схем права і повноваження надаються конкретному співробітнику не особисто (безпосередньо), а через призначення його на певну посаду (роль), з якою він і отримує певний типовий набір прав і повноважень.

Ще одним аспектом реальних організаційно-технологічних і управлінських схем є використання понять прав і повноважень, як якихось процедур над ресурсами системи, що відбивають організаційно-технологічні процеси предметної області КС. Інакше кажучи, права і повноваження співробітникам за їхнім посадам надаються не на рівні елементарних операцій над ресурсами (читати, змінювати, додавати, видаляти, створювати), а на рівні сукупностей елементарних операцій, згрупованих в окремі логічно узагальнені процедури оброблення інформації (наприклад, кредитні або дебетні операції над певними бюджетами).

Таким чином, політика розмежування доступу в комп'ютерних системах, що автоматизують ті чи інші організаційно-технологічного чи організаційно-управлінські процеси, повинна будуватися на основі функціонально-рольових відносин, що складаються в предметної області КС.

Вперше подібний підхід був розглянутий в кінці 70-х - початку 80-х роках у дослідженнях з процесів розмежування доступу корпорації IBM і отримав назву рольового управління доступом. На початку 80-х років була представлена модель Лендвера-Макліна, що зустрічається в літературі також під назвою MMS-моделі (MilitaryMessageSystem), що поєднує дискреційний і мандатний принципи розмежування доступу з використанням поняття та механізму ролей. Трохи пізніше з'явилися і формальні визначення рольових основ управління доступом (Role-BasedAccessControl - RBAC). [4]

Основою рольових моделей, як зазначалося, є введення в суб'єктно-об'єктну модель КС додаткової категорії активних сутностей - ролей. Можна дати наступне формальне визначення ролей:

Роль - це активно діюча в системі абстрактна сутність, з якою пов'язаний

обмежений, логічно зв'язаний набір повноважень, необхідних для здійснення певної діяльності.

У РПБ класичне поняття «суб'єкт» заміщується поняттями «користувач» і «роль».

Користувач - це людина, яка працює з системою і виконує певні службові обов'язки.

Справді, по суті, користувачі, що працюють у системі, діють не від свого власного імені - вони завжди виконують певні службові обов'язки, тобто виконують деякі ролі, які аж ніяк не пов'язані з їх особистістю. Тому цілком логічно здійснювати керування доступом і призначати повноваження не реальним користувачам, а абстрактним (не персоніфікованим) ролям, які представляють учасників певного процесу обробки інформації. Такий підхід до ПБ дозволяє врахувати розподіл обов'язків і повноважень між учасниками прикладного інформаційного процесу, оскільки з точки зору РПБ має значення не особистість користувача, що здійснює доступ до інформації, а те, які повноваження йому необхідні для виконання його службових обов'язків.

Наприклад, у реальній системі обробки інформації системний адміністратор, менеджер баз даних і прості користувачі. У такій ситуації РПБ дає змогу розподілити повноваження між цими ролями відповідно до їх службових обов'язків: ролі адміністратора призначаються спеціальні повноваження, які дозволять йому контролювати роботу системи і керувати її конфігурацією, роль менеджера баз даних дозволяє здійснювати керування сервером БД, а права простих користувачів необхідним для запуску прикладних програм. Крім того, кількість ролей у системі може не відповідати кількості реальних користувачів - один користувач, якщо він має різні повноваження, може виконувати (водночас або послідовно) кілька ролей, а кілька користувачів можуть користуватися однією й тією ж роллю, якщо вони виконують однакову роботу.

При використанні РПБ керування доступом здійснюється в дві стадії: по-перше, для кожної ролі вказується набір повноважень, що представляють набір прав доступу до об'єктів, і, по-друге, кожному користувачеві призначається

список доступних йому ролей. Повноваження призначаються ролям відповідно до принципу найменших привілеїв, з якого випливає, що кожний користувач повинен мати тільки мінімально необхідні для виконання своєї роботи повноваження.

Повноваження, як уже зазначалося, трактуються, як право здійснюють деякі функціонально-логічні процедури над всією сукупністю об'єктів системи або над певною їх групою. При цьому, у відомих формальних рольових моделях не вводяться окремі механізми специфікації повноважень, а використовується традиційний набір елементарних методів доступу (читання, запис, і т. п.).

У той же час в таких широко поширених різновидах систем, як СКБД, детальні специфікації функціонально-логічних процедур над даними використовуються повсюдно. Основу обробки даних у реляційних СКБД складають запити, відокремлюються в окремі іменовані операції над даними (інструкції SELECT, INSERT, UPDATE, DELETE), об'єкти даних (таблиці) і результати обробки. Сконструйовані і виражені мовою SQL запити зберігаються в БД разом з даними і становлять окрему групу об'єктів (сутностей) бази даних. Користувачам системи надаються права запускати визначені запити, які можна інтерпретувати як дискреційний спосіб надання повноважень з обробки даних.

В операційних системах, зважаючи на їх більшій універсальності і орієнтованості на широке коло предметних областей, повноваження ролей (наприклад, для ролей адміністраторів, аудиторів, або повноваження для робочих груп користувачів) визначаються частіше всього на основі дискреційного принципу через права за певними методами доступу до певних об'єктів системи або до об'єктів окремих категорій (до списків доступу, до журналу аудиту і т.п.). Подібний підхід називають механізмом привілеїв.

Введення ролей призводить до двоетапної організації системи розмежування доступу:

– створення ролей і визначення їх повноважень (прав доступу до об'єктів);

– призначення ролей користувачам системи.

Відповідно формальні специфікації рольових моделей повинні регламентувати тим чи іншим способом, точніше в рамках тієї чи іншої політики, і визначення повноважень ролям і призначення ролей користувачам.

Управління доступом в рольових системах вимагає розбиття процесу функціонування системи та роботи користувача на сеанси, в кожному з яких, у свою чергу, виділяється дві фази:

1 Авторизація в даному сеансі користувача з однієї або декільком дозволеними (призначеними на другому етапі організації доступу) для нього ролями;

2 Дозвіл або заборона суб'єктам користувача доступу до об'єктів системи в рамках повноважень відповідних ролей, з котрими авторизований в даному сеансі користувач.

Неважко побачити, що рольові моделі поєднують мандатний підхід до організації доступу через певну агрегацію суб'єктів та об'єктів доступу, і тим самим забезпечують жорсткість правил розмежування доступу, і дискреційний підхід, що забезпечує гнучкість в налаштуванні системи розмежування доступу на конкретні функціонально-організаційні процеси предметної області КС.

Даніособливостірольовоїполітикидозволяютьбудуватисистемирозмежування доступу з хорошою керованістю в складних системах з великою кількістю користувачів та об'єктів, і тому знаходять широке застосування в практичних системах.

1.3.6 Трирівнева модель політики безпеки

Бібліотека ITIL (Information Technology Infrastructure Library) містить комплекс необхідних для побудови СУІБ рекомендацій.

По-перше, в ITIL з певним ступенем деталізації описаний процес управління безпекою (Security Management). Вдруге, надання IT- послуг, включаючи сервіси інформаційної безпеки, відносяться к відповідальності служб інформаційних технологій и інформаційної безпеки. Методи ефективної організації діяльності IT- служб узагальнені в бібліотеці ITIL и багаторазово апробовані.

Крім того, компанії пред'являють сьогодні жорсткі вимоги щодо якості IT-послуг (у тому числі і з інформаційної безпеки), що забезпечують підтримку базових бізнес-процесів. Забезпечення гарантованої якості IT- послуг - одна з основних задач процесів ITIL.

Важливо, що для організації ефективної системи управління ІБ, аналогічно управлінню IT- послуг, необхідна чітко діюча система оперативного управління змінами. У ITIL ці завдання вирішені шляхом організації процесів управління змінами. (Change Management).

В даний час бібліотека ITIL стала фактично стандартом в галузі управління IT послугами і увібрала в себе кращі підходи та методики, узагальнюючі накопичений світовий досвід. На рис 1.2 представлені процеси еталонної моделі ITIL.

Згідно з методологією ITIL в забезпеченні інформаційної безпеки беруть участь практично всі процеси еталонної моделі ITIL. Зв'язки процесу управління безпекою з іншими процесами ITIL наведено на рис. 1.3.

Інтеграція процесу управління безпекою в систему процесів управління

IT- ресурсами та IT- послугами і застосування сервісно-ресурсного підходу при побудові СУІБ (коли забезпечення ІБ розглядається як сервіс з певним рівнем якості, надання якого забезпечується певними фінансовими, технічними, людськими ресурсами) дає цілий ряд переваг. Зокрема, з'являється можливість правильної розстановки пріоритетів для вирішуваних завдань ІБ, підвищення ефективності витрачання ресурсів та коштів, що виділяються на управління безпекою, і як наслідок - підвищення керованості системи ІБ в цілому.

Разом з тим, одних рекомендацій ITIL для побудови повнофункціональної СУІБ недостатньо. По-перше, необхідно підтримку життєздатності СУІБ в часі,забезпечити її життєвий цикл. Необхідні для цього компоненти і властивості СУІБ наведені у використовуваному нами стандарті ISO 27001 [5].

Рисунок 1.2 - Процеси еталонної моделі ITIL

По-друге, в ITIL не містяться деякі важливі складові СУІБ, наприклад, планування забезпечення безперервності ведення бізнесу. Крім того, необхідно більш глибоке визначення процесів забезпечення ІБ і їх взаємозв'язків.

Наприклад, для виявлення інцидентів необхідно вести моніторинг підсистем ІБ, який пов'язаний з процесом моніторингу IT- систем, системами AssetManagement і т.д. Для усунення інцидентів необхідна організація процесу управління інцидентами. Для підтримки життєздатності системи ІБ необхідні регулярні внутрішні аудити системи ІБ, що вимагає певного навчання співробітників.

І, природно, певного фінансування внутрішні аудити системи ІБ, що вимагає певного навчання співробітників і, природно, певного фінансування. Важливими складовими забезпечення інформаційної безпеки є також процеси управління інформаційними ризиками, інформування співробітників про політику ІБ, правилах роботи з конфіденційною інформацією та ін.

Рисунок 1.3 - Зв'язки процесу управління безпекою з іншими процесами ITIL

Крім того, необхідно накладення на модель процесів рольової моделі СУІБ, тобто визначення власників процесів, ролей співробітників, які експлуатують підсистеми ІБ і відповідають за відповідні сегменти системи. Тоді у разі інциденту ІБ, наприклад, порушення мережевого захисту, можна буде простежити його вплив на інші процеси і підсистеми ІБ, визначити відповідальних за усунення таких інцидентів, оцінити економічні параметри (яких збитків завдано, які кошти знадобляться для запобігання такого роду інцидентів і т. д.). Певні рекомендації по побудові рольової моделі містяться в документах Microsoft service management function (SMF).

Тому при побудові СУІБ ми використовуємо наведені вище рекомендації та стандарти та на їх основі будуємо модель СУІБ компанії, яка містить три рівні процесів.

– Процеси стратегічного рівня - управління ризиками, управління безперервністю ведення бізнесу, розробка та розвиток політики ІБ верхнього рівня;

– Тактичні процеси - розробка та розвиток процедур ІБ, технічної архітектури системи ІБ, класифікація ІТ- ресурсів, моніторинг і управління інцидентами та інші;

– Процеси операційного рівня - управління доступом, управління мережевою безпекою, перевірка відповідності та ін.

Визначаються взаємозв'язку процесів. В результаті ми отримуємо трирівневу провесно - сервісну модель системи управління ІБ, відповідну вимогам стандарту ISO 27001, на яку накладається рольова модель.

Модель СУІБ формалізується в єдиному комплексі нормативних документів. У цей комплекс входять наступні основні документи.

1 Концепція забезпечення ІБ;

2 Політика інформаційної безпеки;

3 Положення про інформаційну безпеку компанії;

4 План забезпечення безперервної роботи і відновлення працездатності інформаційної системи в кризових ситуаціях;

5 Правила роботи з захищається інформацією;

6 Журнал обліку нештатних ситуацій;

7 План захисту інформаційних систем компанії;

8 Положення про права доступу до інформації;

9 Інструкція по внесенню змін до списків користувачів і наділення їх повноваженнями доступу до інформаційних ресурсів компанії;

10 Інструкція щодо внесення змін до складу і конфігурацію технічних і програмних засобів інформаційних систем;

11 Інструкція по роботі співробітників в мережі Інтернет;

12 Інструкція з організації парольного захисту;

13 Інструкція з організації антивірусного захисту.;

14 Інструкція користувачеві інформаційних систем по дотриманню режиму інформаційної безпеки;

15 Інструкція адміністратора безпеки мережі;

16 Аналітичний звіт про проведену перевірку системи інформаційної безпеки;

17 Вимоги до процесу розробки програмного продукту;

18 Положення про розподіл прав доступу користувачів інформаційних систем;

19 Положення з обліку, зберігання і використання носіїв ключової інформації;

20 План забезпечення безперервності ведення бізнесу;

21 Положення з резервного копіювання інформації;

22 Методика проведення повного аналізу та управління ризиками, пов'язаними з порушеннями інформаційної безпеки.

Перший крок у побудові провесно - рольової моделі управління системи ІБ - це складання та / або аналіз CMDB (configuration management data base) - бази елементарних одиниць, що містить активи системи ІБ (ПО, апаратне забезпечення, співробітники і процедури). Як правило, якісь процеси управління IT у компанії вже є. На жаль, вони часто недостатньо організовані, не формалізовані і погано відповідають вимогам ITIL. Тому для початку потрібно зрозуміти, що є в компанії, потім проаналізувати ключові процеси, які необхідно покращувати. Вибрати один-два процеси, найбільш важливих і вимагають модернізації. Як правило, більшість компаній починають з організації служби Help Desk (сучасна назва-це Service Desk) і впровадження процесу управління інцидентами. У деяких компаніях система Help Desk вже існує і працює, а більш актуальним залишається питання створення процесу управління змінами.

У будь-якому випадку, потрібно розставити пріоритети впровадження процесів і співвіднести їх з планами створення СУІБ.

Всі послуги (поточні, знову розроблені і заплановані) повинні дотримуватися суворих корпоративних стандартів, що стосуються безпеки інформації.

1.3.7 П’ятирівнева модель політики безпеки

Мета створення системи забезпечення інформаційної безпеки Кінцевою метою створення системи забезпечення безпеки інформаційних

технологій є запобігання або мінімізація збитку (прямого або непрямого, матеріального, морального або іншого), що завдається суб'єктам інформаційних відносин за допомогою небажаного впливу на інформацію, її носії і процеси обробки.

Основним завданням системи захисту є забезпечення необхідного рівня доступності, цілісності і конфіденційності компонентів (ресурсів) АС відповідними безлічі значущих загроз методами і засобами. Забезпечення інформаційної безпеки – це безперервний процес, основний зміст якого складає управління - управління людьми, ризиками, ресурсами, засобами захисту і т. п. Люди – обслуговуючий персонал і кінцеві користувачі АС, - є невід'ємною частиною автоматизованої (тобто «людино-машинної системи. Від того, яким чином вони реалізують свої функції в системі, суттєво залежить не тільки її функціональність (ефективність рішення задач), але і її безпеку.

– Опис моделі

З раніше сказаного випливає, що забезпечення безпеки – це процес управління ризиками. Це означає, що система захисту – це система управління, яка реалізує технологію забезпечення безпеки .Будь-яка технологія передбачає певний набір операцій і процесів їх взаємодії виконавців, спрямований на досягнення кінцевого результату (мети),яке виражено на (рис.1.4).рівень інформаційної безпеки організації істотно залежить від діяльності таких категорій працівників і посадових осіб організації:

– співробітників структурних підрозділів (кінцевих користувачів АС), які вирішують свої функціональні завдання із застосуванням засобів автоматизації;

– програмістів, які здійснюють розробку (придбання та адаптацію) необхідних прикладних програм (завдань) для автоматизації діяльності співробітників організації;

– співробітників підрозділу впровадження та супроводу ПЗ, що забезпечують нормальне функціонування і встановлений порядок інсталяції і модифікації прикладних програм (задач);

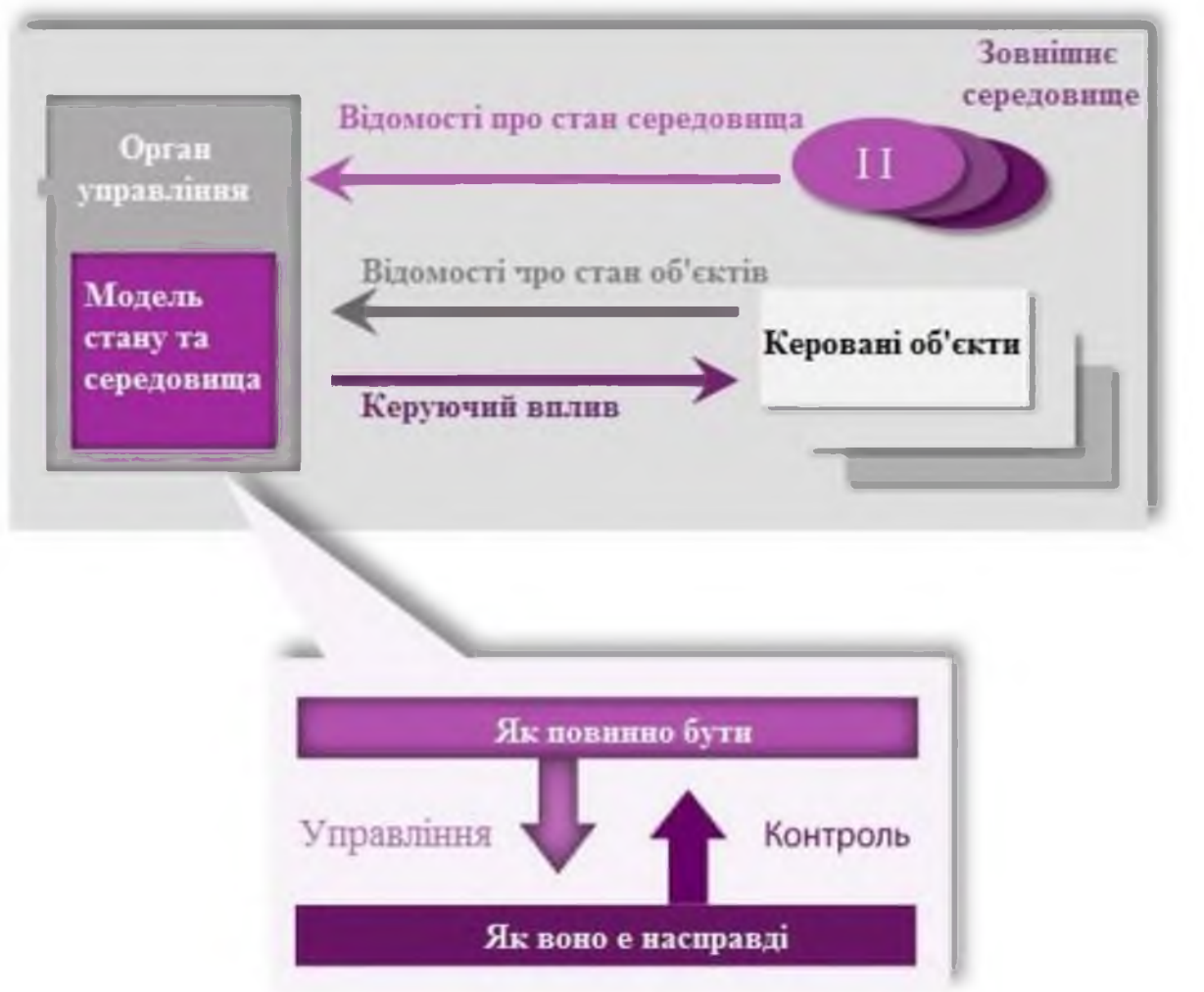

Рисунок 1.4 - Набір операцій і процесів

– співробітників підрозділу експлуатації ТЗ, що забезпечують нормальну роботу і обслуговування технічних засобів обробки і передачі інформації та системного програмного забезпечення;

– системних адміністраторів штатних засобів захисту (ОС, СУБД тощо);

– співробітників підрозділу захисту інформації, які оцінюють стан інформаційної безпеки, що визначають вимоги до системи захисту, що

розробляють організаційно-розпорядчі документи з питань ОІБ (аналітиків), які впроваджують і адмініструють спеціалізовані додаткові засоби захисту (адміністраторів безпеки);

– керівників організації, що визначають цілі та завдання функціонування АС, напрямки її розвитку, що приймають стратегічні рішення з питань безпеки і затверджують основні документи, що регламентують порядок безпечної обробки та використання інформації, що захищається співробітниками організації.

Крім того, на інформаційну безпеку організації можуть впливати сторонні особи і сторонні організації, які спробують втручання в процес нормального функціонування АС або несанкціонованого доступу до інформації як локально, так і віддалено що зображено на (рис.1.5).

Обслуговуючий персонал і користувачі, як невід'ємна частина АС, самі є джерелом внутрішніх загроз інформаційній безпеці організації і одночасно можуть бути частиною системи захисту АС. Тому одним з основних напрямків ОІБ є регламентація дій всіх користувачів і обслуговуючого персоналу АС, цілями якої є:

– скорочення можливостей осіб з числа користувачів і персоналу по вчиненню порушень (як ненавмисних, так і навмисних);

– реалізацію спеціальних заходів протидії іншим внутрішнім і зовнішнім

– для системи загрозам (пов'язаним з відмовами і збоями устаткування, помилками в програмах, стихійними лихами і діями сторонніх осіб, які не є частиною АС).

Регламентація передбачає введення таких обмежень і впровадження таких прийомів роботи співробітників, які, не створюючи перешкод для виконання ними своїх функціональних обов'язків (технологічних функцій), мінімізують можливість вчинення ними випадкових або навмисних порушень (наприклад,

наділення кожного співробітника (користувача) мінімально необхідними для виконання ним своїх обов'язків повноваженнями по доступу до ресурсів АС).

Рисунок 1.5 - Впливи на АС

Крім того, щоб персонал і користувачі як частина системи безпеки АС реалізували свої «захисні можливості», регламентації підлягають питання виконання ними додаткових спеціальних обов'язків (функцій), пов'язаних з посиленням режиму інформаційної безпеки. Так, для захисту від дій сторонніх осіб і «підкріплення» вводяться обмежень на дії своїх співробітників на комп'ютерах АС можуть застосовуватися засоби захисту, що працюють на фізичному, апаратному або програмному рівні. Застосування таких засобів захисту вимагає регламентації питань їх використання кінцевими користувачами і процесів їх адміністрування співробітниками підрозділів автоматизації та забезпечення інформаційної безпеки.

З урахуванням усього сказаного вище, можна зробити висновки:

– до забезпечення безпеки інформаційних технологій організації (і певною мірою до управління її інформаційною безпекою) повинні залучатися практично всі співробітники, що беруть участь у процесах автоматизованої обробки інформації, і всі категорії обслуговуючого АС персоналу;

– за формування системи захисту та реалізацію єдиної політики інформаційної безпеки організації і здійснення контролю і координації дій усіх підрозділів і співробітників організації з питань ІБ має безпосередньо відповідати спеціальний підрозділ (служба) захисту інформації (забезпечення інформаційної безпеки);

В силу нечисленності даного підрозділу рішення ним багатьох процедурних питань і ефективний контроль за дотриманням всіма співробітниками вимог по ОІБ можливі тільки при призначенні у всіх підрозділах, які експлуатують підсистеми АС, позаштатних помічників - відповідальних за забезпечення інформаційної безпеки.

Ефективне використання штатних (для ОС і СУБД) та додаткових засобів захисту забезпечується як системними адміністраторами та адміністраторами засобів захисту, так і системними адміністраторами, переважно вхідними в штат підрозділів автоматизації. Адміністратори додаткових засобів захисту, як правило, є співробітниками підрозділу захисту інформації.

Таким чином, організаційну структуру системи забезпечення інформаційної безпеки АС організації можна представити у вигляді сукупності наступних рівнів Рис.1.6:

- Рівень 1 – Керівництво організації
- Рівень2 – Підрозділ Інформаційної безпеки
- Рівень 3 – Адміністратори штатних і додаткових засобів захисту
- Рівень 4 – Відповідальні за ОІБ в підрозділах (на технологічних дільницях)
- Рівень 5 – Кінцеві користувачі і обслуговуючий персонал

При цьому, серед основних функцій підрозділів із захисту інформації можна назвати:

- формування вимог до системи захисту в процесі створення (розвитку) АС організації;
- визначення потреб у захисті конкретних ресурсів АС, розробка (вдосконалення), погодження та затвердження у керівництва політики безпеки і вимог до системи ЗІ;
- розробка, проведення заходів та координація дій усіх підрозділів і співробітників по реалізації затвердженої політики безпеки, створенню та ефективному застосуванню комплексної системи захисту;
- контроль за виконанням регламентів та процедур забезпечення безпеки, оцінка ефективності та достатності вжитих заходів (застосовуваних процедур і засобів ЗІ);
- участь у проєктуванні системи захисту, її випробуваннях і прийманні в експлуатацію;
- планування, організація та забезпечення функціонування системи захисту інформації в процесі функціонування АС;
- розподіл між користувачами необхідних реквізитів захисту;
- спостереження за функціонуванням системи захисту та її елементів;
- організація перевірок надійності функціонування системи захисту;
- навчання користувачів і персоналу АС правилам безпечної обробки інформації;
- регламентація дій і контроль за адміністраторами баз даних, серверів і мережевих пристроїв (за співробітниками, що забезпечують правильність застосування наявних у складі ОС, СУБД і т.п. засобів розмежування доступу та інших засобів захисту інформації);
- взаємодія з відповідальними за безпеку інформації в підрозділах організації;
- контроль за дотриманням користувачами і персоналом АС встановлених правил;

Рисунок 1.6 - Рівні управління безпекою

– вжиття заходів при спробах несанкціонованого доступу до інформації і при порушеннях правил функціонування системи захисту поводження з захищається в процесі її автоматизованої обробки;

У підсумку можна визначити наступні рівні (ролі) з управління інформаційною безпекою в організації:

1 Рівень прийняття рішень

Керівництво організації - приймає стратегічні рішення з питань автоматизації та ОІБ, затверджує основні документи, що регламентують порядок функціонування та розвитку АІС, що забезпечує безпечну обробку та використання інформації, що захищається.

Керівники та фахівці IT-підрозділів, технічного захисту інформації, начальники служб безпеки, керівники та фахівці служб економічної безпеки.

Керівники організації і підрозділів ІБ і ІТ визначають критичність процесів, ресурсів і необхідний ступінь їх захисту, а також координує управління і розподіл обов'язків служб ІБ і ІТ

2 Рівень підготовки інформації для прийняття рішень

Аудитори і аналітики з питань безпеки ІТ

Аналітики підрозділів ІБ і ІТ відповідають за аналіз стану безпеки ІТ, визначення вимог до захищеності різних підсистем АІС і вибір методів і засобів захисту, розробляють регламенти (політику ІБ)

3 Рівень організації та контролю виконання рішень

Системні і мережеві адміністратори, адміністратори серверів, додатків, баз даних і т.п. відповідають за ефективне їх застосування штатних засобів захисту та розмежування доступу всіх використовуваних ОС і СУБД

Адміністратори додаткових засобів захисту, контролю та управління безпекою відповідають за ефективне застосування спеціалізованих засобів захисту (впливають на безпеку і персонал через засоби захисту), адміністратори безпеки

Менеджери, відповідальні за роботу з персоналом з питань ОІБ

4 Рівень підтримки виконання політики ІБ

Відповідальні за забезпечення безпеки ІТ в підрозділах (на технологічних дільницях) - це посередники між нечисленним підрозділом безпеки і численними користувачами (це «представники ІБ» на місцях). Основні функції відповідальних за забезпечення безпеки ІТ - ефективна підтримка реалізації розроблених підрозділом безпеки і затверджених керівництвом регламентів.

5Рівень виконання політики ІБ (співробітники)

Співробітники структурних підрозділів (кінцеві користувачі системи та обслуговуючий персонал, що працюють із засобами автоматизованої обробки інформації), які вирішують свої функціональні завдання із застосуванням засобів автоматизації.

Всі керівники та фахівці, включаючи підрозділи ІБ і ІТ, при роботі в АІС.

1.4 Аналіз моделей управління інформаційною безпекою

Щоб використовувати ефективні засоби захисту, потрібно проводити аналіз співвідношення витрат і одержуваного ефекту. При цьому треба оцінювати не тільки вартість придбання рішення, але і вартість підтримки його роботи. У витрати можуть включатися:

– вартість реалізації проєкту, включаючи додаткове програмне і апаратне забезпечення;

– зниження ефективності виконання системою своїх основних завдань;

– впровадження додаткових політик і процедур для підтримки засобу;

витрати на найм додаткового персоналу або перенавчання працюючого.

1.5 Порівняння політик управління інформаційною безпекою

В таблиці 1.2 наведена інформація про порівняння методик управління ризиками, які були розглянуті в попередньому розділі.

Таблиця 1.2 – Порівняння політик управління інформаційною безпекою

Модель безпеки	Переваги	Недоліки
Дискреційна політика безпеки	Простота реалізації механізмів захисту.	статична система.
Мандатна політика безпеки	Більш високий ступінь надійності, правила ясні і зрозумілі.	Реалізація систем з політикою безпеки даного типу досить складна і вимагає значних ресурсів обчислювальної системи.
Мандатна політика цілісності	В моделі об'єкти піддаються класифікації, а кожен суб'єкт зараховується до одного з рівнів допуску до класів об'єктів.	Перевірка безпеки системи полягає в перевірці всіх її реалізацій.

Продовження таблиці 1.2

1	2	3
Рольова модель політики безпеки	Відображення множини користувачів на множину ролей і обмежень, які накладаються на функцію авторизації користувача в даному сеансі.	Можливі відносини між ролями, в тому, числі можлива передача (делегування) повноважень і прав від одних ролей іншим ролям.
Трирівнева модель політики безпеки	Не складний у використанні; не потребує залучення зовнішніх експертів; Швидко впроваджується; Безкоштовна для використання.	Відсутня можливість деталізації ризику; Потрібні навики для правильного аналізу ризиків.
П'ятирівнева модель політики безпеки	Містить кількісний аналіз ризиків; Містить автоматизовані засоби аналізу; Підходить для підприємств будь-якого розміру; Велика кількість контрмір у базі знань.	Потребує спеціальної підготовки та високої кваліфікації; довготривалий процес аналізу ризиків.
Microsoft	Підходить для підприємств будь-якого розміру; Містить кількісний аналіз ризиків; Не потребує обов'язкового залучення зовнішніх експертів; Відносна простота впровадження; Безкоштовна для використання.	Відсутність автоматизації; Потрібні навики для правильного аналізу ризиків.

Отже з вище розглянутих моделей найбільш перспективною та оптимальною для наших цілей е трирівнева модель у сукупності з моделью Microsoft.

1.6 Обґрунтування вибору оптимальної методики управління ризиками для для підприємств готельного бізнесу

Після усього вищезазначеного, при урахуванні усіх переваг та недоліків, кожної з методик та враховуючи основні особливості у діяльності підприємств готельного бізнесу, можливо зробити вибір методики.

Більшість українських різноманітних компаній, починаючи з великих компаній, які є лідерами у сфері надання готельних послуг, приймають на посади людей які часто не мають достатнього рівня знань у готельній сфері, особисто в понятті інформаційної безпеки. Це є значною загрозою для безпеки даних які оброблюються в продуктивних системах (наприклад база персональних даних клієнтів. Розповсюдження персональної інформації клієнтів (наприклад: паспортні дані, П.І.Б., інша особиста інформація), може суттєво вплинути на імідж компанії та довіру до неї з боку клієнтів. Також можливо розглядати як одну з загроз – розповсюдження комерційної таємниці конкурентним компаніям (наприклад, розголошення інформації про нову послугу або сервіс – конкурентам, ще до того як вона надійшла на ринок). Тобто недостатній рівень підготовки співробітників, в особистості знання політик у сфері інформаційної безпеки та дотримання їх положень, призводить до підвищення рівня порушення інформаційної безпеки компанії.

У якості найбільш оптимальної методики управління ризиками було запропоновано вибір методики трирівневої моделі . У якості основних переваг цієї методики можливо визначити наступні пункти:

– методика вміщує в собі деякі принципи міжнародних стандартів, таких як ISO 27001, що визначає її відповідність міжнародним підходам до інформаційною безпеки;

– методика є циклічною, що дає змогу постійно вести моніторинг рівня ризиків в компанії, це відповідає вимогам міжнародного стандарту ISO 27005;

– комбінований підхід до управління ризиками є більш простим в порівнянні з традиційним кількісним підходом до управління ризиками, що знов таки надає більше можливостей для використання власного персоналу, без залучення зовнішніх спеціалістів. Цей підхід використовується значно швидше ніж традиційний кількісний підхід до управління ризиками інформаційної безпеки, та дозволяє отримати більш детальніші та зручні в використанні результати ніж традиційний якісний метод, що знов надає перевагу цій методиці перед іншими.

Слід зазначити, що при отриманні додаткових знань або вимог від керівництва, або при зміні умов функціонування підприємства, можливий перехід на інші методики управління ризиками. Так при значному збільшенні підприємства, можливий перехід на методики, які є автоматизованими.

1.7 Висновки. Постановка задачі

У цьому розділі були розглянуті основні особливості процесу управління ризиками ІБ та основні методик оцінки ризику, які використовуються під час процесу управління ІБ.

Була проаналізована нормативна база України, яка регулює процес управління ризиками ІБ, а також розглянуті міжнародні стандарти у сфері управління інформаційними ризиками.

На основі порівняння методик оцінки ризиків, з урахуванням особливостей функціонування, було запропоновано використовувати трирівневу модель управління ризиками.

У наступному розділі буде проведений аналіз загрози та вразливості ІБ в, а також визначена модель загроз та модель порушника для типових. Також буде розглянуто застосування обраної методики управління ризиками.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Особливості організації захисту інформації в на підприємствах готельного бізнесу

В даний час готельна індустрія являє собою галузь з дуже високим рівнем конкуренції. Будь-який сучасний готель - це складний комплекс функціональних ланок. Від злагодженості роботи цього комплексу залежить успішність існування підприємства на ринку. При зростанні обсягу продажів, з одного боку, і зростаючої конкуренції, з іншого, підвищується значення оперативності в роботі персоналу. Гостро постає необхідність автоматизації більшості робочих місць готельного персоналу. Вирішенням цієї проблеми може стати комплексна система захисту інформації, що досягається застосуванням ефективної моделі управління безпекою.

Основні підрозділи готелю:

- Генеральний директор;
- Служба прийому і розміщення;
- Кадрова служба або служба розвитку;
- Служба харчування персоналу;
- Відділ закупок;
- Служба обслуговування гостей;
- Господарська служба або служба експлуатації номерного фонду;
- Інженерна служба;
- Служба захисту;
- Бухгалтерія;

Найбільш важливі підрозділи з точки зору циркулюючої в них інформації та їх основні функції наведено в таблиці 2.1:

Таблиця 2.1 Основні підрозділи готелю та їхфункції

№ п/п	Найменування	Основні функції
1	2	3
1	Генеральний директор	Здійснює щоденне оперативне керівництво персоналом готелю, контролює роботу підлеглих і вирішує всі виникаючі проблеми. Разом з цим він повинен забезпечити і стратегічні завдання управління. Саме генеральний директор представляє на раду директорів фінансовий план (budget) готелю і відповідає за його виконання. Крім щорічних планів генеральний директор відповідає за розробку довгострокового (зазвичай п'ятирічного) плану, в якому повинні бути визначені довгострокові цілі підприємства і розроблені стратегії досягнення цих цілей.
2	Служба прийому і розміщення	Як правило, СПиР включає в себе працівників кількох посад: агент з прийому та розміщення гостей або черговий адміністратор; касир, що приймає оплату і виписує рахунок клієнтові; портьє - відповідальний за надання інформації гостю про функціональні підрозділах готелю, а так само за збір, підшивку і збереження інформації; телефонний оператор, що підтримує зв'язок з міжміськими і міжнародними телефонними станціями, фіксує телефонні дзвінки з номерів, контролюючий їх оплату/ агент з бронювання місць у готелі; портьє з видачі ключів. Інформацією про гостей і безпосереднім спілкуванням з VIP-клієнтами займається менеджер по роботі з гостями.
3	Кадрова служба або служба розвитку	Займаються підбором та профілактикою персоналу,підвищенням рівня його кваліфікації.
4	Інженерна служба	Ремонт,профілактика і підтримка в дієвому стані.
5	Служба захисту	захист гостей, їх майна та майна готелю від можливої шкоди з боку різного роду кримінальних елементів перевірка кредитоспроможності гостей, участь у контролі за комп'ютерною безпекою (запобігання проникнення хакерів) . забезпечення збереження майна і порядка охорона інкасації, контроль за всіма ключами замки з ключами, сейфи в номерах, радіозв'язок співробітників.
6	Бухгалтерія	Облік фінансових потоків.

Основне завдання адміністрації готелів полягає в попередженні всіх можливих ризиків для життя і здоров'я постояльців. Принциповими положеннями забезпечення безпеки готелю є:

– формування вичерпного переліку цілей і завдань із забезпечення безпеки готелю;

– аналіз переліку можливих загроз, ранжирування ймовірностей ризику і потенційного збитку;

– реалізація комплексного підходу і взаємного поєднання організаційних, технічних та кадрових заходів і рішень;

– мінімізація витрат за критерієм «ефективність / вартість»;

– забезпечення живучості, гнучкості і керованості комплексу безпеки;

– можливість розвитку, модернізації і зміни конфігурації комплексу безпеки.

Поняття безпеки включає в себе не тільки захист від кримінальних посягань, але ще більшою мірою створення запобіжних заходів забезпечення захисту від пожежі, вибуху й інших надзвичайних подій [9]. Ефективне вирішення проблеми безпеки готелю вимагає системного підходу, заснованого на аналізі функціонування об'єкта, виявленні найбільш вразливих зон і особливо небезпечних загроз, складання всіх можливих сценаріїв кримінальних дій і вироблення адекватних заходів протидії. Комплексний підхід передбачає оптимальне поєднання організаційних, технічних і фізичних заходів попередження і своєчасного реагування на будь-яку небезпечну ситуацію. Ключове значення набуває правильний вибір технічних засобів і систем безпеки, їх правильне проєктування, монтаж і обслуговування. Тактико-організаційні заходи забезпечення безпеки.

Традиційний метод посилення безпеки шляхом збільшення чисельності співробітників не дає бажаного результату, як через економічні міркування, так і малої ефективності такого підходу. Людина, яка несе службу, схильна до втоми, неуважності, не виключена змова зі злочинцями, шантаж, залякування

і т.д. Єдине правильне вирішення питання безпеки використання системного, комплексного підходу, що поєднує в собі методи організаційного, технічного і фізичного характеру в їх правильному поєднанні і розумному визначенні частки кожної складової. До організаційних заходів належать: спеціально розроблені системи регламентації поведінки обслуговуючого персоналу і співробітників, відповідальних за безпеку; проведення заходів для спеціальної підготовки персоналу служби безпеки; технологія готельного обслуговування; принципи організації порядку доступу й охорони різних категорій готельних номерів і службових приміщень; регламентація дій співробітників в екстремальних ситуаціях.

Забезпечити належну безпеку може комплексний підхід. Можна виділити три рівні забезпечення безпеки: програмно-технічний, процедурний та організаційний.

Для забезпечення безпеки на програмно-технічному рівні, необхідно розмежовувати права доступу на апаратному рівні (канали зв'язку, телефонна станція,…). Безпека на процедурному рівні досягається розмежуванням доступу до додатків та даних, які в них містяться. Наприклад, працівників готелю слід обмежити лише тією інформацією, яка їм необхідна при обслуговуванні клієнтів; менеджери або керівники підрозділів – до тієї частини інформації, яка визначається взаємодією з керівництвом компанії або клієнтами.

У поняття ІБ на організаційному рівні включається забезпечення безпеки на рівні «людського фактору». Її реалізація забезпечується за допомогою контролю виконання посадових інструкцій персоналом. Необхідно також встановити персональну відповідальність кожного співробітника, закріплену на юридичному рівні.

ІБ на організаційному рівні є основною в запобіганні витоку інформації. У більшості випадків витік інформації відбувається з вини співробітників, які мають до неї доступ. Особливо це актуально там, де до доступу до

конфіденційних даних,які обробляються в ІС може привести недостатні знання з питань ІБ співробітниками компанії.

Модель комплексного забезпечення режиму інформаційної безпеки досягається за рахунок структуризації керуючих впливів по рівнях або областях відповідальності.

В таблиці 2.2 наведена структура управління ІБ з урахуванням рівнів відповідальності, класів керуючих впливів та критеріїв безпеки.

Таблиця 2.2 – Структура управління ІБ

Рівень	Класи керуючих впливів і критерії безпеки
1	2
Організаційний рівень	- розмежування відповідальності; - періодичний перегляд системи управління в галузі ІБ; - протоколювання і розбір інцидентів в області ІБ; - оцінка ризиків; - навчання в області ІБ; - процедура авторизації в ІС та видалення облікових записів; - підтримка в актуальному стані плану забезпечення ІБ.
Процедурний рівень	Забезпечення правил підтримання режиму ІБ, зокрема: - доступ до носіїв інформації; - контроль за роботою співробітників в ІС; - забезпечення належної якості роботи силової мережі, кліматичних установок; - контроль за поступаючими в ІС даними.
Програмно-технічний рівень	Комплекс заходів захисту програмно-технічного рівня: - активний аудит і система реагування; - ідентифікація і аутентифікація; - криптографічний захист; - реалізація рольової моделі доступу; - контроль за режимом роботи мережевого обладнання.

2.2 Особливості загроз ІБ

Вище були розглянуті основні загальні загрози інформаційної безпеки підприємства. Нижче буде розглянуто більш деталізовано, загрози безпеки даних які оброблюються в інформаційній системі готелю. Захисту підлягає наступна інформація:

– про клієнтів категорії VIP;

– про факт прибуття та вибуття, час проживання, розпорядок дня, відвідувачів і телефонних абонентів клієнта;

– про зміст переговорів, що ведуться клієнтом (у номері або в спеціально відведених кімнатах)

– інформація, яка обробляється із застосуванням клієнтської або готельної оргтехніки (персональний комп'ютер, друкарська машинка, електронна записна книжка і т.д.);

– інформація, обговорювана або оброблювана із застосуванням технічних засобів під час нарад у спеціально виділених приміщеннях

– комерційна таємниця.

Комерційну таємницю про діяльність готелю можуть складати відомості про окремі фінансові показники, про систему ділових зв'язків, відомості по клієнтах, дані по кадрам, відомості про організацію охорони та протипожежної безпеки. Захист відомостей здійснюється за допомогою певних організаційно-технічних заходів. До організаційних заходів слід віднести обмеження доступу до відомостей, які захищаються, і введення адміністративної і правової відповідальності за їх розголошення. Технічні заходи мають на меті виключити витік відомостей, що захищаються технічними каналами за рахунок прослуховування по акустичних і віброакустичних каналах, побічних електромагнітних випромінювань і наведень технічних засобів зв'язку, електроживлення, радіотелевізійної прийомної апаратури, електропобутових приладів, оргтехніки і т.п .; оптичним каналом, за рахунок засобів несанкціонованого зчитування інформації (закладок).

Склад і зміст загроз безпеки персональних даних визначаються сукупністю умов і факторів, що створюють небезпеку несанкціонованого, в тому числі випадкового, доступу до даних.

Сукупність таких умов і факторів формується з урахуванням характеристик ІС, властивостей середовища розповсюдження інформативних

сигналів, що містять інформацію, яка заміщується та можливих джерел загрози.

До характеристик ІС, що обумовлює виникнення ЗПД, можливо віднести категорію і обсяг оброблюваних в ІС персональних даних, структуру ІС, наявність підключень ІС до мереж зв'язку загального користування і (або) мереж міжнародного інформаційного обміну, характеристики підсистеми безпеки даних, що обробляються в ІС, режими обробки персональних даних, режими розмежування прав доступу користувачів ІС, місцезнаходження та умовами розміщення технічних засобів ІС.

Основними елементами ІС є:

– персональні дані, що містяться в базах даних, як сукупність інформації та її носіїв, які використовуються в ІС;

– відомості про окремі фінансові показники, про систему ділових зв'язків; відомості по клієнтах;

– дані по кадрам;

– відомості про організацію охорони та протипожежної безпеки.

– інформаційні технології, застосовувані при обробці даних;

– технічні засоби, що здійснюють обробку даних (засоби обчислювальної техніки, інформаційно-обчислювальні комплекси та мережі, засоби і системи передачі, прийому й обробки ПД, засоби і системи звукозапису, звукопідсилення, звуковідтворення, переговорні і телевізійні пристрої, засоби виготовлення, тиражування документів та інші технічні засоби обробки мовної, графічної, відео-і літерно-цифрової інформації) (далі – технічні засоби ІС);

– програмні засоби (операційні системи, системи управління базами даних тощо);

– засоби захисту інформації;

– допоміжні технічні засоби і системи – технічні засоби і системи, їх комунікації, не призначені для обробки даних, але розміщені в приміщеннях (далі – службові приміщення), в яких розташовані ІС, їх технічні засоби

(різного роду телефонні засоби і системи, засоби обчислювальної техніки, засоби та системи передачі даних в системі радіозв'язку, засоби і системи охоронної та пожежної сигналізації, засоби і системи оповіщення та сигналізації, контрольно-вимірювальна апаратура, засоби і системи кондиціювання, засоби і системи провідної радіотрансляційної мережі та приймання програм радіомовлення та телебачення, засоби електронної оргтехніки).

Властивості середовища розповсюдження інформативних сигналів, що містять інформацію, яка підлягає захисту, характеризуються видом фізичного середовища, в якому вони поширюються, і визначаються при оцінці можливості реалізації ЗБД.

Можливості джерел ЗБД обумовлені сукупністю способів несанкціонованого і випадкового доступу до ПД, в результаті якого можливе порушення конфіденційності (копіювання, неправомірне розповсюдження), цілісності (знищення, зміна) і доступності (блокування) ПД.

Загроза безпеки ПД реалізується в результаті утворення каналу реалізації ЗБД між джерелом загрози і носієм (джерелом) ПД, що створює умови для порушення безпеки ПД (несанкціонований або випадковий доступ).

Основними елементами каналу реалізації ЗБД, як наведено на рисунку 2.1 є:

– джерело ЗБД – суб'єкт, матеріальний об'єкт або фізичне явище, що створюють ЗБД;

– середовище (шлях) розповсюдження інформації або вплив, в який фізичне поле, сигнал, дані або програми можуть поширюватися і впливати на властивості, які захищаються (конфіденційність, цілісність, доступність) ПД;

– носій даних – фізична особа або матеріальний об'єкт, в тому числі фізичне поле, в якому дані знаходять своє відображення у вигляді символів, образів, сигналів, технічних рішень і процесів, кількісних характеристик фізичних величин.

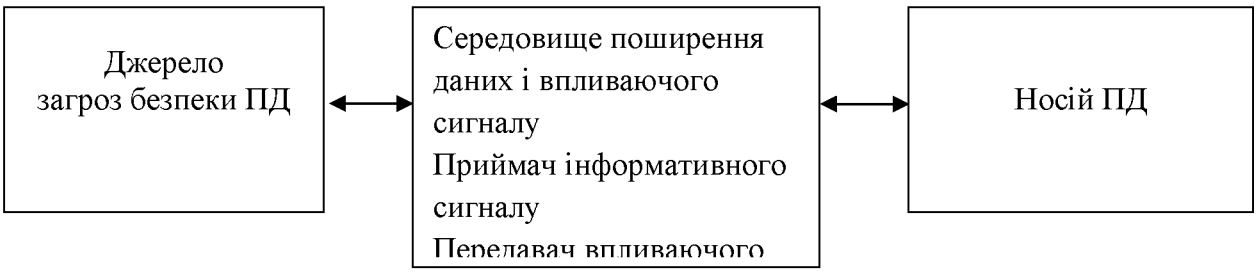

Рисунок 2.1 – Узагальнена схема каналу реалізації загроз безпеки даних

Носії даних можуть містити інформацію, представлену в наступних видах:

– акустична (мовна) інформація, що міститься безпосередньо в вимовній мові користувача ІС при здійсненні ним функції голосового введення в ІС, або відтворювана акустичними засобами ІС (якщо такі функції передбачені технологією обробки даних), а також міститься в електромагнітних полях і електричних сигналах, які виникають за рахунок перетворень акустичної інформації;

– видова інформація, представлена у вигляді тексту і зображень різних пристроїв відображення інформації засобів обчислювальної техніки, інформаційно-обчислювальних комплексів, технічних засобів обробки графічної, відео- та літерно-цифрової інформації, що входять до складу ІС;

– інформація, що обробляється (циркулює) в ІС, у вигляді електричних електромагнітних, оптичних сигналів;

– інформація, що обробляється в ІС, представлена у вигляді біт, байт, файлів і інших логічних структур.

З метою формування систематизованого переліку ЗБД при їх обробці в ІС і розробці на їх основі приватних моделей стосовно до конкретного виду ІС загрози класифікуються згідно з такими ознаками:

– за видом інформації, яка захищається від ЗБД та містить ПД;

– за видами можливих джерел ЗБД;

– за типом ІС, на які спрямована реалізація ЗБД;

– за способом реалізації ЗБД;

– за видом порушуваної властивості інформації (виду несанкціонованих дій, здійснюваних з ПД);

– по використовуваній уразливості;

– по об'єкту впливу.

За видами можливих джерел ЗБД виділяються наступні класи загроз:

– загрози, пов'язані з навмисними або ненавмисними діями осіб, які мають доступ до ІС, включаючи користувачів ІС, що реалізують загрози безпосередньо в ІС (внутрішній порушник);

– загрози, пов'язані з навмисними або ненавмисними діями осіб, які не мають доступу до ІС, що реалізують загрози з зовнішніх мереж зв'язку загального користування і (або) мереж міжнародного інформаційного обміну (зовнішній порушник).

Крім того, загрози можуть виникати в результаті впровадження апаратних закладок і шкідливих програм.

За типом ІС, на які спрямована реалізація ЗБД, виділяються такі класи загроз:

– загрози безпеціданим, що обробляються в ІС на базі автономного автоматизованого робочого місця;

– загрози безпеці даним, що обробляються в ІС таяка, підключена до мережі загального користування (до мережі міжнародного інформаційного обміну);

– загрози безпеці даним, що обробляються в ІС на базі локальних інформаційних систем без підключення до мережі загального користування (до мережі міжнародного інформаційного обміну);

– загрози безпеці даним, що обробляються в ІС на базі локальних інформаційних систем з підключенням до мережі загального користування (до мережі міжнародного інформаційного обміну);

– загрози безпеці даним, що обробляються в ІС на базі розподілених інформаційних систем без підключення до мережі загального користування (до мережі міжнародного інформаційного обміну);

– загрози безпеці ПД, що обробляються в ІС на базі розподілених інформаційних систем з підключенням до мережі загального користування (до мережі міжнародного інформаційного обміну).

За способами реалізації ЗБД виділяються наступні класи загроз:

– загрози, пов'язані з НСД до даних (у тому числі загрози впровадження шкідливих програм);

– загрози витоку даних технічними каналами витоку інформації;

– загрози спеціальних дій на ІС.

По виду несанкціонованих дій, здійснюваних з ПД, виділяються такі класи загроз:

– загрози, що призводять до порушення конфіденційності (копіювання або несанкціонованого розповсюдження), при реалізації яких не здійснюється безпосереднього впливу на зміст інформації;

– загрози, що призводять до несанкціонованого, в тому числі випадкового, впливу на зміст інформації, в результаті якого здійснюється зміна даних або їх знищення;

– загрози, що призводять до несанкціонованого, в тому числі випадкового, впливу на програмні або програмно-апаратні елементи ІС, в результаті якого здійснюється блокування даних.

По використовуваній уразливості виділяються наступні класи загроз:

– загрози, що реалізуються з використанням уразливості системного ПЗ;

– загрози, що реалізуються з використанням уразливості прикладного ПЗ;

– загрози, що виникають в результаті використання уразливості, викликаної наявністю в ІС апаратної закладки;

– загрози, що реалізуються з використанням вразливостей мережевих протоколів і каналів передачі даних;

– загрози, що виникають в результаті використання уразливості, викликаної недоліками організації ТЗІ від НСД;

– загрози, що реалізуються з використанням вразливостей, що обумовлюють наявність технічних каналів витоку інформації;

– загрози, що реалізуються з використанням вразливостей СЗІ.

По об'єкту впливу виділяються такі класи загроз:

– загрози безпеці даним, оброблюваним в інформаційній системі;

– загрози безпеці даним, оброблюваним у виділених засобах обробки (принтерах, винесених монітори, відеопроєктори, засобах звуковідтворення тощо);

– загрози безпеці даним, переданим по мережах зв'язку;

– загрози прикладним програмам, за допомогою яких обробляються дані;

– загрози системного ПЗ, що забезпечує функціонування ІС.

Реалізація однієї з ЗБД перерахованих класів або їх сукупності може привести до наступних типів наслідків для суб'єктів:

– значні негативні наслідки для суб'єктів ;

– негативні наслідки для суб'єктів ;

– незначні негативні наслідки для суб'єктів .

Загрози витоку даних технічними каналами однозначно описуються характеристиками джерела інформації, середовища розповсюдження і приймача інформативного сигналу, тобто визначаються характеристиками технічного каналу витоку даних.

Загрози, пов'язані з несанкціонованим доступом (далі – загрози НСД в ІС), подаються у вигляді сукупності узагальнених класів можливих джерел загроз НСД, вразливостей програмного і апаратного забезпечення ІС, способів реалізації погроз, об'єктів впливу (носіїв інформації, що захищається, тек, каталогів, файлів з даними або самих даних) і можливих деструктивних дій. Таке уявлення описується наступним формалізованим записом:

загроза НСД: = <джерело загрози>, <вразливість програмного або апаратного забезпечення>, <спосіб реалізації загрози>, <об'єкт впливу>, <несанкціонований доступ>.

2.2.1 Модель порушників

Загрози НСД пов'язані з діями порушників, які мають доступ до ІС, включаючи користувачів ІС, що реалізують загрози безпосередньо в ІС, а Також порушників, які не мають доступу до ІС, що реалізують загрози з міжнародного інформаційного обміну[9].

Зовнішніх мереж зв'язку загального користування і (або) мереж.

Загрози НСД, пов'язані з діями порушників, які мають доступ до ІС. Джерелами загроз НСД до інформації можуть бути апаратні закладки та відчужувані носії шкідливих програм.

Крім того, в такій ІС мають місце загрози, що реалізуються з використанням протоколів міжмережевої взаємодії із зовнішніх мереж, в тому числі:

– загрози, що реалізуються в ході завантаження операційної системи і спрямовані на перехоплення паролів або ідентифікаторів, модифікацію базової системи введення / виводу (BIOS), перехоплення управління завантаженням;

– загрози, реалізовані після завантаження операційної системи і спрямовані на виконання несанкціонованого доступу із застосуванням стандартних функцій (знищення, копіювання, переміщення, форматування носіїв інформації тощо) операційної системи або будь-якої прикладної програми (наприклад, системи управління базами даних), із застосуванням спеціально створених для виконання НСД програм (програм перегляду і модифікації реєстру, пошуку текстів в текстових файлах і т.п.);

– загрози «Аналізу мережевого трафіку» з перехопленням передано із ІС та прийнятої в ІС із зовнішніх мереж інформації;

– загрози сканування, спрямовані на виявлення типу або типів використовуваних операційних систем, мережевих адрес робочих станцій ІС, топології мережі, відкритих портів і служб, відкритих з'єднань та ін.;

– загрози впровадження помилкового об'єкта як в ІС, так і в зовнішніх мережах;

– загрози нав'язування хибного маршруту шляхом несанкціонованої зміни маршрутно-адресних даних як всередині мережі, так і у зовнішніх мережах;

– загрози виявлення паролів;

– загрози віддаленого запуску додатків;

– загрози впровадження по мережі шкідливих програм;

– загрози витоку інформації, що оброблюється, або обговорюється з використанням технічних засобів під час нарад та переговорів у спеціально виділеному приміщенні.

З оглядом на різноманіття загроз безпеки інформації потрібно визначити основних суб'єктів загроз – порушників, дії яких викликають нестабільне положення системи, яка захищається. Їх будемо класифікувати враховуючі такі фактори, як місце дії, їх можливості, знання та термін тривалості дії.

Порушник – це особа, що зробила спробу виконання заборонених операцій (дій) помилково, незнання або усвідомлено зі злим умислом (з корисливих інтересів) або без такого (заради гри або задоволення, з метою самоствердження і т.п.) і використовує для цього різні можливості, методи і засоби. [12]

Зловмисником будемо називати порушника, який навмисно йде на порушення з корисливих спонукань.

Неформальна модель порушника відображає його практичні та теоретичні можливості, апріорні знання, час і місце дії і т.п. Для досягнення своїх цілей порушник повинен прикласти деякі зусилля, затратити певні ресурси. Дослідивши причини порушень, можна вплинути на самі ці причини (звичайно якщо це можливо), або точніше визначити вимоги до системи захисту від даного виду порушень або злочинів.

У кожному конкретному випадку, виходячи з конкретної технології обробки інформації, може бути визначена модель порушника, яка повинна бути адекватна реальному порушнику для даної ІС.

При розробці моделі порушника визначаються:

- припущення про категорії осіб, до яких може належати порушник;
- припущення про мотиви дій порушника (переслідуваних порушником цілях);
- припущення про кваліфікацію порушника і його технічну оснащеність (про використовувані для вчинення порушення методи і засоби);
- обмеження і припущення про характер можливих дій порушників.

По відношенню до ІС порушники можуть бути внутрішніми (з числа персоналу системи) або зовнішніми (сторонніми особами). Внутрішнім порушником може бути особа з наступних категорій персоналу:

- користувачі (оператори, менеджери) системи;
- персонал, що обслуговує технічні засоби (інженери, техніки);
- співробітники відділів розробки і супроводу ПЗ (прикладні та системні програмісти);
- технічний персонал, що обслуговує приміщення готелю (прибиральники, електрики, сантехніки та інші співробітники, що мають доступ в приміщення, де розташовані компоненти ІС);
- співробітники служби безпеки ІС;
- керівники різних рівнів посадової ієрархії.

Сторонні особи, які можуть бути порушниками:

- клієнти готелю;
- відвідувачі (запрошені з якого-небудь приводу);
- представники організацій, що взаємодіють з питань забезпечення життєдіяльності організації (енерго-, водо-, теплопостачання тощо);
- представники конкуруючих організацій або особи, що діють за їх завданням;
- особи, випадково чи навмисне порушили пропускний правила готелю (без мети порушити безпеку ІС);
- будь-які особи за межами контрольованої території.

Можна виділити три основні мотиви порушень: безвідповідальність, самоствердження і корисливий інтерес.

При порушеннях, викликаних безвідповідальністю, користувач цілеспрямовано або випадково застосовує будь-які руйнуючі дії, не пов'язані проте зі злим умислом .У більшості випадків це наслідок некомпетентності або недбалості.

Деякі користувачі вважають отримання доступу до системних наборів даних великим успіхом, затіваючи свого роду гру "користувач – проти системи" заради самоствердження або у власних очах, або в очах колег, або знайомих.

Порушення безпеки може бути викликане і корисливим інтересом користувача системи. У цьому випадку він буде цілеспрямовано намагатися подолати систему захисту для доступу до збереженої, що передається та оброблюваної в ІС інформації. Навіть якщо ІС має засоби, що роблять таке проникнення надзвичайно складним, повністю захистити її від проникнення практично неможливо.

Усіх порушників можна класифікувати наступним чином.

За рівнем знань про ІС:

- знає функціональні особливості ІС, основні закономірності формування в ній масивів даних і потоків запитів до них, вміє користуватися штатними засобами;

- володіє високим рівнем знань та досвідом роботи з технічними засобами системи та їх обслуговування;

- володіє високим рівнем знань в області програмування та обчислювальної техніки, проєктування та експлуатації автоматизованих інформаційних систем;

- знає структуру, функції і механізм дії засобів захисту, їх сильні і слабкі сторони.

За рівнем можливостей (методам і засобам, які використовуються):

– застосовує чисто агентурні методи одержання відомостей;

– застосовує пасивні засоби (технічні засоби перехоплення без модифікації компонентів системи);

– використовує тільки штатні засоби і недоліки систем захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії інформації, які можуть бути приховано пронесені;

– застосовує методи і засоби активного впливу (модифікація і підключення додаткових технічних засобів, підключення до каналів передачі даних, впровадження програмних закладок і використання спеціальних інструментальних і технологічних програм).

За часом дії:

- в процесі функціонування ІС (під час роботи компонентів системи);
- в період не активності компонентів системи (у неробочий час, під час планових перерв у її роботі, перерв для обслуговування і ремонту і т.п.);
- як в процесі функціонування ІС, так і в період не активності компонентів системи.

За місцем дії:

- без доступу на контрольовану територію організації;
- усередині приміщень, але без доступу до технічних засобів ІС;

з робочих місць кінцевих користувачів (операторів, або клієнтів готелю) ІС;

- з доступом в зону даних (баз даних, архівів тощо);
- з доступом в зону управління засобами забезпечення безпеки ІС.

Можуть враховуватися такі обмеження і припущення про характер дій можливих порушників:

- робота з підбору кадрів та спеціальні заходи ускладнюють можливість створення коаліцій порушників, тобто об'єднання (змови) і цілеспрямованих дій щодо подолання підсистеми захисту двох і більше порушників;
- порушник, плануючи спроби НСД, приховує свої несанкціоновані дії від інших співробітників;
- НСД може бути наслідком помилок користувачів, адміністратора, що експлуатує та обслуговуючого персоналу, а також недоліків прийнятої технології обробки інформації і т.д.

В таблиці 2.3 наведена типова модель порушника .

Визначення конкретних значень характеристик можливих порушників у значній мірі суб'єктивно. Модель порушника, побудована з урахуванням особливостей конкретної предметної області та технології обробки інформації, може бути представлена перерахуванням декількох варіантів його вигляду. Кожен вид порушника має бути охарактеризований значеннями характеристик, наведених вище[9].

Таблиця 2.3 – Типова модель порушника

Ідентифікатор	Назва	Опис
1	2	3
Зовнішні		
1	Фізичні особи, які ведуть зловмисну діяльність	- можуть діяти в інтересах зацікавлених осіб або приступних груп; - загрози можуть бути реалізовані через зовнішню мережу зв'язку загального користування;
2	Організовані приступні групи	
Внутрішні		
3	Відвідувачі, або клієнти, які не мають постійного доступу	Сторонні особи, які можуть отримати доступ в організацію
4	Обслуговуючий персонал або представники ремонтних організацій, які не мають постійного доступу	- представники сторонніх компаній, які за угодою виконують обслуговування функціонування ЦОА, при виникненні складнощів; - доступ, як правило, надається одноразово.
5	Представники технічних служб	- обслуговуючий персонал(наприклад прибиральники);
6	Співробітники які не є операторами	- співробітники, які не є операторами або адміністраторами ІС (наприклад, офіс-менеджер); - не є користувачами ІС; - постійно не знаходяться на території
7	Оператори	- користувачі ІС, де оброблюється конфіденційна інформація; - має змогу самостійно здійснювати атаки.
8	Адміністратори ІС	- технічні спеціалісти які обслуговують технічні та програмні засоби, займаються їх налаштуванням та конфігуруванням
9	Співробітники органі-зацій, які здійснюють обслуговування ІС на постійній основі відповідно до умов угоди	- розробники ПЗ, організації, які здійснюють технічну підтримку; - мають доступ до ІС

2.2.2 Модель загроз

Нижче розглянута типова модель загроз безпеки інформації готелю, яка оброблюється в розподілених інформаційних системах, що мають підключення до мереж зв'язку загального користування і (або) мереж міжнародного інформаційного обміну.

При обробці даних в розподілених ІС, що мають підключення до мереж зв'язку загального користування і (або) мереж міжнародного інформаційного обміну, можлива реалізація наступних ЗБД:

– загрози витоку інформації технічними каналами;

– загрози НСД до даних, оброблюваних на автоматизованому робочому місці.

Загрози витоку інформації по технічним каналам включають в себе:

– загрози витоку акустичної (мовної) інформації;

– загрози витоку видової інформації;

– загрози витоку інформації по каналу ПЕМВН.

Виникнення загроз витоку акустичної (мовної) інформації, можливо при наявності функцій голосового введення даних в ІС або функцій відтворення даних акустичними засобами ІС.

Реалізація загрози витоку видової інформації можлива за рахунок перегляду інформації за допомогою оптичних (оптико електронних) засобів з екранів дисплеїв і інших засобів відображення обчислювальної техніки, інформаційно-обчислювальних комплексів, технічних засобів обробки графічної, відео-і літерно-цифрової інформації, що входять до складу ІС.

Загрози витоку інформації по каналу ПЕМВН можливі через наявність електромагнітних випромінювань, в основному, монітора і системного блоку комп'ютера. Основну небезпеку представляють загрози витоку через наявність електромагнітних випромінювань монітора.В таблиці 2.4 наведена модель загроз.

Таблиця 2.4 – Модель загроз ІБ

Найменування загрози	Імовірність реалізації загрози	Можливість реалізації загрози	Небезпека загрози	Актуальність загрози
1	2	3	4	5
Загрози навмисного електромагнітного впливу на елементи ІС в готелі	Мало ймовірна	Низька	Низька	Неактуальна
Загрози витоку акустичної інформації	Мало ймовірна	Середня	Низька	Неактуальна
Загрози витоку видової інформації				
Перегляд інформації на дисплеї співробітниками , які не допущені до обробки інформації	Висока	Висока	Середня	Актуальна
Перегляд інформації на дисплеї сторонніми особами, не співробітниками, що знаходяться в приміщенні в якому ведеться обробка інформації	Низька	Середня	Середня	Актуальна
Перегляд інформації на дисплеї сторонніми особами, що знаходяться за межами приміщення в якому ведеться обробка інформації	Низька	Низька	Низька	Неактуальна
Перегляд інформації за допомогою спеціальних електронних пристроїв впроваджених в приміщенні в якому ведеться обробка інформації	Мало ймовірна	Низька	Низька	Неактуальна
Загрози витоку інформації каналами ПЕМВН				
Витік інформації з мереж електроживлення	Мало ймовірна	Низька	Низька	Неактуальна
Витік за рахунок наведень на лінії зв'язку, технічні засоби розташовані в приміщенні і системи комунікацій	Мало ймовірна	Низька	Низька	Неактуальна
Побічні випромінювання технічний засобів	Мало ймовірна	Низька	Низька	Неактуальна
Витоку за рахунок, електромагнітного впливу на технічні засоби	Мало ймовірна	Низька	Низька	Неактуальна
Загрози несанкціонованого доступу до інформації				
Загрози знищення, розкрадання апаратних засобів ІС носіїв інформації шляхом фізичного доступу до елементів ІС				
Крадіжка ПЕОМ	Середня	Середня	Середня	Актуальна
Крадіжка носіїв інформації	Середня	Середня	Середня	Актуальна

Крадіжка ключів доступу	Висока	Висока	Висока	Актуальна
Крадіжки, модифікації, знищення інформації.	Висока	Висока	Висока	Актуальна
Виведення з ладу вузлів ПЕОМ, каналів зв'язку	Низька	Середня	Середня	Актуальна
Несанкціонований доступ до інформації при технічному обслуговуванні (ремонті, знищення) вузлів ПЕОМ	Низька	Середня	Середня	Актуальна
Несанкціоноване відключення засобів захисту	Середня	Середня	Середня	Актуальна
Загрози розкрадання, несанкціонованої модифікації або блокування інформації за рахунок несанкціонованого доступу (НСД) із застосуванням програмно-апаратних і програмних засобів (у тому числі програмно-математичних впливів);				
Комп'ютерні віруси				
Недекларованe можливості системного ПЗ та ПЗ для обробки персональних даних	Низька	Середня	Середня	Актуальна
Установка ПЗ не пов'язаного з виконанням службових обов'язків	Низька	Середня	Середня	Актуальна
Наявність апаратних закладок в придбаних ПЕОМ	Низька	Середня	Середня	Актуальна
Впровадження апаратних закладок сторонніми особами після початку експлуатації ІС	Низька	Низька	Низька	Неактуальна
Впровадження апаратних закладок співробітниками організації	Низька	Середня	Середня	Актуальна
Впровадження апаратних закладок обслуговуючим персоналом (ремонтними організаціями)	Низька	Середня	Середня	Актуальна
Загрози не навмисних дій користувачів і порушень безпеки функціонування ІС і ЗЗІ в її складі через збої в програмному забезпеченні, а також від загроз не антропогенного (збоїв апаратури через ненадійність елементів, збоїв електроживлення) і стихійного (ударів блискавок, пожеж, повеней і т.п.) характеру.				
Ненавмисна модифікація (знищення) інформації співробітниками	Висока	Висока	Висока	Актуальна
Ненавмисне відключення засобів захисту	Низька	Середня	Середня	Актуальна
Вихід з ладу апаратно-програмних засобів	Висока	Висока	Висока	Актуальна
Збій системи електропостачання	Висока	Висока	Висока	Актуальна
Стихійне лихо	Низька	Середня	Середня	Актуальна
Загрози навмисних дій внутрішніх порушників				
Доступ, модифікація, знищення інформації особами, не допущеними до її обробці	Середня	Середня	Середня	Актуальна

Розголошення інформації, модифікація, знищення представниками організації	Висока	Висока	Висока	Актуальна
Загрози несанкціонованого доступу по каналах зв'язку				
Несанкціонований доступ через ЛОМ організації	Середня	Середня	Середня	Актуальна
Загрози перехоплення при передачі по провідних (кабельним) лініях зв'язку				
Перехоплення за межами контрольованої зони	Висока	Висока	Висока	Актуальна
Перехоплення в межах контрольованої зони зовнішніми порушниками	Низька	Середня	Середня	Актуальна
Перехоплення в межах контрольованої зони внутрішніми порушниками	Низька	Середня	Середня	Актуальна

2.3 Функціональні профілі захищеності

Відповідно НД ТЗІ 2.5-005-99, автоматизована система, що забезпечує функціонування автоматизованої системи підприємства, представляє собою АС 3 класу, тобто розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності[11].

Автоматизована система являє собою організаційно-технічну систему, що об’єднує ОС, фізичне середовище, персонал і оброблювану інформацію.

Згідно з НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС. На основі типовий умов функціонування і класу системи був обраний наступний стандартний профіль захищеності:

3.КЦД.2 = { КД-2, КА-2, КО-1, КВ-2,

ЦД-1, ЦА-2, ЦО-1, ЦВ-2,

ДР-1, ДВ-1,

НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1}

КД-2. Базова довірча конфіденційність:

– політика довірчої конфіденційності, що реалізується КЗЗ,повинна визначати множину об'єктів КС, до яких вона відноситься;

– КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта;

– запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта;

– КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити: конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта;

– КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити: конкретних користувачів і/або групи користувачів, які мають право ініціювати процес;

– права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту.

КА-2. Базова адміністративна конфіденційність:

– політика адміністративної конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС, до яких вона відноситься;

– КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта;

– запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження;

– КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожногозахищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта;

– КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес;

– права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту.

КО-1. Повторне використання об'єктів:

– політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС;

– перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані;

– перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.

КВ-2. Базова конфіденційність при обміні:

– політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься;

– політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується

механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності;

– КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається;

– запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження;

– запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу;

– запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу.

ЦД-1. Мінімальна довірча цілісність:

– КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу;

– політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься: користувача і захищеного об'єкта;

– запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта;

– КЗЗ повинен надавати користувачу можливість для кожного захищеного об’єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт;

– права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.

ЦА-2. Базова адміністративна цілісність:

– політика адміністративної цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься;

– КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта;

– запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження;

– КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити: конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт;

КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес;

– права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.

ЦО-1. Обмежений відкат:

– політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься;

– повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір(множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

ЦВ-2. Базова цілісність при обміні:

– політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності;

– КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається

також фактів його видалення або дублювання;

– запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу;

– запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу;

– запити на присвоєння або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження.

ДР-1. Квоти:

– політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься;

– політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу;

– запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки

в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

ДВ-1. Ручне відновлення:

політика відновлення, що реалізується КЗЗ, повинна визначати

множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС;

– після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження.

НР-2. Захищений журнал:

– політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються;

– КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки;

– журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події;

– КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування;

– адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

НИ-2. Одиночна ідентифікація і аутентифікація:

– Політика ідентифікації і аутентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ;

– перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму;

– КЗЗ повинен забезпечувати захист даних аутентифікації від несанкціонованого доступу, модифікації або руйнування.

НК-1. Однонаправлений достовірний канал:

– політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ;

– достовірний канал повинен використовуватися для початкової ідентифікації і аутентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

НО-2. Розподіл обов'язків адміністраторів:

– політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції;

– політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі;

– користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

НЦ-2. КЗЗ з гарантованою цілісністю:

– політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів;

– КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування;

– повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

НТ-2. Самотестування при старті:

– політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ;

– КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні

виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ.

НВ-1. Аутентифікація вузла:

– політика ідентифікації і аутентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ;

– КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і аутентифікувати цей КЗЗ с використанням захищеного механізму;

– підтвердження ідентичності має виконуватися на підставі затвердженого протоколу аутентифікаці.

Для забезпечення виконання всіх послуг функціонального профілю захищеності 3.КЦД.2, потрібно забезпечити:

1 КА-2. Базова адміністративна конфіденційність. Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів;

2 КВ-2. Базова конфіденційність при обміні. Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення зінформацією, що міститься в них, під час їх експорту / імпорту через незахищене середовище;

3 ЦА-2. Базова адміністративна цілісність. Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів;

4 ЦВ-2. Базова цілісність при обміні. Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище.

Всі ці вимоги можна виконати при використанні комп’ютерної системи управління роботою готелю.

2.4 Практичне застосування методики управління інформаційною безпекою на підприємствах готельного бізнесу

Встановлюваний комплекс засобів і систем захисту має бути адекватним можливій загрозі та розробленій моделі порушника , тобто засоби і системи мають бути розумно достатні. Неможливо, та й недоцільно, виключити будь-яку можливість нанесення збитку насамперед з економічних міркувань. Засоби забезпечення безпеки досить дорогі, тому їх вибір має визначатися дійсно розумним аналізом можливих ризиків і збитку. Наповнення комплексу засобів повинно залежати від розміру готелю та виду послуг, які він надає. Крім того, використовувана апаратура не повинна створювати додаткових перешкод і великих ускладнень для нормального функціонування готелю як для обслуговуючого персоналу, так і для гостей. Зайва таємничість, жорсткий режим, постійна демонстрація збройної охорони і підозрілості може відлякати частину клієнтів і позбавити готель іміджу «відкритого будинку». Система повинна бути збалансованою, тобто засоби захисту повинні розподілятися по можливості рівномірно у відповідності зі значимістю зон, що захищаються.

Усі застосовувані заходи і засоби не повинні створювати додаткової небезпеки здоров'ю і життю гостей і співробітників готелю.

Використати обрану модель управління інформаційною безпекою пропонується для типового готельного комплексу на прикладі готелю «Схід».

Комплекс включає бізнес-центр і готель на 49 номерів. Інфраструктура готелю включає в себе конференц-зал, фітнес-центр, боулінг, ресторан та ін. Комплекс обладнаний системою бездротового доступу в Інтернет за технологією Wi-Fi.

Площа готельного комплексу - 10 тис. Кв.м, бізнес-центру - 3 тис. Кв.м.

У номерах для гостей передбачено все найнеобхідніше у тому числі: прямі телефонні лінії;

бездротовий доступ до Інтернету за технологією WiFi;

індивідуальний сейф в кожному номері.

Чисельність персоналу залежить від рівня готелю, кількості номерів,

етажності будівлі. Служба безпеки як правило складає 10-15% від загальної чисельності персоналу[6].

За мету, під час реалізації методики на практиці, було визначене не детальний аналіз ризиків існуючого підрозділу, а встановлення принципів та ефективність використання методики управління ризиками, для типового класу підприємств.

2.5 Техніко-економічне обґрунтування впровадження комп'ютерної системи управління

Для забезпечення високого рівня обслуговування клієнтів комплексу необхідно забезпечити автоматизовану систему управління готелем, а також рестораном і розважальним комплексом.

Система повинна забезпечити вирішення наступних завдань:

1 Забезпечити швидке і зручне рішення повсякденних завдань при роботі з клієнтами: бронювання номерів, оформлення гостей, попереднє замовлення столиків і обробка замовлень в ресторані;

2 Забезпечити контроль в реальному часі за станом складів, діяльністю персоналу і рухом фінансів в рамках всього комплексу;

3 Забезпечити індивідуальний підхід до кожного клієнта, з урахуванням його переваг і категорії;

4 Забезпечити ведення статистики та інструменту прогнозування роботи комплексу, включаючи можливість обміну даними системи автоматизації з програмами бухгалтерського та фінансового обліку;

5 Забезпечити клієнтів готелю сучасними засобами зв'язку, включаючи бездротовий Інтернет за технологією Wi-Fi та міжміського / міжнародного телефонного зв'язку;

6 Забезпечити надійний захист всіх категорій інформації, що циркулює на підприємстві;

7 Забезпечити надійний захист даних згідно обраного профілю захищеності.

В якості прикладу комп'ютерної системи управління обираємо комплекс бронювання. Обираємо тому, що цей комплекс було створено виробниками з урахуванням нормативної бази України.

2.6 Підходи до вирішення проблем впровадження та експлуатації комп'ютерної системи управління

Для вирішення вищезазначених завдань розроблено спеціалізоване рішення, що включає в себе: інфраструктурна складова: структуровану кабельну систему, сертифіковану за 5-ої категорії, 26 точок Wi-Fi - доступу для формування Wi-Fi - зони; INTEL-сервера інфраструктури та додатків функціонують на базі програмних продуктів Microsoft.

Систему автоматизації готелю, ресторану і розважального комплексу на базі програмного продукту Tillypad, включаючи інтеграцію цих продуктів з бухгалтерською програмою 1С; автоматичною системою контролю фізичного доступу VingCard і системою обробки кредитних карт UCS.

Систему білінгу (обліку) телефонних переговорів і доступу в Інтернет клієнтів комплексу в рамках реалізованої Wi-Fi-зони.

В рамках вирішення використовуються промислові СУБД і серверна операційна система Windows.

Найбільш інтенсивно використовується СУБД SQL 2008 Server Standard, що входить до складу Small Business Server 2008. Вона забезпечує роботу наступних програмних продуктів: комплекс Tillypad, Barsum Pro. Програмний продукт бронювання працює спільно з інстальованою на одному з серверів програмою СУБД Sybase.

Крім того, на базі SQL-сервера працює система моніторингу та управління електронних замків VingCard. З її допомогою забезпечується як доступ для гостей та персоналу в різні приміщення готелю, так і моніторинг пересувань персоналу по готелю, зокрема, відстеження роботи покоївок і т.п.

В рамках вирішення реалізований подвійний рівень захисту даних, що зберігаються:

1 Засобами Windows проводиться регулярне архівування даних файлової

структури серверів;

2 Впроваджено «віддзеркалення» жорстких дисків серверів, а також періодичне резервування даних SQL-сервера.

Крім того, з метою забезпечення безпечної роботи серверів і комплексу в цілому, розгорнута система антивірусного захисту на базі програмного продукту Panda Antivirus Business Secure.

Основні блоки управління готелем, що входять до складу автоматизованого комплексу «Схід» зазначені на рисунку 2.2.

Системи будуються в архітектурі клієнт-сервер.

Рисунок 2.2 - Основні блоки управління готелем, що входять до складу автоматизованого комплексу бронювання

На центральному сервері системи зберігається вся інформація коли-небудь занесена в систему. По периметру розташовуються робочі місця користувачів. На малюнку вонизіставлені конкретним відділам, а кількість робочих місць в кожному відділі встановлюється за необхідності. Стрілками показані основні інформаційні потоки, що протікають між робочими станціями та сервером. Основні інформаційні потоки та інформація

циркулююча в організації готельного бізнесу наведені в таблиці 2.5.

Ефективність впровадження автоматизованої інформаційної системи залежить від цілого комплексу скоординованих заходів щодо перегляду сформованих методів і порядку роботи ,як працівників так і автоматизованих систем, перепідготовки персоналу, розробці та втіленню інформаційно-технологічної стратегії підприємства.

Таблиця2.5. Основніінформаційні потоки в готелі

Служба	Потік	Інформація
Портьє	введення даних про заїздах; розміщення гостей; поточна робота з клієнтом (внесення інформації про користування послугами, переселення з номера в номер)	інформація про майбутні заїздах і виїздах; інформація про наявність місць у готелі; інформація про стан рахунків гостей
Ресторан	інформація про зміну вартості тих чи інших стандартних типів або страв, або інших послуг, що надаються рестораном	інформація про кількість і тип замовлених пансіонів на найближчі дні
Телефонна довідкова служби	повна інформація про здійснені дзвінки та їх вартості з одночасним включенням	інформація про відкриття / закриття певного класу телефонного доступу в
Кіоски	інформація про запит клієнтом тих чи інших послуг	інформація про надані послуги, про їх вартість та оплату
Покоївки	інформація про заїзд і виїзд; передача повідомлень для клієнтів; сервісні функції	інформація про стан номера
Комерційний відділ	зміна цін, видів послуг, надання знижок для тих чи інших туроператорів, груп або індивідуалів, категорій туристів, встановлення квот по завантаженню та порядку поселення при овербукинг і т.д.	статистична інформація з можливістю аналізу за різними критеріями або групі критеріїв (соціальний статус, бажані види послуг, мета поїздки і т. п.)
Відділ бронювання	резервування з зазначенням статусу (тимчасове, постійне; можлива і більш детальна градація), кількості та типу замовляються номерів,	інформація про поточне завантаження і кількості броні на майбутнє, автоматична друк підтверджень по броні

	інформації про групу (тип, стать, вік та ін.), час прибуття та від'їзду, можливих замовлені послуги та ін .; інформація про внесення депозитів за бронь	
Бухгалтерія	інформація про всі платежі (вид платежу, хто, коли, від кого і за що прийняв), отриманих усіма службами і її збереження протягом заданого періоду; зведення бухгалтерських проводок за звітний період (зміна, бізнес-день, тиждень, місяць і т.д.)	виставлення рахунків клієнтам; зміна (спільно з відділом маркетингу) розцінок на ті чи інші готельні послуги; зміна різних коефіцієнтів, процентних ставок і т.п.

2.7 Оцінка ризиків впровадження комп'ютерної системи управління

Фірма розглядає інвестиційний проєкт з впровадження інформаційної системи. У процесі попереднього аналізу експертами були виявлені три ключові параметри проєкту та визначено можливі межі їх змін (таблиця 2.6). Інші параметри проєкту вважаються постійними величинами (таблиця 2.7).

Таблиця 2.6 – Ключові параметри проєкту

Показники	сценарій		
	найгірший	найкращий	ймовірний
Кількість поселень - Q	1000	1300	1200
Середня сума доходу - P	14,0	15,5	15,0
Змінні витрати - V	13,5	12,5	13,0

Таблиця 2.7 – Незмінні параметри проєкту

Показники	Найбільш ймовірне значення
Постійні витрати - F	75,0
Амортизація - A	15,0
Податок на прибуток - T	60%
Норма дисконту - r	20%

Термін проєкту - n	10
Початкові інвестиції - I_0	250,0

Першим етапом аналізу є визначення залежності результуючого показника від вихідних. Використовуваним критерієм є чиста сучасна вартість проєкту NPV,

ДеNCFt - величина чистого потоку платежів у періоді t .

Ключовими варійованими показниками є змінні витрати, обсяг випуску і ціна. Діапазони можливих змін варійованих показників наведені в таблиці При цьому виходимо з припущення, що всі ключові змінні мають рівномірний розподіл ймовірностей.

Для підтвердження економічної ефективності впровадження даної системи було проведено імітаційним експеримент в середовищі EXCEL за допомогою вбудованих функцій. Бачимо, що за результатами імітаційного аналізу ризик проєкту дуже низький, тобто, можемо застосувати автоматизований комплекс бронювання для готелю. Але за допомогою цього комплексу ми можемо виконати тільки частину поставлених задач, яка стосується безпеки і комфорту клієнтів готелю та роботи бухгалтерії. Невирішеними залишаються задачі регулювання доступу до даних з метою забезпечення цілісності конфіденційної інформації, стосується даних про клієнтів, співробітників, постачальників відомості про окремі фінансові показники, про систему ділових зв'язків, дані по кадрам, відомості про організацію охорони та протипожежної безпеки і т.п. Вирішити ці проблеми пропоную за рахунок активу «Паролі співробітників» (методика розроблена компанією Microsoft), який є значним та важливим для будь-якого підприємства цього класу, в незалежності від розміру та послуг, які надає компанія. Активи цього типу є в кожній компанії, їх можливо розглядати як універсальні, тобто в незалежності від послуг (мобільний зв'язок, Інтернет послуги, послуги цифрового телебачення), які надає компанія. Цей актив також був обраний, тому що має великий вплив на діяльність об’єкту в

цілому.у випадку якщо паролі будуть змінені шкідливою програмою, що призведе до відсутності доступу співробітників до продуктивних систем, таких як ІС бізнес-процесів та операційних процесів оператору зв'язку (клієнта).

Формалізований опис активу наведений у таблиці 2.8.

Таблиця 2.8 – Опис активу

Клас активу	Загальне середовище	Назва активу	Рівень вартості активу
Матеріальний	Дані інтрамережі	Паролі співробітників	5

На першому етапі потрібно визначити активи організації, для яких будуть визначатися ризики та проводитися управління цими ризиками. В якості приклада, був обраний актив «Паролі співробітників». Далі починається опис цього активу, та збір інформації про нього. Інформацію поступово, при отриманні нових даних, потрібно заносити у шаблон збору даних. Не завжди є змога заповнити шаблон одразу, при відсутності достатніх даних, тому внесення інформації відбувається при надходженні нових даних або при збільшенні ступеня деталізації ризиків та активів.

Далі потрібно визначити загрози та вразливості, рівень схильності до впливу та рівень впливу, а також виявлення існуючих елементів контролю. Для визначення цих показників, збирається група співробітників компанії, які мають відношення до цього активу, тобто використовують його в своїй щоденній праці, також можливо залучати зовнішніх експертів, які можуть надати якісну оцінку показників, та допомогти з встановленням загроз та вразливостей.

Для визначення схильності активу до впливу, активи можливо розрізняти на наступні групи:

- висока схильність до впливу. Значний або повний збиток для активу;
- середня схильність до впливу. Середній або обмежений збиток;
- низька схильність до впливу. Незначний збиток або його відсутність.

Для обраного активу, при визначених загрозах та вразливостях

встановлені рівні схильності до впливу, які наведені у таблиці 2.9 (для подальшого спрощення надання інформації, пари «загроза-вразливість», які відповідають кожному окремому ризику, буде пронумеровано, як 1, 2 і т.д.):

Останньою задачею тематичного збору даних є аналіз інформації, отриманої під час розгляду ризиків. Результатом аналізу є перелік формулювань, які характеризують активи та їх потенційну схильність до загроз та вразливостей. Зібрана інформація заноситься у таблицю «Основна інформація о ризиках». Для створення формулювань впливу використовуються дані з таблиці «Шаблон збору даних».

Наступним етапом є пріоритезація ризиків. На цьому етапі до формулювання впливу додається формулювання вірогідності. При повному формулюванні ризику вказується як вплив на організацію, так і вірогідність виникнення відповідного впливу. Цей етап розділяється на дві стадії – процес на узагальненому рівні та процес на рівні деталізації. Це робиться для зменшення витрат часу на пріоритезацію, та створення можливості спочатку виділити значні ризики, а потім зробити їх деталізацію.

Таблиця 2.9 – Рівні схильності до впливу

Ризик	Загрози	Вразливості	Рівень
1	2	3	4
1	Отримання паролів за рахунок отримання несанкціонованого доступу до них внутрішніми зловмисниками (співробітниками тієї ж компанії)	Викрадення паролів співробітником компанії, шляхом підслуховування, соціальної інженерії або інших методів, без використання технічних засобів	Високий, тому що в працюють молоді люди, що призводить до збільшення вірогідності отримання інформації за допомогою соціальної інженерії
2	Отримання паролів за рахунок отримання несанкціонованого доступу до них внутрішніми зловмисниками (співробітниками тієї ж компанії)	Викрадення паролів при відсутності блокування працюючої системи	Середній, тому що на ПК встановлені системи автоматичного блокування сеансу при бездіяльності, та процес блокування закріплений в політиці безпеки, яку підписує кожний співробітник

3	Отримання паролів за рахунок отримання несанкціонованого доступу до них внутрішніми зловмисниками (співробітниками тієї ж компанії)	Викрадення паролів за допомогою використання шкідливого програмного забезпечення (віруси)	Низький, тому що доступ до зовнішньої мережі обмежений, постійно оновлюється антивірусне забезпечення, USB-хости блоковані
4	Отримання паролів за рахунок отримання несанкціонованого доступу до них зовнішніми зловмисниками	Передавання паролів у відкритому вигляді	Середній, тому що доступ до мережі обмежений, важлива інформація передається з використанням шифрованого протоколу
5	Отримання паролів за рахунок отримання несанкціонованого доступу до них зовнішніми зловмисниками	Недостатня обізнаність персоналу у питаннях інформаційної безпеки	Середній, недостатня обізнаність в питаннях ІБ може призвести до використання паролів за межами організації, зберігання за межами організації, проте отримання пароля таким шляхом, не буде вест до значного впливу, тому що потрібен ще доступ до внутрішніх ІС
6	Компрометації паролів доступу	Порушення персоналом правил зберігання паролів	Високий, тому що паролі можуть бути збережені на папері, або зберігатися на електронній скрині у відкритому вигляді, в компанії відсутнє обов'язкове використання менеджерів паролів

На узагальненому рівні використовується інформація отримана у процесі збору даних, з таблиць «Шаблон збору даних» та «Основна інформація о ризиках», та проводиться встановлення рівня впливу та оцінка вірогідності на узагальненому рівні.

Для встановлення рівня впливу поєднуються відомості о класі активу та о рівні схильності до впливу, приклад зіставлення цих величин наведений у таблиці 2.10.

Отримані результати заносяться у таблицю «Основна інформація о ризиках».

Наступний кроком є встановлення рейтингу вірогідності, за допомогою експертних оцінок або зовнішньої інформації, отриманої від статистичних центрів. Також можливо використовувати таблицю 2.11.

Таблиця 2.10 – Рівні впливу

	Рівні впливу			
Клас активу	Вис.	Середн.	Вис.	Вис.
	Середн.	Низьк.	Середн.	Вис.
	Низьк.	Низьк.	Низьк.	Середн.
		Низьк.	Середн.	Вис.
		Рівеньсхильності		

Таблиця 2.11 – Категорії вірогідності

Якісна оцінка	Опис
Висока	Ймовірно виникнення одного або більше наслідків протягом одного року
Середня	Вплив може виникнути хоча б раз протягом двох або трьох років
Низька	Виникнення впливу протяг трьох років маловірогідне

Для встановлених пар «загроза-вразливість», на основі існуючої інформації о діяльності підприємства можливо визначити вірогідності, як наведено у таблиці 2.12.

Таблиця 2.12 – Вірогідність вразливості

Риз-ик	Загрози	Вразливості	Вірогідність
1	2	3	4
1	Отримання паролів за рахунок отримання несанкціонованого доступу до них внутрішніми зловмисниками (співробітниками тієї ж компанії)	Викрадення паролів співробітником компанії, шляхом підслуховування, соціальної інженерії або інших методів, без використання технічних засобів	Висока, тому що працівники відділу працюють в одному приміщенні, мають дружні відносини, що збільшує можливість використання соціальної інженерії

2	Отримання паролів за рахунок отримання несанкціонованого доступу до них внутрішніми зловмисниками (співробітниками тієї ж компанії)	Викрадення паролів при відсутності блокування працюючої системи	Середня, тому що на ПК встановлені системи автоматичного блокування сеансу при бездіяльності, проте блокування відбувається не одразу, а через певний проміжок часу, що дає змогу зловмиснику
3	Отримання паролів за рахунок отримання несанкціонованого доступу до них внутрішніми зловмисниками (співробітниками тієї ж компанії)	Викрадення паролів за допомогою використання шкідливого програмного забезпечення (віруси)	Низька, тому що доступ до зовнішньої мережі обмежений, постійно оновлюється антивірусне забезпечення, USB-хости блоковані, потрапляння вірусів у систему маловірогідне
4	Отримання паролів за рахунок отримання несанкціонованого доступу до них зовнішніми зловмисниками	Передавання паролів у відкритому вигляді	Середня, тому що доступ до мережі обмежений, важлива інформація передається з використанням шифрованого протоколу, але листування не здійснюється у зашифрованому вигляді
5	Отримання паролів за рахунок отримання несанкціонованого доступу до них зовнішніми зловмисниками	Недостатня обізнаність персоналу у питаннях інформаційної безпеки	Висока, недостатня обізнаність в питаннях ІБ може призвести до використання паролів за межами організації, зберігання їх за межами організації
6	Компрометації паролів доступу	Порушення персоналом правил зберігання паролів	Висока, тому що паролі можуть бути збережені на папері, або зберігатися на електронній скрині, в компанії відсутнє обов'язкове використання менеджерів паролів, що може призвести до потрапляння паролів до внутрішніх та зовнішніх зловмисників

Отримавши інформацію про вірогідність та рівні впливу, використовуючи Рис. 2.3, можливо визначити рівні ризику.

Рівні в списку з узагальненими відомостями о ризиках

Вплив	Вис.	Середн.	Вис.	Вис.
	Середн.	Низьк.	Середн.	Вис.
	Низьк.	Низьк.	Низьк.	Середн.
		Низьк.	Середн.	Вис.
		Рівень вірогідності		

Рисунок 2.3 – Підсумковий рівень ризику

Таким чином отримана інформація о ризиках на узагальненому рівні. При необхідності можливо додати до таблиці стовбці з допоміжною інформацією, наприклад додатковий опис ризиків або виділяти будь які зміни при ризиків, які виникли після попередньої оцінки.

Наступною задачею пріоритезації є вивчення отриманих узагальнених результатів, з ціллю визначити ризики, які потребують деталізації. До цих ризиків можливо віднести ризики, за наступними критеріями:

– ризики високого рівня. До переліку на рівні деталізаціїнеобхідно включити всі ризики високого рівня. В процесі підтримки прийняття рішень для кожного ризику повинно бути прийнято окреме рішення (наприклад, чи вважати ризик допустимим або розробляти рішення по його нейтралізації);

– граничні ризики. Спочатку виконується детальний аналіз пріоритетів для ризиків середнього рівня, які необхідно знижувати (детальний перелік може включати всі ризики середнього рівня);

– суперечливі ризики. Якщо ризик є новим і знань про цей ризик недостатньо або різні зацікавлені особи оцінюють цей ризик по-різному, тоді потрібно виконувати детальний аналіз цього ризику, щоб краще зрозуміти цей ризик.

На основі цих критеріїв та отриманих узагальнених результатів, детального аналізу потребують усі ризики, окрім ризику номер три – викрадення паролів за допомогою використання шкідливого програмного забезпечення, так як його рівень встановлений як низький.

При аналізі ризиків на деталізованому рівні, використовуються дані які були отримані при складанні переліку ризиків на узагальненому рівні, але при більш детальному аналізі потрібно отримати більш конкретний опис впливу та вірогідності. Для деталізованої оцінки ризику потрібно виконати наступні чотири етапи:

1) визначення величини впливу та схильності до впливу;
2) визначення поточних елементів контролю;
3) визначення вірогідності впливу;
4) детальне визначення рівня ризику.

На етапі визначення впливу та схильності до впливу, в таблицю «Детальна оцінка ризику» спочатку заноситься інформація про клас активу, отримана на етапі узагальненого аналізу ризиків. Далі заноситься інформація про схильність активу до впливу, при цьому схильність вказується більш точно, ніж на узагальнено етапі оцінки ризиків, та вказується в діапазоні від 1 до 5. Для визначення рівня схильності до впливу , потрібно обрати найбільшу величину впливу між двома значеннями – впливу порушення конфіденційності або цілісності активу, чи впливу на доступність активу. Інформація про рівні схильності до впливу відповідно наведена у таблицях: 2.13 та 2.14.

Проаналізувавши схильність до впливу можливо встановити наступні рівні:

– викрадення паролів за рахунок отримання несанкціонованого доступу до них внутрішніми зловмисниками (співробітниками тієї ж компанії) ;

встановлено 4 рівень, так як отримання паролів внутрішніми зловмисниками може призвестидо значного впливу на актив, але не призводить до його втрати або знищення;

Таблиця 2.13 – Рівень схильності до впливу для конфіденційності та цілісності активу

Рівні схильності до виливу	Конфіденційність або цілісність активу
1	Суттєві пошкодження або повний вихід із ладу активу (наприклад, видимі зовні и впливаючи на прибутковість або успішність ведення бізнесу)
2	Суттєві пошкодження, які не приводять до повному виходу з ладу активу (наприклад, які впливають на прибутковість або успішність ведення бізнесу та, можливо, які помітні зовні)
3	Суттєві пошкодження або шкода (наприклад, які впливають на внутрішні рекомендації по веденню бізнесу та спосібні викликати збільшення експлуатаційних витрат або зменшення прибутку)
4	Незначні пошкодження або шкода (наприклад, які впливають на внутрішні рекомендації по веденню бізнесу, але не викликають суттєвого зросту витрат)
5	Незначні зміни в активі або відсутність змін

– викрадення паролів за рахунок отримання несанкціонованого доступу до них зовнішніми зловмисниками – встановлено 4 рівень, так як отримання паролів внутрішніми зловмисниками може призвести до значного впливу на актив, але не призводить до його втрати або знищення;

– компрометації паролів доступу ;

– встановлено 5 рівень, пароль можуть отримати як зовнішні, так і внутрішні зловмисники, доступ до місця зберігання паролів може призвести до повної їх втрати.

Згідно з відношенням класу активу до значення класу впливу, відповідність яких наведена у рисунку 2.4, та визначеним рівнем схильності до впливу – обирається рівень впливу.

Таблиця 2.14 – Рівень схильності до впливу для доступності активу

Рівні схильності до виливу	Дата випуску	Опис
1	Припинення роботи	Великі експлуатаційні витрати або порушення комерційних обов'язків
2	Переривання роботи	Значне збільшення експлуатаційних витрат або затримка при виконанні комерційних обов'язків
3	Затримки в роботі	Помітний вплив на величину експлуатаційних витрат та продуктивність
4	Відволікання від роботи	Вимірний вплив на діяльність компанії відсутній; незначне збільшення експлуатаційних витрат або витрат на інфраструктуру
5	Не впливає на звичайний хід бізнес-операцій	Вимірний вплив на експлуатаційні витрати, продуктивність та комерційні обов'язків відсутні

Клас впливу	Значення класу впливу (З)
ВВБ	10
СВБ	5
НВБ	2

Рівень схильності до впливу	Фактор схильності до впливу (ФСВ)	Рівень впливу (З*ФСВ)	Діапазон впливу	Узагальнене порівняння
5	100%		7 - 10	Вис.
4	80%		4 - 6	Середн.
3	60%		0 - 3	Низьк.
2	40%			
1	20%			

Рисунок 2.4-Визначення величин впливу

Вся отримана інформація у результаті аналізу ризиків, на цьому етапі заноситься в таблицю «Детальна оцінка ризику», де й наведені отримані результати.

Наступним етапом є визначення існуючих елементів контролю. Елементи контролю можуть бути визначені на етапі збору даних, якщо ж це не зроблено на початку, то для кожної пари «загроза-вразливість» будуть розглянуті поточні елементи контролю, якщо вони є. Визначені елементи наведені у таблиці 2.15.

Наступним етапом визначається вірогідність впливу, на основі двох значень.

Таблиця 2.15 – Поточні елементи контролю

Загрози	Вразливості	Поточні елементи контролю
1	2	3
Отримання паролів за рахунок отримання несанкціонованого доступу до них внутрішніми зловмисниками (співробітниками тієї ж компанії)	Викрадення паролів співробітником компанії, шляхом підслуховування, соціальної інженерії або інших методів, без використання технічних засобів	Проведення навчання по ІБ, початкового рівня, при працевлаштуванні
Отримання паролів за рахунок отримання несанкціонованого доступу до них внутрішніми	Викрадення паролів при відсутності блокування працюючої системи	1 Системи розмежування прав доступу

зловмисниками (співробітниками тієї ж компанії)		2 Автоматичне блокування ПК при бездіяльності системи
Отримання паролів за рахунок отримання несанкціонованого доступу до них зовнішніми зловмисниками	Передавання паролів у відкритому вигляді	1 Використання ssl-протоколів 2 Використання firewall
Отримання паролів за рахунок отримання несанкціонованого доступу до них зовнішніми зловмисниками	Недостатня обізнаність персоналу у питаннях інформаційної безпеки	1 Проведення навчання по ІБ, початкового рівня, при працевлаштуванні
Компрометації паролів доступу	Порушення персоналом правил зберігання паролів	1 Політика парольного захисту компанії 2 Проведення навчання по ІБ, початкового рівня, при працевлаштуванні

Перше значення визначає вірогідність існування вразливості, виходячи із атрибутів вразливості та можливості викрадення. Друге значення визначає вірогідність існування вразливості виходячи з ефективності поточних елементів контролю.

Вірогідність існування вразливості визначається на снові наявності інформації про кількість зловмисників, тип доступу, відомість засобів злому, автоматизованість злому. Для кожного ризику визначається вірогідність вразливостей, керуючись інформацією з рисунку 2.5. Отримані результати занесені в таблицю 2.16. На наступному кроці визначаються показники ефективності контролю для кожного ризику, та їх опис, отримані дані наведені у таблиці 2.17.

Визначення вірогідності для вразливостей
Висока
Велика кількість зловмисників - аматори або комп'ютерні хулігани
Віддалене виконання
Можливість використання анонімного доступу
Загальновідомий метод зламування
Автоматизованість
5, якщо виконується хоча б одна з умов
Середня
Середня кількість зловмисників - спеціалісти або експерти
Неможливість віддаленого виконання
Необхідність наявності привілей рівня користувача
Метод зламування не є загальновідомим
Атака не автоматизована
3, якщо виконується хоча б одна з умов
Низька
Невелика кількість зловмисників - необхідна внутрішня інформація
Неможливість віддаленого виконання
Необхідність наявності привілей рівня адміністратора
Метод зламування не є загальновідомим
Атака не автоматизована
1, якщо виконується хоча б одна з умов

Рисунок. 2.5 – Оцінка вразливості

Таблиця 2.16 – Вірогідність існування вразливості

Ризик	Вірогідність
1	атака не автоматизована, для отримання будь-якої інформації потрібне перебування на території підприємства
2	атака не автоматизована, для отримання будь-якої інформації потрібне перебування на території підприємства
4	є можливість віддаленого виконання, атака може бути автоматизована, з використанням програмного забезпечення, яке прискорює збір даних, чим збільшує вірогідність
5	можливість віддаленого виконання
6	велика кількість зловмисників, тому що будь-хто з співробітників має змогу знайти пароль записаний на папері, або віддалено отримати його, якщо представник організації виносить паролі за межі організації, на будь-яких носіях

Таблиця 2.17– Показники ефективності контролю

Ризики	Показник ефективності контролю					Сума атрибутів контролю
	Чи ефективно визначена і реалізована відповідальність?	Чи ефективно здійснюється інформування?	Чи ефективно визначені і реалізовані процеси?	Чи ефективно існуючі технології або елементи контролю знижують загрози?	Чи забезпечують ь існуючі методи аудиту виявлення зловживань і нестачі контролю?	
1	0, в компанії визначена відповідальність	0, при зміні політики або виникненні небезпеки проводиться миттєве інформування	0, в організації є задокументовані процеси з проведення навчання	1, в компанії відсутні достатні елементи для зниження загрози	1, відсутні методи аудиту, які дозволяють миттєво визначати інциденти	2
2	0, в компанії визначена відповідальність за блокування сеансу	0, при змінах технологій, програмного забезпечення, тощо – миттєво проводиться інформування	0, в організації задокументована та здійснюється відповідність встановленим нормам	1, існуючи системи контролю, залишають час для несанкціонованого доступу до системи	0, існуючи засоби ефективно здійснюють вимір та аудит відповідності	1
4	0, в компанії визначена відповідальність за безпечну передачу даних	1, інформування користувачів про безпечну передачу даних постійно не проводяться	0, в організації задокументована та здійснюється відповідність встановленим нормам	0, існуючи системи забезпечення безпечної передачі даних достатні	0, існуючи засоби ефективно здійснюють вимір та аудит відповідності	1

5	0, в компанії визначена відпові-дальність	1, в компанії не відбувається постійного навчання з питань інформаційної безпеки	0, в організації задокументова на та здійснюється відповідність встановленим нормам	1, в компанії відсутні достатні елементи для зниження загрози	1, відсутні методи аудиту, які дозволяють миттєво визначати інциденти	3
6	0, в компанії визначена відпові-дальність за безпечне зберігання паролю	1, в компанії не відбувається постійного навчання з питань інформаційної безпеки	0, в організації задокументова на та здійснюється відповідність встановленим нормам	0, в компанії е парольна політика, яка постійно оновлюється	0, існуючи засоби ефективно здійснюють вимір та аудит відповідност і	1

Так – 0, Ні – 1. Менший результат означає більшу ефективність елементів контролю та їх здатність зменшити вірогідність порушення ІБ.

Для закінчення якісного розділу ризиків, потрібно визначити рівень кожного ризику, який встановлюється на основі рівня впливу та рівня вірогідності, та є добутком цих значень. Отримані результати рівня ризику можливо ранжувати на якісному рівні, застосовуючи ті ж правила, що й на узагальненому рівні, тобто деталізований рівень ризику можливо охарактеризувати як високий, середній та низький. Таким чином рівень ризику, можливо охарактеризувати, як на рисунку 2.6.Отримані результати заносяться у таблицю «Детальні оцінки ризику». З отриманих результатів та відповідно даним з рисунку 2.6, можливо встановити якісні рівні ризику, результат наведений у таблиці 2.18.

Наступним етапом аналізу ризиків, є кількісна оцінка ризиків. Грошова оцінка буде корисною при визначенні затрат на різні стратегії нейтралізації ризиків.

Рівень впливу * Рівень вірогідності = Рівень ризику			
Діапазон рівня впливу		*	Діапазони вірогідності
Високий	10 -- 7		10 -- 7
Середній	6 -- 4		6 -- 3
Низький	3 -- 0		3 -- 0

Загальний	Рівень ризику
41-100	Високий
20-40	Середній
0-19	Низький

Рисунок 2.6 – Результуюче якісне ранжування

Таблиця 2.18 – Рівень ризику

Ризик	Рівень ризику
1	Середній
2	Середній
4	Високий
5	Високий
6	Високий

Для визначення кількісних характеристик, потрібно виконати наступні задачі:

– задача 1. Зіставити кожному класу активів в організації грошову вартість;

– задача 2. Визначити вартість активу для кожного ризику;

– задача 3. Визначити величину очікуваного разового збитку;

– задача 4. Визначити щорічну частоту виникнення;

– задача 5. Визначити очікуваний річний збиток.

На етапі визначення грошової вартості кожного активу, з точки зору його матеріальної та нематеріальної цінності для компанії, розраховують загальну вартість впливу для кожного активу, використовуючи наступні категорії:

– вартість заміни;

- витрати на обслуговування і підтримку працездатності;
- витрати на забезпечення надмірності та доступності;
- репутація організації (репутація на ринку);
- ефективність роботи організації;
- річний дохід;
- конкурентна перевага;
- внутрішня ефективність експлуатації;
- правова та регулятивна відповідальність.

Визначив грошові оцінки для кожної категорії, потрібно їх скласти для визначення загальної оцінку активу.

Інформацію про вартість активу, можливо отримати у відділу управління фінансовими ризиками. Також можливо використовувати рекомендації, щодо визначення суттєвості в фінансових звітах, згідно з вимогами «Ради по стандартам фінансового обліку США» (FASB). Сутність цих рекомендацій полягає в визначенні суттєвості класу активів ВВБ, із розрахунку 5% від чистого доходу компанії. Для спрощення отримання результату відповідності вартості активу, буде використано цей спосіб. Чистий дохід компанії, яку ми обрали за прикладом може становити приблизно 1.5 млн.грн. (дані на 2012 рік), складає 500 млн. грн. З урахуванням рекомендацій FASB, активам класу ВВБ була зіставлена вартість 1,5 млн. грн. Після отримання певного опиту, ці показники будуть переглянуті

Наступним кроком є визначення вартості активу, таким чином з урахуванням встановленої вартості класу активу ВВБ, вартість активу «Паролі співробітників», складає 1,5 млн. грн.

Наступною задачею є визначення ступеня збитку, який може бути завданий активу. Для його визначення використовується рівень схильності до впливу, встановлений на попередніх етапах, це значення зветься фактором схильності впливу. Для визначення ОРаЗ, яка є кількісною оцінкою впливу, потрібно помножити вартість активу на фактор схильності до впливу. Отримані результати наведені в таблиці 2.19.

Таблиця 2.19 – Очікуваний разовий збиток

Ризик	Значення класу активу	Рівень схильності впливу	Величина схильності впливу	ОРаЗ
1	2.5 млн. грн.	4	80%	0.8 млн. грн.
3	2.5 млн. грн.	4	80%	0.8 млн. грн.
4	2.5 млн. грн.	4	80%	0.8 млн. грн.
5	2.5 млн. грн.	4	80%	0.8млн. грн.
6	2.5 млн. грн.	5	100%	1 млн. грн.

Після визначення ОРаЗ необхідно визначити вірогідність збитку, для закінчення грошової оцінки ризику. Для того щоб охарактеризувати цю вірогідність використовується поняття щорічної частоти виникнення. Щоб отримати оцінку вірогідності, використовується якісний підхід, розглянутий раніше. Для спрощення визначення та передачі кількісної оцінки ЩЧВ, можливо використати відповідні дані з рисунку 2.7.

Якісний рівень	Опис	Діапазон щорічно частоти виникнення	Приклади описів
Високий	Дуже вірогідно	>= 1	Вппиває раз на рік або частіше
Середній	Вірогідно	.99 to .33	Не менш ніж раз кожні 1-3 роки
Низький	Маловірогідне	< .33	Менше ніж один раз на 3 роки

Рисунок 2.7 – Кількісна оцінка ЩЧВ

За допомогою отриманої інформації на попередніх етапах та інформації з рисунка 2.7, були визначені наступні ЩЧВ, які наведені у таблиці 2.20.

Таблиця 2.20 – Щорічна частота виникнення

Ризик	Якісний рівень	ЩЧВ	Опис вибору
1	Середній (5)	0,5	Використовуючи якісну оцінку середнього рівня вірогідності, було визначено, що даний ризик може виникати один раз протягом двох років або частіше

2	Середній(4)	0,36	Використовуючи якісну оцінку середнього рівня вірогідності, було визначено, що даний ризик може виникати один раз протягом трьох років або частіше
4	Середній (6)	0,66	Використовуючи якісну оцінку середнього рівня вірогідності, було визначено, що даний ризик може виникати двічі протягом трьох років або частіше
5	Високий (8)	1	Використовуючи якісну оцінку високого рівня вірогідності, було визначено, що даний ризик може виникати один раз на рік або частіше
6	Середній(6)	0,66	Використовуючи якісну оцінку середнього рівня вірогідності, було визначено, що даний ризик може виникати двічі протягом 3 прків.

Для завершення кількісної оцінки ризику, потрібно отримати значення очікуваного річного збитку, який є добутком ОРаЗ та ЩЧВ, як наведено у формулі 2.1.

$$ОРіЗ=ОРаЗ\times ЩЧВ \quad (2.1)$$

Розрахунок ОРіЗ, та отримані результати наведені у таблиці 2.21. Отримані дані заносяться у таблицю «Детальна оцінка ризику».

Таблиця 2.21 – Очікуваний річний збиток

Ризик	Значення класу активу	Рівень схильності до впливу	Величина схильності до впливу	ОРаЗ	ЩЧВ	ОРіЗ
1	2.5 млн. грн.	4	80%	0.8 млн. грн.	0,5	0.4 млн. грн.
2	2.5 млн. грн.	4	80%	0.8 млн. грн.	0,36	0.28 млн. грн.
4	2.5 млн. грн.	4	80%	0.8 млн. грн.	0,66	0.52 млн. грн.
5	2.5 млн. грн.	4	80%	0.8 млн. грн.	1	0.8 млн. грн.
6	2.5 млн. грн.	5	100%	0.8 млн. грн.	0,66	0.52 млн. грн.

Етап оцінки ризиків, один з етапів циклу управління ризиками, необхідний для управління ризиками в рамках об’єкта. Виконуючи

планування, координований збір даних для пріоритизації, визначено, що етап оцінки ризиків покликаний не тільки виявити ризики і визначити їх пріоритети, а й забезпечити виконання цих завдань у стислі терміни і з максимальною ефективністю. Процес управління ризиками безпеки, пропонований корпорацією Майкрософт, використовує комбінований підхід, який базується на застосуванні якісного аналізу для швидкого пошуку ризиків та виявлення найбільш суттєвих з них і наступному визначенні ризиків за допомогою фінансових атрибутів, отриманих в ході кількісного аналізу.

Так як метою цього проєкту є не детальне визначення ризиків та управління ними, для існуючого підприємства, а наведення прикладу управління ризиками, то після повної оцінки ризиків, було обрано лише один ризик, для подальшого управління ним ризик 5: отримання паролів зовнішніми зловмисниками, за рахунок недостатньої обізнаності персоналу у питаннях ІБ.

Наступним етапом управління ризиків є процес підтримки прийняття рішень, який включає формальний аналіз вигод і витрат з визначенням ролей і обов'язків в межах підприємства. На етапі підтримки прийняття рішень необхідно визначити найбільш результативні і економічно ефективні заходи протидії основним ризикам безпеки. Кінцевим результатом даного процесу є розробка чітких планів, що дозволяють зменшити, прийняти, передати або усунути кожен з основних ризиків, виявлених в ході оцінки ризиків. Етап підтримки прийняття рішень включає наступні шість кроків:

1) визначення функціональних вимог;

2) вибір можливих рішень для контролю;

3) перевірка відповідності рішень вимогам;

4) оцінка рівня зниження ризику, забезпечуваного застосуванням кожного рішення для контролю;

5) оцінка вартості кожного рішення;

6) вибір стратегії нейтралізації ризику.

Було встановлено, що одним з найбільш пріоритетних ризиків для основних активів організації є отримання паролів зовнішніми зловмисниками,

за рахунок недостатньої обізнаності персоналу у питаннях ІБ. Найбільш ефективним засобом, що дозволяє зменшити використання паролів при перевірці достовірності є застосування двохфакторної перевірки автентичності, наприклад з використанням смарт-карт. Так як в готелі працює багато співробітників, то вартість реалізації буде досить високою, але обґрунтованою, проте програми, які діють в готелі, використовують систему перевірки справжності на основі паролів та внесення змін у ці програми або їх заміна приведуть до дуже великих витрат і будуть потребувати декілька років. В результаті найбільш ефективним рішенням є відмова від використання смарт-карт для всіх співробітників, проте необхідно ввести обов'язкове використання смарт-карт при перевірці достовірності керівників, працівників, що володіють істотними правами або мають доступ до важливих даних.

Наступним кроком є визначення функціональних вимог, які являють собою формулювання, які описують елементи контрою, необхідні для нейтралізації ризиків. Функціональні вимоги повинні бути визначені для кожного ризику, розглянутого в процесі підтримки прийняття рішень. Функціональні вимоги для досліджуваного ризику, були сформульовані таким чином: «при вході користувачів у системи необхідна перевірка автентичності із застосуванням двох або більше факторів». Інформація про визначені функціональні вимоги, потрібно занести у стовпчик «Функціональні вимоги до безпеки» в таблиці «Детальна оцінка ризиків».

Наступним кроком етапу підтримки прийняття рішень, є визначення нових потенційних елементів контролю для кожного ризику. Існує два підходи, які можуть допомогти в пошуку нових ідей. Перший підхід полягає в організації неформальних мозкових штурмів, а другий є більш формальним і ґрунтується на класифікації та впорядкуванні елементів контролю. Можливо використовувати обидва ці підходи. Елементів контролю може бути запропоновано декілька варіантів. Наступним кроком аналізуються запропоновані елементи контролю, на відповідність функціональним вимогам.

Відомості про визначені елементи контролю, потрібно внести до таблиці «Детальна оцінка ризиків».

Наступним кроком визначається оцінка зниження ризику. Після вибору способу нейтралізації ризику, потрібно повторно визначити загальне зниження ризику для організації. Використовуючи засоби, розглянуті раніше було встановлене що рівень впливу залишається не змінним і дорівнює 8. Для визначення рівня вірогідності потрібно встановити новий рівень вірогідності існування вразливості та показники ефективності контролю, отримані результати наведені в таблиці 2.22 та таблиці 2.23 відповідно.

Таблиця 2.22 – Нова вірогідність існування вразливості

Ризик	Вірогідність
5	1, атака не автоматизована, для отримання будь-якої інформації потрібне перебування на території підприємства, відсутня можливість віддаленого виконання, необхідність наявності привілей рівня керівника

Таблиця 2.23 – Нові показники ефективності контролю

Ризики	Показник ефективності контролю					Сума атрибутів контролю
	Чи ефективно буде визначена і реалізована відпов-ідальність?	Чи ефективно здійснюється інформування ?	Чи ефективно будуть визначені і реалізовані процеси?	Чи ефективно пропоновані технології або елементи контролю знижують загрози?	Чи забезпечують пропоновані методи аудиту виявлення зловживань і нестачі контролю?	
5	в компанії визначена відпові-дальність	в компанії буде проведено навчання перед впроваджу-нням нової системи, та буде проводитися постійне інформування при будь-яких змінах	0в організації задокументо вана та здійснюється відповідність встановлени м нормам	в компанії будуть встановлені достатні елементи для зниження загрози	будуть використані методи аудиту, які дозволяють миттєво визначати інциденти	0

Згідно отриманим результатам, рівень вірогідності впливу з використанням нових елементів контролю, буде становити 1. Отримана інформація заноситься до таблиці «Детальна оцінка ризиків».

Для визначення нового рівню ризику, з використання нових елементів контролю, потрібно помножити рівень впливу на рівень вірогідності, таким чином було отримано результат 8.

Наступним завданням є визначення відносних витрат на реалізацію елементів контролю. До витрат можливо віднести наступні напрямки:

- витрати на придбання;
- витрати на впровадження;
- витрати на інформування;
- витрати на навчання персоналу;
- витрати на забезпечення зручності та продуктивності;
- витрати на аудит та перевірку ефективності.

Для розрахунку витрат потрібно залучати представників економічних відділів компанії або бухгалтерів для невеликих компаній, де таких відділів не існує. В таблиці наведені категорії витрат та їх опис, за якими виконується розрахунок загального показника витрат на реалізацію елементів контролю. Для розрахунку економічних показників необхідно враховувати масштаб підприємства, показник річного обороту, кількість персоналу і т.п., згідно з якими проводиться вибір елементів контролю для зниження ризиків, приклад вибору наведений у таблиці 2.24.

Таблиця 2.24 – Витрати на реалізацію

Категорія	Опис
Витрати на придбання	Витрати складаються з розрахунку витрат на одну смарт-карту і вартості одного пристрою зчитування. Оскільки тільки супервізорам та керівникам груп потрібно доступ до систем, з використанням смарт-карт,

	загальні витрати складатимуться з суми витрат на смарт-карти та пристрої зчитування, кількості співробітників
Витрати на впровадження	Витрати будуть складатися з вартості послуг консалтингової компанії, яка допоможе впровадити дане рішення.
Витрати на інформування	Для інформування співробітників про зміни будуть використані внутрішні веб-сайти та списки розсилки електронної пошти, тому витрати на інформування про розгортання смарт-карт будуть несуттєвими
Витрати на навчання IT-персоналу	Можливо звернутися в консалтингову компанію для навчання IT-персоналу, що має допомогти при впровадженні нового рішення, ця компанії взначить вартість послуги. Частина IT-співробітників витратить на навчання від 4 до 8 годин робочого часу. Загальні витрати робочого часу на навчання будуть розраховані в грошовому еквіваленті.
Витрати на навчання користувачів	Для навчання співробітників правилам застосування смарт-карт можливо використовувати навчальні матеріали з веб-інтерфейсом, надані постачальником смарт-карт. Вартість навчальних матеріалів входить у вартість устаткування. Кожен співробітник витратить на навчання близько години робочого часу. Загальний збиток від зниження продуктивності праці розраховані в грошовому еквіваленті.
Витрати на забезпечення зручності та продуктивності	Керівництво компанії передбачає, що співробітники витратять близько години робочого часу і ще один з чотирьох користувачів звернеться в службу підтримки для отримання допомоги у використанні смарт-карт. Згідно цим показникам розраховується загальна вартість витрат цієї категорії.

Витрати на аудит та перевірку ефективності	Вартість виконання аудиту та перевірки ефективності нового елемента, визначається відділом ІБ, за перший рік експлуатації.

Отримані результати заносяться до таблиці «Детальна оцінка ризиків».

Наступним значним етапом управління ризиками є реалізація обраних на попередньому етапі елементів контролю. При розробці планів придбання та реалізації рішень з нейтралізації ризику, співробітникам відповідальним за нейтралізацію ризику, необхідно враховувати вимоги всієї ІТ-системи, всього підрозділу або навіть організації в цілому. Елементи контролю, були визначені, та зафіксовані в таблиці «Детальна оцінка ризику». Після виконання цього етапу повинен бути сформований перелік обраних елементів контролю і реалізованих відповідальними за нейтралізацію ризику, а також серія звітів, створених відповідальними за нейтралізацію ризику і де описано хід розгортання обраних рішень для контролю.

Етап оцінки ефективності програми дозволяє формально задокументувати поточний стан ризиків в організації. По мірі проходження циклу управління ризиками даний етап допомагає продемонструвати зниження ризиків до прийнятного рівня в процесі управління ризиками. На цьому етапі використовуються всі дані отримані на попередніх етапах, а саме:

– перелік ранжируваних за пріоритетами ризиків, які необхідно нейтралізувати;

– перелік рішень для контролю, ранжируваних за пріоритетами;

– звіти про розгортання елементів контролю.

На цьому етапі проводиться розробка системи показників ризиків безпеки, яка є важливим засобом, який допомагає інформувати о поточнім стані ризиків в компанії та демонструвати зміни в управлінні ризиками. Також на етапі оцінки ефективності програми, проводиться вимір ефективності контролю, для того щоб з’ясувати, що всі рішення діють належним чином та забезпечують відповідний рівень захисту. Найбільш ефективним методом визначення величини зниження рівня ризику, забезпечуваного елементами

контролю, є безпосереднє тестування. Для виконання подібного тестування можуть використовуватися різні методи, включаючи автоматизовані засоби оцінки вразливостей, оцінку вручну і тестування проникнення.

Для ефективного управління ризиками необхідно, щоб цей процес носив постійний характер в рамках готелю, а не залишився тимчасовим проєктом. Першим етапом повторного виконання циклу управління ризиками є періодична повторна оцінка ризиків. Через певні періоди потрібно повторно використовувати і оновити перелік активів, вразливостей, елементів контролю та іншу інтелектуальну власність, розроблену в ході виконання початкового проєкту з управління ризиками.

Після виконання цього етапу, створюються звіти про поточний профіль ризику. Відповідні основні елементи звітів, наведені в таблиці 2.25.

Таблиця 2.25 – Звіт з оцінки ефективності програми

Інформація, яку необхідно зібрати	Опис
Розглянуті зміни	Звіти з інформацією про заплановані зміни в IT-середовищі
Затверджені зміни	Звіти з інформацією про зміни в IT-середовищі, які повинні бути внесені найближчим часом
Події безпеки	Звіти з докладною інформацією про незаплановані події безпеки, що вплинули на IT-середовище
Загальні характеристики ефективності рішень для контролю	Звіт з загальними даними про зниження рівня ризику рішеннями для контролю
Зміни профілю ризиків організації	Звіт, що показує, яким чином виявлені раніше загрози змінилися внаслідок появи нових загроз, і містить відомості про нові вразливості і зміни в IT-середовищі організації

Система показників ризиків безпеки	Узагальнена система показників, що характеризує поточний профіль ризиків організації

Підсумовуючи все вище сказане в цій частині можемо сформувати організаційну структуру системи забезпечення інформаційноїбезпеки готелю увигляді сукупності наступних рівней:

- рівень 1 керівництво організації.
- рівень 2 підрозділ інформаційноїбезпеки
- рівень 3адміністратористатних и допоміжних засобів захисту (системний адміністратор).
- рівень4 кінцеві користувачі та обслуговуючий персонал.

На першому рівні керівництвом готелю формуються:

- концепція забезпечення іб;
- політика інформаційної безпеки;
- положення про інформаційну безпеку компанії;
- план забезпечення безперервності ведення бізнесу.

На другому рівні Підрозділом Інформаційної безпеки формуються:

- план забезпечення безперервної роботи і відновлення працездатності інформаційної системи в кризових ситуаціях;
- методика проведення повного аналізу та управління ризиками, пов'язаними з порушеннями інформаційної безпеки;
- журнал обліку нештатних ситуацій;
- план захисту інформаційних систем компанії;
- положення про права доступу до інформації;
- інструкція по внесенню змін до списків користувачів і наділення їх повноваженнями доступу до інформаційних ресурсів компанії;
- інструкція щодо внесення змін до складу і конфігурацію технічних і програмних засобів інформаційних систем;
- інструкція адміністратора безпеки мережі;

– аналітичний звіт про проведену перевірку системи інформаційної безпеки;

– вимоги до процесу розробки програмного продукту;

– положення про розподіл прав доступу користувачів інформаційних систем;

– положення з обліку, зберігання і використання носіїв ключової інформації;

– положення про паролі співробітників.

На третьому рівні адміністратором штатних та допоміжних засобів захисту (системний адміністратор) формуються:

– інструкція по роботі співробітників в мережі Інтернет;

– інструкція з організації парольного захисту;

– інструкція з організації антивірусного захисту;

– інструкція користувачеві інформаційних систем по дотриманню режиму інформаційної безпеки;

– інструкція з резервного копіювання інформації;

– інструкція про паролі співробітників.

Програмний комплекс, на якому будуть базуватися всі підсистеми безпеки, повинен бути сумісним з системою управління. Сучасні інформаційно-комп'ютерні бази це апаратно-програмні комплекси з сумісною базою даних. В якості пристрої в управління використовуються комп'ютери зі спеціалізованим програмним забезпеченням.

2.8 Висновок

Результатом проведеної роботи в даному розділі стало визначення найбільш небезпечних загроз які з'являються при функціонуванні підприємства та його ІС, де оброблюється конфіденційна інформація. Після аналізу була побудована типова модель загроз та модель порушника, для цього типу підприємства.

Визначений клас автоматизованої системи до якого відноситься підприємство.

На наступному етапі була розглянута обрана методика управління ризиками інформаційної безпеки готелю, розроблена корпорацією Microsoft. Також було запропоновано використання автоматизованого комплексу керування основними інформаційними потоками готелю.

Були визначені основні етапи управління ризиками ІБ, наведений приклад аналізу ризику для активу, який має великий вплив на бізнес, та є важливим активом – паролі співробітників. Запропоновані рекомендації для успішної реалізації процесу управління ризиками та впровадження системи контролю, яка дозволяє нейтралізувати ці ризики.

На основі організаційної структури готелю сформована синтезована модель управління інформаційною безпекою, яка має чотири рівні.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Мета роботи – обґрунтування економічної ефективності управління інформаційною безпекою підприємств готельного бізнесу України на прикладі готелю "Схід".

В даний час готельна індустрія являє собою галузь з дуже високим рівнем конкуренції. Будь-яка сучасна готель – це складний комплекс функціональних ланок. Від злагодженості роботи цього комплексу залежить успішність існування підприємства на ринку. При зростанні обсягу продажів, з одного боку, і зростаючої конкуренції, з іншого, підвищується значення оперативності в роботі персоналу. Гостро постає необхідність автоматизації більшості робочих місць готельного персоналу. Вирішенням цієї проблеми може стати комплексна система захисту інформації, що досягається застосуванням ефективної моделі безпеки подібної.

В готелі є 49 номерів, з котрих 2 люкса та 47 стандартних. Для обслуговування роботи готелю правують 11 чоловік:

Штат працівників:

Директор – 1 чол.

Служба прийому і розміщення – 2 чол.(правують по змінно)

Кадрова служба – 1 чол.

Служба харчування –2 чол.

Відділ закупок – 1 чол.

Служба обслуговування гостей – 3 чол.

Інженерна служба – 1 чол.

До бази даних клієнтів має доступ:

- Директор, служба прийому і розміщення та кадрова служба.

Заробітна плата персоналу який працює з базою даних клієнтів складає 44500 грн у місяць

(Директор - 6700грн., служба прийому і розміщення - 3500грн, кадрова служба - 4200 грн.).

Загальних дохід готелю за 2021 рік склав 5224000 грн.

3.1 Визначення витрат на проєктування та експлуатацію системи інформаційної безпеки

3.1.1 Розрахунок капітальних витрат

3.1.1.1 Визначення трудомісткості налаштування пароля на комп'ютері готелю "Схід"

Трудомісткість налаштування пароля на комп'ютері готелю розраховується з урахуванням кількості витраченого часу за формулою (3.1) [12]:

$$t = t_o + t_i + t_a + t_c, \text{ люд.-год,} \quad (3.1)$$

де t_o - витрати праці на підготовку та описання поставленої задачі;

t_i - витрати праці на збір потрібної інформації нормативно-правової бази;

t_a - витрати на аналіз та обробку інформації;

t_c - витрати на створення основних елементів консультаційної системи.

В даному питанні важливу роль відіграє нормування в якості одного з основних елементів організації заробітної плати.

Оцінка витрат праці на підготовку й опис завдання визначається на підставі експертної оцінки. У даному випадку t_o=2 люд.-год.

Приблизна кількість різноманітних складових системи розраховується за формулою: (3.2)

$$Q = q \cdot c, \quad (3.2)$$

де q - передбачувана кількість настроювань;

c - коефіцієнт складності роботи (змінюється в діапазоні 1,25...2,0).

Приблизна кількість потрібної пошукової інформації дорівнює 50, коефіцієнт складності роботи 1,25.

$$Q = 50 \cdot 1{,}25 = 62{,}5$$

Витрати праці на збір потрібної інформації нормативно-правової бази розраховуються за формулою:

$$t_i = t_{др} + t_{до}, \quad \text{люд.-год.} \qquad (3.3)$$

де $t_{др}$ - трудомісткість пошуку матеріалів;

$t_{до}$ - трудомісткість редагування та оформлення знайденої інформації.

$$t_{др} = \frac{Q}{(15...20)k}, \text{люд.-год,} \qquad (3.4)$$

де k-коефіцієнт кваліфікації співробітника, обумовлений у залежності від стажу роботи на даній посаді або від спеціальності за фахом.

Він складає при стажі роботи, років:

до 2 - 0,8;

від 2 до 3 - 1,0;

від 3 до 5 - 1,1...1 ,2;

від 5 до 7 - 1,3...1,4;

понад 7 - 1,5...1 ,6.

Для усіх подальших розрахунків значення в дужках, наприклад, в цьому випадку (15...20), обирається з урахуванням суміжного коефіцієнту.

В нашому випадку коефіцієнт кваліфікації робітника складає k=0,8, оскільки освіта отримана за фахом (формула 3.4):

$$t_{др} = \frac{62,5}{15 \cdot 0,8} = 5,00 \text{ люд.-год.}$$

$$t_{до} = 0,75 \cdot t_{др}, \quad \text{люд.-год.} \qquad (3.5)$$

$$t_{до} = 0,75 \cdot 5,00 = 3,75 \text{ люд.-год.}$$

Отже, $t_i = 5,00 + 3,75 = 8,75$ люд.-год.

Витрати на аналіз та обробку інформації:

$$t_a = \frac{Q \cdot B}{(75...85)k}, \text{ люд.-год,} \qquad (3.6)$$

де В- коефіцієнт збільшення витрат праці внаслідок недостатнього опису задачі, В = 1,2...1,5.

Коефіцієнт збільшення витрат праці візьмемо В=1,2:

$$t_a = \frac{62,5 \cdot 1,2}{75 \cdot 0,8} = 1,25 \text{ люд.-год.}$$

Витрати на створення основних елементів консультаційної системи розраховуються за формулою(3.7):

$$t_c = \frac{Q}{(4...5)k} \text{, люд.-год..} \qquad (3.7)$$

$$t_c = \frac{50}{4 \cdot 0,8} = 15,63 \text{ люд.-год.}$$

Розрахована трудомісткість розробки політики на підприємстві дорівнює:

$$t = 3,75 + 8,75 + 1,25 + 15,63 = 29,38 \text{ люд.-год.}$$

Капітальні витрати на налаштування пароля на комп'ютері включають витрати на заробітну плату спеціалістів, що здійснюють розробку.

$$З_{ЗП} = t \cdot C_{ПР} \text{, грн.,} \qquad (3.8)$$

де t - загальна трудомісткість впровадження і настроювання, що визначається по формулах (3.1 – 3.7);

$C_{ПР}$ - середня годинна заробітна плата співробітника з нарахуваннями, грн./година.

Середня заробітна плата робітника з нарахуваннями на фонд заробітної плати за місяць складає 9700*1,22 = 11834 гривень. При 40 годинному робочому тижню місячний фонд робочого часу дорівнює 160 годин, тоді середня годинна заробітна плата $C_{ПР}$=11834/160=73,96 грн./година.

$\boldsymbol{З_{ЗП} = 29,38 \cdot 73,96 = 2172,95}$ грн.

Отже, для налаштування пароля на комп'ютері трудомісткість має дорівнювати 29,38 люд.-год, а заробітна плата дорівнює 2172,95 грн.

3.1.2 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки розраховуються за формулою (3.9):

$$С = С_в + С_к + С_{ак}, \quad тис. грн., \tag{3.9}$$

де $С_в$ - витрати на оновлення й модернізацію системи ІБ входять до заробітної плати обслуговуючого персоналу;

$С_к$ - витрати на керування системою ІБ, обчислюється за формулою 3.10;

$С_{ак}$ - витрати, викликані активністю користувачів системи (0 грн.).

Витрати на керування системою ІБ, обчислюється:

$$С_К = С_н + С_а + С_з + С_{єв} + С_е + С_о, грн., \tag{3.10}$$

де $С_н$ - витрати на навчання адміністративного персоналу ($С_н$=5000,00 грн.);

$С_а$ - річний фонд амортизаційних відрахувань ($С_а$=2500,00 грн.);

$С_з$ - річний фонд заробітної плати інженерно-технічного персоналу, обчислюється за формулою (3.11);

$С_е$ - вартість електроенергії, що споживається апаратурою системи ІБ протягом року, обчислюється за формулою (3.12);

$С_о$ - витрати на залучення сторонніх організацій для виконання деяких видів обслуговування ($С_о$=0 грн.);

Річний фонд заробітної плати інженерно-технічного персоналу (виконує директор), що обслуговує систему інформаційної безпеки, складає:

$$С_з = З_{осн} + З_Є, грн., \tag{3.11}$$

де $З_{осн}$ – основна заробітна плата ($З_{осн}$= 200400, грн. на рік);

$З_Є$ – єдиний соціальний внесок за рік – 22% ($З_Є$=44088 грн. на рік);

За формулою (3.15) визначається річний фонд заробітної плати:

$$С_з = 200400 + 44088 = 244488 \text{ грн.}$$

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

$$С_е = Р \times F_р \times Ц_е, \text{ грн.,} \quad (3.12)$$

де Р – встановлена потужність апаратури ІБ (Р=0,55 , кВт);

$F_р$ – річний фонд робочого часу системи ІБ ($F_р$=1920,годин);

$Ц_е$ – тариф на електроенергію ($Ц_е$=4,26, грн./кВт·годин).

Згідно формули (3.10) обчислюється вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$\boldsymbol{C_e = 0,55 \times 1920 \times 4,26 = 4498},56, \text{ грн.}$$

Згідно формули (3.14) обчислюються витрати на керування системою ІБ:

$$\boldsymbol{C_к = 5000,00 + 2500,00 + 244488 + 4498,56 = 256486,56}, \text{ грн.}$$

Згідно формули (3.9) обчислюються поточні витрати на функціонування системи ІБ:

$$C = 0 + 256486,56 + 0 = 256486,56, \text{ грн.}$$

3.2 Оцінка можливого збитку від атаки на сегмент мережі

3.2.1 Оцінка величини збитку

Необхідні дані для розрахунку:

- $t_п$ – час простою вузла або сегмента мережі внаслідок атаки ($t_п$=8 годин);

- $t_в$ – час відновлення після атаки персоналом підприємства ($t_в$=2 годин);
- $t_{ві}$ – час повторного введення загубленої інформації ($t_{ві}$=16 годин);
- $З_о$ – заробітна плата обслуговуючого персоналу ($З_о$=9000 грн. на місяць);
- $З_с$ – заробітна плата співробітників атакованого вузла ($З_с$=9200 грн. на місяць);
- $Ч_о$ – чисельність обслуговуючого персоналу ($Ч_о$=2 осіб);
- $Ч_с$ – чисельність співробітників атакованого вузла ($Ч_с$=1 осіб);
- О – обсяг продажів атакованого вузла (О=5224000 грн. у рік);
- $П_{зч}$ – вартість заміни встаткування або запасних частин ($П_{зч}$=0 грн.);
- I – число атакованих вузлів (I=1);
- N – середнє число атак на рік (N=12).

Упущена вигода від простою атакованого вузла розраховується згідно формули (3.17):

$$U = П_п + П_в + V, \text{ грн.}, \qquad (3.13)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла, грн.;

$П_в$ – вартість відновлення працездатності вузла, грн.;

V – втрати від зниження обсягу продажів за час простою атакованого вузла, грн.

Втрати від зниження продуктивності співробітників атакованого вузла являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки та обчислюються за формулою (3.14):

$$П_П = \frac{Зс}{F} \times t_П \ , \quad \text{грн.}, \qquad (3.14)$$

де F – місячний фонд робочого часу (F=160 годин).

Витрати на відновлення працездатності вузла обчислюються за формулою (3.15):

$$П_в = П_{ві} + П_{пв} + П_{зч}, \text{ грн.}, \quad (3.15)$$

де $П_{ві}$ – витрати на повторне уведення інформації, грн.;

$П_{пв}$ – витрати на відновлення вузла, грн.;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ві}$ розраховуються за формулою (3.16), виходячи з розміру заробітної плати співробітників атакованого вузла $З_с$, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ві} = \frac{З_С}{F} \times t_{ві} = \frac{9200}{160} \times 16 = 920{,}00, \text{ грн.} \quad (3.16)$$

Витрати на відновлення вузла $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу та обчислюється за формулою (3.17):

$$П_{пв} = \frac{З_О}{F} \times t_в = \frac{9000}{160} \times 2 = 112{,}5, \text{ грн.} \quad (3.17)$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла визначаються за формулою (3.14), виходячи із середньогодинного обсягу продажів типового підприємства і сумарного часу простою атакованого вузла:

$$V = \frac{O}{F_р} \times (t_П + t_В + t_{ві}), \text{ грн.}, \quad (3.14)$$

де $F_Р$ – річний фонд часу роботи організації ($F_Р$=1920 годин).

Згідно формули (3.14) розраховуються втрати від зниження продуктивності співробітників атакованого вузла:

$$П_{п} = \frac{9200}{160} \times 8 = 460 \text{ , грн.}$$

Згідно формули (3.15) розраховуються витрати на відновлення працездатності вузла:

$$П_{в} = 920{,}00 + 112{,}5 = 1032{,}50 \text{ , грн.}$$

Згідно формули (3.18) визначаються втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла:

$$V = \frac{5224000}{1920} \times (8 + 2 + 16) = 70741{,}67 \text{, грн.}$$

Згідно формули (3.13) визначаються упущена вигода від простою атакованого вузла:

$$U = 460 + 112{,}5 + 70741{,}67 = 71314{,}17 \text{, грн.}$$

Загальний збиток від атаки на вузол складається з суми упущеної вигоди помноженої на середню кількість атак та зниженню обсягів продажу на половину, через відтік клієнтів, зниженню рейтингу в пошукових система і визначається за формулою (3.19):

$$B = U \times N + \frac{O}{2} = 71314{,}17 \times 12 + 5224000/2 = 3467770{,}04 \text{, грн.} \quad (3.19)$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і обчислюється за формулою (3.20):

$$E = B \times R - C \text{ , грн.,} \quad (3.20)$$

де R – очікувана імовірність атаки на (R=0,3, частки одиниці);

Згідно формули (3.20) обчислюється загальний ефект від впровадження системи інформаційної безпеки:

$$E = 3467770{,}04 \times 0{,}3 - 256486{,}56 = 783844{,}45, \text{ грн.}$$

3.3 Висновок

Результатом проведеної роботи у даному розділі став розрахунок налаштування пароля на комп'ютері готелю "Схід", що становлять 2172,95 грн. Та загальний ефект від впровадження даної політики безпеки який станове безпеки 783844,45 грн. Якщо система захисту коштує менш ніж втрати при скоєні загрози, система враховується ефективною.

В ході роботи було визначено величину можливого збитку, що становить 3467770,04 грн.

ВИСНОВКИ

У роботі були розглянуті особливості функціонування компаній готельного бізнесу, з точки зору інформаційної безпеки. Для організацій цього типу визначені головні загрози ІБ. Були проаналізовані декілька моделі управління інформаційною безпекою, проведений їх порівняльний аналіз.

На основі отриманих даних була побудована модель загроз та модель порушника, які притаманні підприємствам цього класу. Був здійснений вибір найбільш оптимальної методики для управління ризиками інформаційної безпеки підприємств готельного бізнесу. На прикладі автоматизованого комплексу бронювання та методики пропонованої корпорацією Microsoft надані рекомендації на впровадження даних методик до процесу управління ІБ.

Сформована синтезована модель управління інформаційною безпекою, яка має чотири рівня. Впровадження системи управління ІБ дає можливість вибрати економічно ефективні елементи контролю, що зменшують ризик до прийнятного рівня.

Було проведено обґрунтування економічної ефективності управління інформаційною безпекою підприємств готельного бізнесу України.

ПЕРЕЛІК ПОСИЛАНЬ

1 НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу / ДСТСЗІ СБ України – Київ, 1999.

2 НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.

3 НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.

4 НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу / ДСТСЗІ СБ України – Київ, 1999.

5 Закон України «Про інформацію» (Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650) / Спосіб доступу: URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

6 Закон України «Про захист інформації в інформаційно-комунікаційних системах» (Відомості Верховної Ради України (ВВР), 1994, № 31, ст.286) / Спосіб доступу: URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

7 Закон України «Про захист персональних даних» (Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481) / Спосіб доступу: URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

8 ISO / IEC 27001 «Системи менеджменту інформаційної безпеки. Вимоги»

9 ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls.

10 ISO/IEC 27003:2017. Information technology - Security techniques - Information security management systems – Guidance

11 ДСТУ ISO/IEC 27004:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання

12 ISO/IEC 27005:2022 Information technology — Security techniques — Information security risk management

13 Кондрашов Ю.Н. Организация сетей и сетевых приложений в финансово-бюджетных организациях на базе технологий фирмы Microsoft.

14 ISO/IEC 27006:2015 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

15 ISO/IEC 27007:2020 Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing

16 ДСТУ ISO/IEC TS 27008:2019 Информационные технологии. Методы защиты. Руководство по оценке защиты информационной безопасности

17 ISO/IEC TS 27008:2019 Information technology — Security techniques — Guidelines for the assessment of information security controls

18 ISO/IEC 27010:2021 Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	33	
6	А4	2 Розділ	65	
7	А4	3 Розділ	10	
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	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК
на кваліфікаційну роботу магістра на тему:
Розробка моделі управління інформаційною безпекою готельного підприємства
Білової Юлії Олексіївни

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 123 сторінках та містить 13 рисунків, 27 таблиць, 18 джерел та 4 додатка.

Об'єкт дослідження: особливості управління інформаційною безпекою підприємств готельного бізнесу України.

Мета роботи: визначення особливостей аналізу та управління інформаційною безпекою підприємств готельного бізнесу України, дослідження існуючих методів та особливостей їх використання на практиці.

У роботі проаналізовано державні стандарти у сфері інформаційної безпеки України. Міжнародні стандарти управління ризиками інформаційної безпеки.

У спеціальній частині визначено найбільш небезпечних загроз які з'являються при функціонуванні підприємства та його ІС, де оброблюється конфіденційна інформація. Після аналізу була побудована типова модель загроз та модель порушника, для цього типу підприємства.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник