ЗМІСТ

ВСТУП 9

РОЗДІЛ 1. АНАЛІЗ МЕТОДИК ПРОВЕДЕННЯ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 10

1.1. Актуальність проблем інформаційної безпеки об’єктів електронної комерції 10

1.1.2 Основні моделі електронної комерції та особливості їх реалізації 11

1.1.3 Класифікація типів шахрайства в електронній комерції 14

1.1.4 Види загроз електронної комерції 16

1.2 Визначення аудиту інформаційної безпеки 22

1.2.1 Основні напрямки діяльності в області аудиту безпеки інформації 22

1.2.2 Види і цілі аудиту 23

1.2.3 Основні етапи аудиту безпеки 24

1.3 Висновки. Постановка задачі. 27

РОЗДІЛ 2. РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПРОВЕДЕННЯ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ’ЄКТІВ ЕЛЕКТРОННОЇ КОМЕРЦІЇ 28

2.1 Особливості проведення аудиту об’єктів електронної комерції. 28

2.2. Розробка рекомендацій щодо проведення аудиту об’єктів электронной комерції. 34

2.3. Аудит об’єктів електронної комерції на прикладі інтернет магазину. 41

2.3.1 Загальні відомості про організацію 42

2.3.2 Організаційна структура підприємства 42

2.3.3 Обстеження об’єкта інформаційної діяльності 43

2.3.4 Обстеження обчислювальної системи ТОВ «Авалон Днепр» 45

2.3.5 Аналіз загроз інформації 48

2.3.5 Модель порушника 52

2.3.6 Аналіз ризиків 55

2.3.7 Профіль захищеності WEB-сторінки 56

2.3.8 Рекомендації щодо підвищення рівня інфомаційної безпеки 64

2.3.9 Аналіз ризиків після впровадження рекомендацій 66

2.4 Висновки 67

РОЗДІЛ 3.ЕКОНОМІЧНА ЧАСТИНА 68

3.1.Розрахунок вартості проведення аудиту....68
3.2 Розрахунок експлуатаційних витрат....71
3.3 Оцінка економічної ефективності системи захисту інформації....74
3.4 Висновки до третього розділу....76
ВИСНОВКИ....77
ПЕРЕЛІК ПОСИЛАНЬ....78
ДОДАТОК А. Відомість матеріалів дипломного проекту....80
ДОДАТОК Б. Перелік файлів на електронному носії....81
ДОДАТОК В. Відгук керівника економічного розділу....82
ДОДАТОК Г. Відгук....83

ВСТУП

В основі успіху будь-якої комерційної діяльності лежить довіра споживачів. Стрімкий зліт електронної комерції за останні кілька років загострив цю проблему, виявивши недовіру користувачів до перенесення бізнесу у сферу Інтернет.

Саме у взаємодії перерахованих компонентів формується довіра споживачів до підприємств електронної комерції. Основ-ним користувачі вважають безпеку проведення платіжних трансакцій і конфіденційність їхньої персональної інформації. На захист інтересів користувачів спрямовані законодавчі акти, технологічні й організаційні заходи, процедури страхування і контролю. Не менш важливим користувачі вважають гарантування послідовності та цілісності трансакцій і правомочність їх проведення всіма сторонами.

На думку експертів, розвиток електронного бізнесу багато в чому визначається прогресом у галузі інформаційної безпеки, під якою розуміється стан стійкості інформації до випадкових чи навмисних впливів, що виключає неприпустимий ризик ЇЇ знищення, спотворення і розкриття, які призводять до матеріальних збитків власника чи користувача інформації

Метою роботи є підвищення ефективності інформаційної безпеки об’єктів інформаційної безпеки за допомогою проведення аудиту інформаційної безпеки.

Об’єктом досліджень в роботі є процес проведення аудиту інформаційної безпеки об’єктів електронної коммерції.

Предметом досліджень є аудит інформаційної безпеки.

Наукова новизна роботи полягає у визначенні особливостей та виборі методики реалізації процесу аудиту інформаційної безпеки

РОЗДІЛ 1. АНАЛІЗ МЕТОДИК ПРОВЕДЕННЯ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Актуальність проблем інформаційної безпеки об’єктів електронної комерції

Безпека на сьогоднішній день є ключовим питанням при впровадженні та використанні систем електронної комерції. Під електронною коммерцією розуміється технологія, яка забезпечує повний замкнутий цикл операцій, що включає замовлення товару (послуги), проведення платежів, участь в управлінні доставкою товару (виконання послуги). Ці операції проводяться з використанням електронних засобів та інформаційних технологій і забезпечують передачу прав власності або прав користування однією юридичною (фізичною) особою іншому.

Об'єктивно оцінити поточний стан інформаційної безпеки компанії, а також її адекватність поставленим цілям і задачам бізнесу з метою збільшення ефективності та рентабельності економічної діяльності організації суть основні завдання аудиту інформаційної безпеки. Тому під терміном "аналіз захищеності економічних інформаційних систем електронної комерції будемо розуміти системний процес отримання об'єктивних якісних і кількісних оцінок про поточний стан інформаційної безпеки економічної системи відповідно до визначених критеріїв та показників безпеки.

Важко переоцінити значимість забезпечення безпеки при користуванні ресурсами Інтернету з персональних комп'ютерів або мобільних пристроїв. Згідно зі статистикою, Україна опинилася на 4 місці в світі за кількістю кібератак, що виходять з країни. Україна опинилася на 4 місці після Росії, Тайваню та Німеччини. За останній місяць з українських серверів було скоєно 566 531 атак.

У зв'язку з вищевикладеним на сьогодні аудит інформаційної безпеки економічних інформаційних систем (ЕІС) при веденні бізнесу за допомогою інтернет технологій все ще актуальний.

1.1.2 Основні моделі електронної комерції та особливості їх реалізації

Електро́нна коме́рція— це сфера цифрової економіки, що включає всі фінансові та торгові транзакції, які проводяться за допомогою комп'ютерних мереж, та бізнес-процеси, пов'язані з проведенням цих транзакцій.

Схема роботи електронної комерції наведена на рисунку 1.1

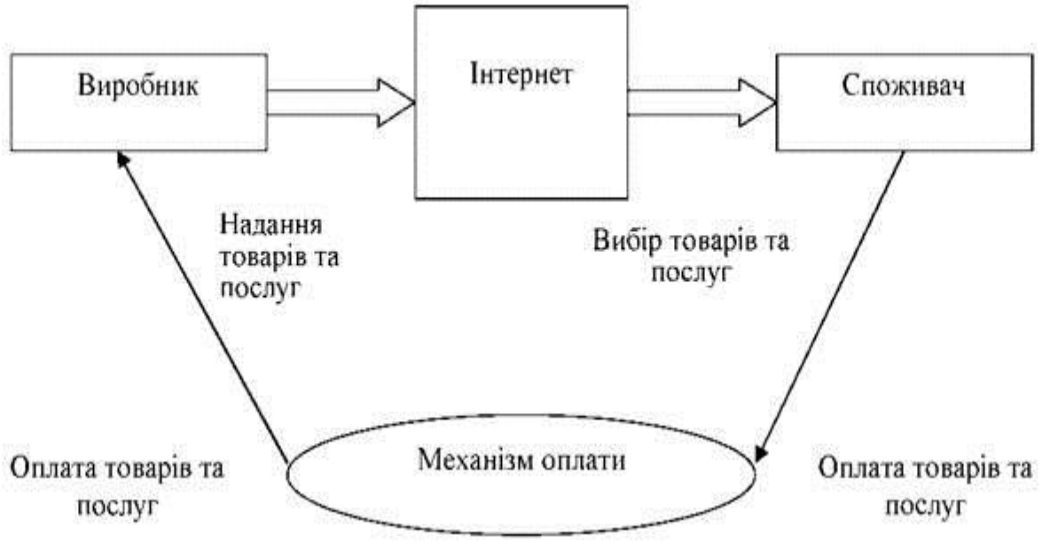

Рисунок 1.1 – Схема роботи електронної комерції

Традиційно здійснення бізнесу методами ЕК відбувається на основі одної з двох наступних моделей (рисунок 1.2).

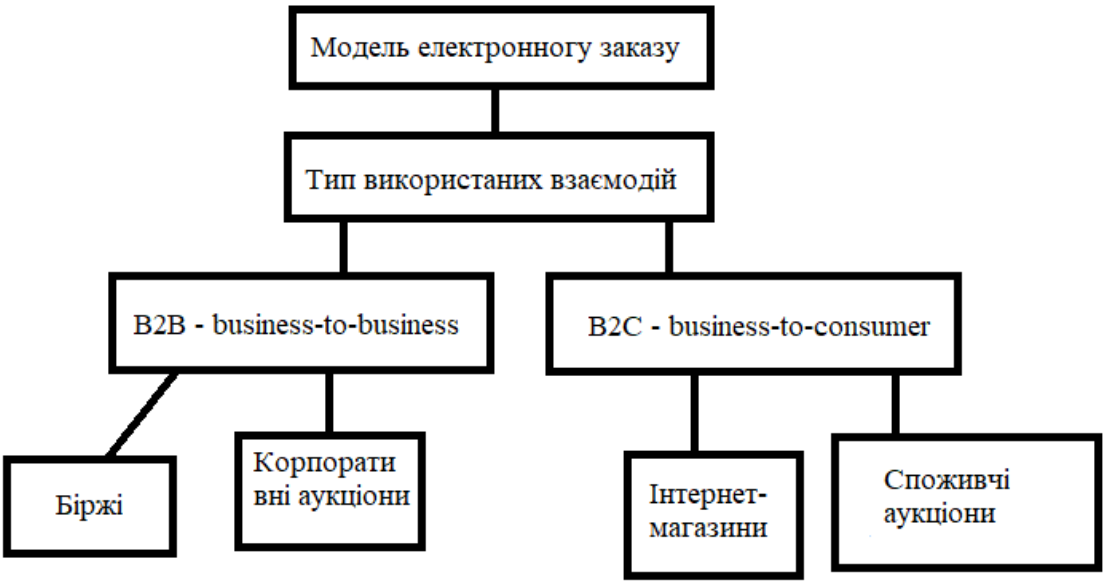

Рисунок 1.2 – Типи електронної комерції

1 B2B (Business-Te-Business), при якій компанія (юридична особа) пропонує (продає) свої товари (послуги) іншій компанії (юридичній особі). При цьому автоматизуються бізнес-процеси, характерні для виробничого або оптової ланки ланцюжка руху товару: закупівля сировини і комплектуючих; оптові продажі готових товарів і їх доставка; безготівкові платежі, включаючи сплату податків і митних зборів; укладання договорів; обмін документами та ін.

2 B2C (Business-Te-Customer / Consumer), при якій компанія пропонує (продає) свої товари (послуги) фізичним особам. Модель B2C застосовується при реалізації товару в роздріб і, відповідно, упор робиться на різного виду готівки платежах, роздрібних продажах, сервісному обслуговуванні, супровідних документах і ін.

Модель B2B в даний час найбільш часто реалізована у вигляді торгових майданчиків або повнофункціональних систем класу B2B.

Торгові майданчики являють собою спеціалізовані сайти в мережі Інтернет, на яких будь-яка компанія може розмістити свої комерційні пропозиції або запити. Такі майданчики можуть бути як галузевими, на яких розміщуються запити і пропозиції компаній, що працюють в певних галузях,

або багатогалузевих. При цьому запити і пропозиції компаній формуються у вигляді інформації в загальному каталозі сайту майданчики, що спрощує їх пошук як в розрізі товарів (послуг), так і компаній / галузей.

У повнофункціональної системі класу B2B методами ЕК реалізовані всі або основні бізнес-процеси компанії. При цьому існує основна (серверна) програмна частина системи, поставлена на комп'ютери компанії, і клієнтські частини, поставлені на комп'ютери клієнтів - як постачальників, так і споживачів. При роботі системи ЕК взаємодія відбувається між серверної частина і клієнтськими частинами системи.

Модель B2C в даний час найбільш часто реалізована у вигляді електронних торговельних рядів (іноді їх називають також онлайн-супермаркети, торговельні центри, інтернет-вітрини), електронних аукціонів або інтернет-магазинів.

Електронні торгові ряди за своїми завданнями і можливостями дуже схожі на торговельні майданчики систем класу B2B. На них, так само як і на торгових майданчиках класу B2B, компанії розміщують свої прайс-листи в каталозі прайс-листів торгового ряду. Покупець може переглянути їх списком, або в ряду цін пропозицій інших учасників торгового ряду, відсортованих за категоріями, характеристикам або моделям пропонованих товарів. Після вибору товару покупець перенаправляється на сайт компанії, продавця, де і здійснюється операція.

Інтернет-аукціон - вид ЕК, який найчастіше реалізується на основі моделі B2C (хоча є і приклади реалізації в моделі B2B - наприклад, exleasingcar.com). У цій моделі реалізується принцип аукціону, коли продаж товарів (послуг) здійснюється на публічних конкурентних торгах, в процесі яких і встановлюється кінцева ціна на них.

Інтернет-магазин - найбільш функціонально повна реалізація методів ЕК в роздрібному бізнесі. Зазвичай під інтернет-магазином розуміють сайт, який торгує товарами (послугами) в мережі Інтернет.

1.1.3 Класифікація типів шахрайства в електронній комерції

Міжнародні платіжні системи призводять наступну класифікацію можливих типів шахрайства через Інтернет:

- транзакції, виконані шахраями з використанням правильних реквізитів картки (номер картки, термін її дії та т. п.);

- компрометація даних (отримання даних про клієнта через злом баз даних (БД) торгових підприємств або шляхом перехоплення повідомлень покупця, що містять його персональні дані) з метою їх використання в шахрайських цілях;

- магазини, що виникають, як правило, на нетривалий час для того, щоб зникнути після отримання від покупців коштів за неіснуючі послуги або товари;

- зловживання торгових підприємств, пов'язані зі збільшенням вартості товару по відношенню до запропонованої покупцеві ціною або повторними списаннями з рахунку клієнта;

- магазини та торгові агенти (Acquiring Agent), призначені для збору інформації про реквізити карт і інших персональних даних покупців.

Коротко зупинимося на перелічених типах шахрайства в окремо. Як уже зазначалося, перший тип шахрайства є найбільш масовим. Для здійснення транзакції шахраєві зазвичай досить знати тільки номер карти і термін її дії. така інформація потрапляє в руки шахраїв різними шляхами. Найбільш поширений спосіб отримання шахраями реквізитів карт - змова з співробітниками торгових підприємств (ТП), через які проходять сотні і тисячі транзакцій по пластикових картах. Результатом змови стає передача інформації про реквізити карт в руки кримінальних структур.

Інший спосіб отримання інформації про реквізити карт, що став популярним останнім часом, - крадіжка баз даних карток в ТП. Ще одним способом генерації правильного номера карти є спеціальні програми.

Програма генерує правильні номери карт, емітованих деякими банками, використовуючи для генерації номерів той же алгоритм, що і банк-емітент.

Досить поширеним є спосіб, коли кримінальні структури організовують свої магазини, головною метою яких є отримання в своє розпорядження значних наборів реквізитів карт. Інша функція подібних магазинів полягає в їх використанні для «відмивання» отриманих реквізитів карт. Через подібні сайти «прокачуються» сотні тисяч і навіть мільйони вкрадених реквізитів карт.

Нарешті, існує і ще один спосіб дізнатися правильні реквізити карт. Точніше не впізнати, а емпірично обчислити. Справа в тому, що Інтернет являє собою прекрасний плацдарм для проведення різного роду «випробувань» з метою визначення правильних реквізитів карт. наприклад, якщо шахраєві відомий номер карти, але ніхто не знає термін її дії, то визначити цей параметр карти не складає великих труднощів. Дійсно, пластикова карта зазвичай випускається терміном на два роки. Параметр «термін дії карти» визначає місяць і останні дві цифри року, коли дія картки закінчується. Таким чином, шахраєві потрібно перебрати всього лише 24 можливих варіанти цього параметра. В реальному світі зробити це не просто. У віртуальному світі рішення подібної завдання не складає труднощів. Шахраєві потрібно відправити не більше 24 авторизаційних запитів для того, щоб зі 100% -й вірогідністю визначити вірний термін дії карти. Після цього скористатися відомими реквізитами карти можна різними способами. Найпростіше здійснити транзакцію. Більш ефективний спосіб скористатися здобутим знанням - виготовити підроблену карту з обчисленими реквізитами карти і використовувати її для оплати покупок в реальних ТП. У цьому випадку таке шахрайство потрапить в розряд «підроблена карта»

Третій тип шахрайства - магазини-метелики, які відкриваються з метою «відмивання» вкрадених реквізитів карт. Після того як в руках кримінальних структур з'являються вкрадені реквізити карт, виникає задача ними

скористатися. Один із способів - організація віртуального ТП, «який торгує» програмним забезпеченням або іншими інформаційними ресурсами (програми телевізійних передач, підписка на новини і т. д.). Насправді, таке ТП, як правило, має свій сайт, але нічим реально не торгує. При цьому в обслуговуючий банк регулярно направляються авторизовані запити, що використовують вкрадені номери карток. Отже, магазин регулярно отримує від обслуговуючого банку відшкодування за скоєні в ньому «покупки». Так триває до тих пір, поки рівень chargeback (відмов від платежів), від емітентів вкрадених реквізитів карт не стане свідченням того, що має місце шахрайство.

Магазини-метелики зазвичай вибирають дві крайні стратегії своєї роботи. Вибір стратегії визначається розміром вкраденої БД карток. Якщо розмір вкраденої БД досить великий (десятки тисяч карт), то вибирається стратегія, відповідно до якої транзакції робляться на невеликі суми (близько $ 10 США). Основна ідея такої стратегії полягає в тому, що дійсний власник кар ти помітить невелику втрату коштів на своєму рахунку далеко не відразу і в результаті за наявне в розпорядженні шахраїв час (як правило, 1-3 місяці) можна на подібних невеликих транзакціях вкрасти сотні тисяч доларів. Навпаки, коли в розпорядженні шахраїв кілька десятків карт, вибирається стратегія виконання транзакцій на великі суми (кілька тисяч доларів). В цьому випадку активне життя магазину-метелики становить кілька тижнів, після чого магазин зникає.

1.1.4 Види загроз електронної комерції

Всю множину потенційних загроз комп'ютерної інформації корисно представити згідно природи їх виникнення, розділивши на два класи: природні і штучні, що впливають на роботу інформаційної системи (ІС), яка обслуговує заходи з електронної комерції.

Природні загрози – це загрози, викликані впливами на АС і її компонентів фізичних процесів або стихійних природних явищ, незалежних від людини. їх можна розділити на природні і технічні.

Штучні – це загрози, викликані діяльністю людини. Серед них, виходячи з мотивації дій, можна виділити:

– Ненавмисні, випадкові загрози, викликані помилками людей при проектуванні АС, і її компонентів, а також в процесі їх експлуатації. – Навмисні загрози, пов'язані з корисливими устремліннями людей (зловмисників). Джерела загроз по відношенню до АС можуть бути зовнішніми або внутрішніми (компоненти самої ЕОМ – її апаратура, програми, персонал).

Природні загрози.

– Стихійні лиха (урагани, повені, землетруси, цунамі, пожежі, виверження вулканів, снігові лавини, селеві потоки тощо). Загрози цієї групи пов'язані з прямим фізичним впливом на елементи ІС і системи забезпечення (водо-, тепло-, електропостачання) і ведуть до порушення роботи ІС і фізичному знищенню систем забезпечення, персоналу, засобів обробки й передачі даних, носіїв інформації;

Магнітні бурі чинять електромагнітні впливу на магнітні носії інформації, електронні засоби обробки і передачі даних, обслуговуючий персонал та ведуть до відмов апаратури, викривлення або знищення інформації, помилок персоналу;

Радіоактивні випромінювання і опади. Ці загрози аналогічні за наслідками загрозам попередньої підгрупи і, крім того, ведуть до захворювань персоналу.

Технічні загрози. Загрози цієї групи пов'язані з надійністю технічних засобів обробки інформації та систем забезпечення ІС. 12

Відключення або коливання електроживлення та інших засобів забезпечення ведуть до втрат інформації, виходу з ладу засобів обробки і порушень в управлінні об'єктами в керуючих ІС.

Відмови і збої засобів обробки пов'язані з надійністю роботи апаратнопрограмних засобів та ведуть до спотворення і втрат інформації, порушення управління об'єктами.

На рисунку 1.3. представлено класифікацію загроз електронної комерції.

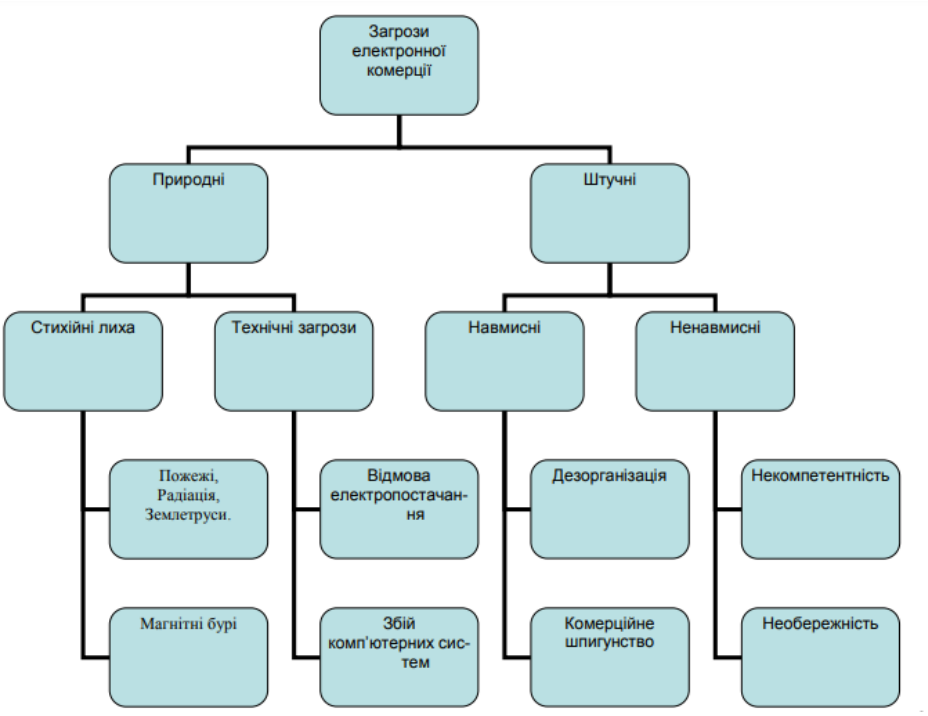

Рисунок 1.3. - Загальна класифікація загроз електроної комерції

Ненавмисні загрози пов'язані з діями, які люди вчиняють випадково, через незнання, неуважність або недбалість, з цікавості, але без злого наміру:

– Ненавмисні дії, що призводять до часткового або повної відмови системи або руйнування апаратних, програмних, інформаційних ресурсів системи (ненавмисна псування устаткування, видалення, перекручування файлів з важливою інформацією або програм, в тому числі системних і т.п.);

– Неправомірне відключення устаткування або зміна режимів роботи пристроїв та програм;

– Ненавмисне псування носіїв інформації;

– Запуск технологічних програм, здатних при некомпетентному використанні викликати втрату працездатності системи (зависання або зациклення) або здійснюють незворотні зміни в системі (форматування або реструктуризацію носіїв інформації, видалення даних і т.п.);

– Нелегальне впровадження та використання неврахованих програм (ігрових, навчальних, технологічних та ін які не є необхідними для виконання порушником своїх службових обов'язків) з подальшим необґрунтованим витрачанням ресурсів (завантаження процесора, захоплення оперативної пам'яті і пам'яті на зовнішніх носіях);

– Зараження комп'ютера вірусами;

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

– Розголошення, передача або втрата атрибутів розмежування доступу (паролів, ключів, шифрування, ідентифікаційних карток, перепусток і т.п.);

– Проектування архітектури системи, технології обробки даних, розробка прикладних програм, з можливостями, які надають небезпеку для працездатності системи та безпеки інформації;

– Ігнорування організаційних обмежень, при роботі в системі;

– Вхід в систему в обхід засобів захисту (завантаження сторонньої операційної системи з дискети і т.п.);

– Некомпетентне використання, налаштування або неправомірне відключення засобів захисту персоналом служби безпеки;

– Пересилання даних по хибному адресу абонента (пристрою);

– Введення помилкових даних;

– Ненавмисне пошкодження каналів зв'язку. Навмисні загрози. Це дії людей здійснюються навмисне для дезорганізації роботи системи, виведення системи з ладу, проникнення в систему і несанкціонованого доступу до інформації:

– Фізичне руйнування системи (шляхом вибуху, підпалу тощо) або вивід з ладу всіх або окремих найбільш важливих компонентів АС (пристроїв, носіїв важливої системної інформації, осіб із числа персоналу і т.п.);

– Відключення або вивід з ладу підсистем забезпечення функціонування обчислювальних систем (електроживлення, охолодження та вентиляції, ліній зв'язку тощо);

– Дії по дезорганізації функціонування системи (зміна режимів роботи пристроїв або програм, страйк, саботаж персоналу, постановка потужних активних радіоперешкод на частотах роботи пристроїв системи і т.п.);

– Впровадження агентів в число персоналу системи (у тому числі, можливо, і в адміністративну групу, яка відповідала за безпеку);

– Вербовка (шляхом підкупу, шантажу і т.п.) персоналу або окремих користувачів, що мають певні повноваження;

– Застосування пристроїв для підслуховування, дистанційна фото та відеозйомка і т.п.;

– Перехоплення побічних електромагнітних, акустичних та інших випромінювань пристроїв і каналів зв'язку, а також наводок активних випромі- 14 нювань на допоміжні технічні засоби, безпосередньо не беруть участь в обробці інформації (телефонні лінії, мережі живлення, опалення тощо);

– Перехоплення даних, переданих по каналах зв'язку, і їх аналіз з метою з'ясування протоколів обміну, правил входження в зв'язок і авторизації користувача і подальших спроб їх систематизації для проникнення в систему;

– Розкрадання носіїв інформації (магнітних дисків, стрічок, запам'ятовуючих пристроїв і самих персональних комп’ютерів);

– Несанкціоноване копіювання носіїв інформації;

– Розкрадання виробничих відходів (роздруківок, записів, списаних носіїв інформації і т.п.);

– Читання залишкової інформації з оперативної пам'яті і з зовнішніх запам'ятовуючих пристроїв;

– Читання інформації з областей оперативної пам'яті, використовуваних операційною системою (в тому числі підсистемою захисту) або іншими користувачами, в асинхронному режимі, використовуючи недоліки мультизадачних операційних систем і систем програмування;

– Незаконне одержання паролів та інших реквізитів доступу (агентурним шляхом, використовуючи недбалість користувачів, шляхом підбору, шляхом імітації інтерфейсу системи і т.д.) з наступним маскуванням під зареєстрованого користувача;

– Несанкціоноване використання терміналів користувачів, що мають унікальні фізичні характеристики, такі як номер робочої станції в мережі, фізичну адресу, адресу в системі зв'язку, апаратний блок кодування і т.п.;

– Злам шифрів криптозахисту інформації;

– Впровадження апаратних, програмних "закладок" і "вірусів" ("троянських коней "і" жучків "), тобто таких ділянок програм, які не потрібні для здійснення заявлених функцій, але дозволяють долати систему захисту, потай і незаконно здійснювати доступ до системних ресурсів з метою реєстрації і передачі критичної інформації або дезорганізації функціонування системи;

– Незаконне підключення до ліній зв'язку з метою роботи "між рядків", з використанням пауз в діях законного користувача від його імені з наступним введенням помилкових спілкувань або модифікацією переданих повідомлень;

– Незаконне підключення до ліній зв'язку з метою прямої підміни законного користувача шляхом його фізичного відключення після входу в

систему і успішної аутентифікації з подальшим введенням дезінформації та нав'язуванням хибних повідомлень.

1.2 Визначення аудиту інформаційної безпеки

Аудит інформаційної безпеки - системний процес отримання об'єктивних якісних і кількісних оцінок про поточний стан інформаційної безпеки компанії відповідно до визначених критеріїв та показниками безпеки.

Таким чином, аудит в даному випадку сводиться до перевірки системи інформаційної безпеки і порівняно її результатів з таким собі ідеалом.

Для різних видів аудиту розрізняються все три складові послуги аудиту: засоби і способи перевірки, результат перевірки та ідеал, з яким порівнюється результат перевірки.

Аудит призначений для оцінки стану інформаційної безпеки інформаційної системи (ІС) і розробки рекомендацій щодо застосування комплексу організаційних заходів та програмно-технічних засобів, спрямованих на забезпечення захисту інформаційних ресурсів ІС від загроз інформаційної безпеки.

1.2.1 Основні напрямки діяльності в області аудиту безпеки інформації

Основні напрямки аудиту інформаційної безпеки деталізуються на наступні: атестацію; контроль захищеності інформації; спеціальні дослідження технічних засобів і проектування об'єктів в захищеному виконанні.

1 Атестація об'єктів інформатизації за вимогами безпеки інформації:

- атестація автоматизованих систем, засобів зв'язку, обробки і передачі інформації;
- атестація приміщень, призначених для ведення конфіденційних переговорів;

– атестація технічних засобів, встановлених в виділених приміщеннях.

2 Контроль захищеності інформації обмеженого доступу:

– виявлення технічних каналів витоку інформації і способів несанкціонованого доступу до неї;

– контроль ефективності застосовуваних засобів захисту інформації.

3 Спеціальні дослідження технічних засобів на наявність побічних електромагнітних випромінювань і наведень (ПЕМВН):

– персональні ЕОМ, засоби зв'язку та обробки інформації;

– локальні обчислювальні системи;

– оформлення результатів досліджень відповідно до вимог ФСБ і ФСТЕК.

4 Проектування об'єктів в захищеному виконанні:

– розробка концепції інформаційної безпеки;

– проектування автоматизованих систем, засобів зв'язку, обробки передачі інформації в захищеному виконанні;

– проектування приміщень, призначених для ведення конфіденційних переговорів.

1.2.2 Види і цілі аудиту

Розрізняють зовнішній і внутрішній аудит.

Зовнішній аудит - це, як правило, разовий захід, що проводиться за ініціативою керівництва організації або акціонерів. Зовнішній аудит рекомендується (а для ряду фінансових установ і акціонерних товариств потрібно) проводити регулярно.

Внутрішній аудит являє собою безперервну діяльність, яка здійснюється на підставі документа, зазвичай носить назву «Положення про внутрішній аудит», і відповідно до плану, підготовка якого здійснюється підрозділом внутрішнього аудиту та затверджується керівництвом організації. Аудит безпеки інформаційних систем є однією зі складових IT-аудиту.

Цілями проведення аудиту безпеки є:

- аналіз ризиків, пов'язаних з можливістю здійснення загроз безпеки щодо ресурсів ІС;

- оцінка поточного рівня захищеності ІС;

- локалізація вузьких місць в системі захисту ІС; - оцінка відповідності ІС існуючим стандартам в області інформаційної безпеки;

- вироблення рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів безпеки ІС.

У число додаткових завдань, що стоять перед внутрішнім аудитором, крім надання допомоги зовнішнім аудиторам, можуть також входити:

- розробка політик безпеки та інших організаційно-розпорядчих документів щодо захисту інформації та участь в їх впровадженні в роботу організації;

- постановка завдань для ІТ-персоналу, що стосуються забезпечення захисту інформації;

- участь в навчанні користувачів і обслуговуючого персоналу ІС питань забезпечення інформаційної безпеки;

- участь в розборі інцидентів, пов'язаних з порушенням інформаційної безпеки;

- інші завдання.

1.2.3 Основні етапи аудиту безпеки

Роботи по аудиту безпеки ІС включають в себе ряд послідовних етапів, які в цілому відповідають етапам проведення комплексного ІТ-аудиту автоматизованої системи, що включає в себе:

- ініціювання процедури аудиту;
- збір інформації аудиту;
- аналіз даних аудиту;
- вироблення рекомендацій;

– підготовку аудиторського звіту.

На етапі ініціювання процедури аудиту повинні бути вирішені наступні організаційні питання:

– права і обов'язки аудитора повинні бути чітко визначені і документально закріплені в його посадових інструкціях, а також в положенні про внутрішній (зовнішньому) аудиті;

– аудитором повинен бути підготовлений і узгоджений з керівництвом план проведення аудиту;

– в положенні про внутрішній аудит має бути закріплено, зокрема, що співробітники компанії зобов'язані сприяти аудитору і надавати всю необхідну для проведення аудиту інформацію.

На етапі ініціювання процедури аудиту повинні бути визначені межі проведення обстеження. План і кордони проведення аудиту обговорюються на робочому зборах, в якому беруть участь аудитори, керівництво компанії і керівники структурних підрозділів.

Етап збору інформації аудиту є найбільш складним і тривалим. Це пов'язано в основному з відсутністю необхідної документації на інформаційну систему і з необхідністю щільного взаємодії аудитора з багатьма посадовими особами організації.

Компетентні висновки щодо стану справ в компанії з інформаційною безпекою можуть бути зроблені аудитором тільки за умови наявності всіх необхідних вихідних даних для аналізу. Перший пункт аудиторського обстеження починається з отримання інформації про організаційну структуру користувачів ІС і обслуговуючих підрозділів. Призначення і принципи функціонування ІС багато в чому визначають існуючі ризики і вимоги безпеки, що пред'являються до системи. Далі, аудитору потрібно більш детальна інформація про структуру ІС. Це дозволить усвідомити, яким чином здійснюється розподіл механізмів безпеки за структурними елементами і рівнями функціонування ІС.

Використовувані аудиторами методи аналізу даних визначаються вибраними підходами до проведення аудиту, які можуть істотно різнитися.

Перший підхід, найскладніший, базується на аналізі ризиків. Спираючись на методи аналізу ризиків, аудитор визначає для обстежуваної ІС індивідуальний набір вимог безпеки, в найбільшою мірою враховує особливості даної ІС, середовища її функціонування і існуючі в даному середовищі загрози безпеки.

Другий підхід, самий практичний, спирається на використання стандартів інформаційної безпеки. Стандарти визначають базовий набір вимог безпеки для широкого класу ІС, який формується в результаті узагальнення світової практики. Стандарти можуть визначати різні набори вимог безпеки, в залежності від рівня захищеності ІС, який потрібно забезпечити, її приналежності (комерційна організація або державна установа), а також призначення (фінанси, промисловість, зв'язок і т. П.). Від аудитора в даному випадку потрібно правильно визначити набір вимог стандарту, відповідність яким потрібно забезпечити.

Третій підхід, найбільш ефективний, передбачає комбінування перших двох. Базовий набір вимог безпеки, що пред'являються до ІС, визначається стандартом. Додаткові вимоги, в максимальному ступені враховують особливості функціонування даної ІС, формуються на основі аналізу ризиків.

Рекомендації, що видаються аудитором за результатами аналізу стану ІС, визначаються використовуваним підходом, особливостями обстежуваної ІС, станом справ з інформаційною безпекою і ступенем деталізації, використовуваної при проведенні аудиту. У будь-якому випадку, рекомендації аудитора повинні бути конкретними і застосовними до даної ІС, економічно обгрунтованими, аргументованими (підкріпленими результатами аналізу) і відсортованими за ступенем важливості. При цьому заходи щодо забезпечення захисту організаційного рівня практично завжди мають пріоритет над конкретними програмно-технічними методами захисту. У той

же час наївно очікувати від аудитора, як результат проведення аудиту, видачі технічного проекту підсистеми інформаційної безпеки, або детальних рекомендацій щодо впровадження конкретних програмно-технічних засобів захисту інформації. Це вимагає більш детального опрацювання конкретних питань організації захисту, хоча внутрішні аудитори можуть приймати в цих роботах найактивнішу участь.

1.3 Висновки. Постановка задачі.

У першому розділі було проаналізовано:

− актуальність проблеми безпеки інформації об’єктів електронної комерції;

− основні загрози інформаційній безпеці об’єктів електронної комерції;

− методики проведення аудиту інформаційної безпеки;

Постановка задачі:

− розглянути особливості проведення аудиту інформаційної безпеки

− розробити рекомендації щодо проведення аудиту інформаційної безпеки об’єктів електронної комерції;

− визначити ефективність проведення аудиту, на прикладі інтернет-магазину;

− визначити капітальні та експлуатаційні витрати проведення аудиту інформаційної безпеки.

РОЗДІЛ 2. РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПРОВЕДЕННЯ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ'ЄКТІВ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

2.1 Особливості проведення аудиту об'єктів електронної комерції.

Згідно з прийнятим 5 жовтня 2017 року Законом України «Про основні засади забезпечення кібербезпеки України» (набирає чинності 9.05.2018 р.), функціонування національної системи кібербезпеки, серед іншого, забезпечується шляхом «досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО», а також з урахуванням «кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту». В аспекті дотримання інформаційної безпеки це, згідно з Законом (статті 6,8), включає в себе насамперед розроблення на цій основі відповідних нормативно-правових актів, створення єдиної (універсальної) системи індикаторів кіберзагроз і запровадження національної системи аудиту інформаційної безпеки на критично важливих об'єктах кіберзахисту. Крім того, в статті 15 Закону затверджується, що основні суб'єкти національної кібербезпеки також підлягають аудиту, який має бути (а) незалежним, (б) щорічним і (в) проводитися «згідно з міжнародними стандартами аудиту».

На сьогодні в Україні чинними є ряд нормативних документів (НДТЗІ), що регулюють технічний захист інформації. Перелік нормативних документів в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України (ДСТУ) стосовно створення і функціонування КСЗІ:

- НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі
- Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96
- НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі
- НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в

комп’ютерних системах від несанкціонованого доступу

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

– НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу

– НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

Положення Конституції України розвиваються та конкретизуються у понад 200 документах, які встановлюють правові норми в інформаційній сфері. Серед них базові Закони України «Про інформацію», «Про друковані засоби масової інформації (пресу) в Україні», «Про телебачення та радіомовлення», «Про інформаційні агентства», «Про державну таємницю», «Про зв'язок», «Про державну підтримку засобів масової інформації та соціальний захист журналістів», «Про рекламу», «Про Концепцію національної програми інформатизації», «Про Національну програму інформатизації», «Про науково-технічну інформацію», «Про захист інформації в автоматизованих системах», «Про електронний підпис», «Про електронний документообіг» та інші.

Закон України «Про захист персональних даних» регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних.

В Україні тривають процеси гармонізації та введення в дію сучасних міжнародних стандартів інформаційної безпеки, насамперед – серії міжнародних стандартів ISO/IEC 27000, розробленою Міжнародною організацією з стандартизації (ISO) спільно з Міжнародною електротехнічною комісією (IEC), яка постійно доповнюється новими

документами. Серія являє собою модель (фреймворк) для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та поліпшення системи менеджменту інформаційної безпеки як на загальному рівні (27001), так і в окремих секторах та галузях – фінанси, транспорт, енергетика, охорона здоров'я, оператори зв'язку, хмарні обчислення, інфраструктурні проекти, аудит і сертифікація тощо.

Впровадження системи управління інформаційною безпекою (СУІБ) відповідно до ISO/IEC 27000 дозволяє оптимізувати процес захисту інформаційних ресурсів і управління ризиками для цих ресурсів.

Стандарт містить вимоги в області інформаційної безпеки для створення, розвитку і підтримки Системи менеджменту інформаційної безпеки. Кращі світові практики в галузі управління інформаційною безпекою описані в міжнародному стандарті на системи менеджменту інформаційної безпеки ISO / IEC 27001 (ISO 27001). ISO 27001 встановлює вимоги до системи менеджменту інформаційної безпеки (СМІБ) для демонстрації здатності організації захищати свої інформаційні ресурси. Поняття захисту інформації трактується міжнародним стандартом як забезпечення конфіденційності, цілісності та доступності інформації. Основа стандарту ICO 27001 – система управління ризиками, пов'язаними з інформацією. Система управління ризиками дозволяє отримувати відповіді на наступні питання: - напрямки інформаційної безпеки на яких потрібно зосередити увагу; - часу і кошти, які можна витратити на дане технічне рішення для захисту інформації.

Стандарт ISO/IEC 15408 «Загальні критерії оцінки безпеки інформаційних технологій» (англ. Common Criteria for Information Technology Security Evaluation) описує інфраструктуру (Framework) в якій користувачі комп'ютерної системи можуть описати вимоги, розробники можуть заявити про властивості безпеки продуктів, а експерти з безпеки визначити, чи задовольняє продукт заявам. Таким чином цей стандарт дозволяє бути

впевненим, що процес опису, розробки та перевірки продукту був проведений в строгому порядку. Прообразом даного документа послужили «Критерії оцінки безпеки інформаційних технологій» (англ. Evaluation Criteria for IT Security, ECITS), робота над якими почалася в 1990 році. Стандарт містить два основних види вимог безпеки: функціональні, що висуваються до функцій безпеки і реалізує їх механізмів, і вимоги довіри, які пред'являються до технології та процесу розробки та експлуатації.

PCI DSS (абревіатура від Payment Card Industry Data Security Standard) - стандарт безпеки даних індустрії платіжних карт. Стандарт розроблений міжнародними платіжними системами Visa та MasterCard і ін.

Оплата в інтернеті банківськими картами передбачає можливу передачу, зберігання і обробку даних платіжної картки, що підвищує ризики кіберзлочинності. PCI DSS захищає персональні дані і запобігає шахрайство при оплаті. Кожна організація, яка приймає і обробляє дані банківських карт на своєму сайті, повинна відповідати вимогам PCI DSS.

Вимоги до безпеки:

Стандарт PCI DSS висуває чіткі вимоги до організацій, які здійснюють платіжні операції в інтернеті. Це 6 сфер безпеки, розділені на 12 пунктів.

Ключові:

- Створення і підтримка безпечної мережі
- Захист даних власників карток (забезпечення захисту даних власників карток в ході їх зберігання, забезпечення шифрування даних власників карток при оплаті).
- Підтримка програми управління уразливими (використання і регулярне оновлення антивірусного програмного забезпечення, розробка та підтримка безпечних систем і додатків).
- Контроль доступу до даних (присвоєння унікального ідентифікатора кожному особі, яка має доступ до інформаційної інфраструктури, обмеження фізичного доступу до даних власників карток).

– Регулярний моніторинг і тестування мережі (контроль і відстеження всіх сеансів доступу до мережевих ресурсів і даних власників карток, регулярне тестування систем і процесів забезпечення безпеки).

– Розробка і виконання політики інформаційної безпеки.

Рівні сертифікації PCI DSS

Існує 4 рівня сертифікації за стандартом PCI DSS:

Level 4 для компаній, що обробляють до 20 тис. транзакцій на рік.

Level 3 від 20 тис. До 1 млн. транзакцій в рік.

Level 2 від 1 млн. До 6 млн. транзакцій на рік.

Level 1 проводиться тільки з залученням незалежного аудитора (QSA) і дозволяє обробляти більше 6 млн. транзакцій на рік.

2 рівня постачальників послуг:

Рівень 2: платіжні системи які обробляють, зберігають або передають дані про менш 300 тис. транзакцій на рік.

Рівень 1: платіжні системи які обробляють, зберігають або передають дані про понад 300 тис. транзакцій на рік.

При оплаті послуг через платіжні сервіси, що відповідають стандарту PCI DSS користувач може бути впевнений у безпеці операції і конфіденційності власних даних. Всі системи і платіжні сервіси, які взаємодіють з картами VISA / MasterCard, зобов'язані проходити щорічну сертифікацію і щоквартальну перевірку.

Загальний регламент щодо захисту даних (англ. General Data Protection Regulation) - постанова Європейського Союзу, за допомогою якого Європейський парламент, Рада Європейського Союзу та Європейська комісія підсилюють і уніфікують захист персональних даних всіх осіб в Європейському Союзі (ЄС). Постанова також направлено на експорт даних з ЄС.

GDPR спрямований перш за все на те, щоб дати громадянам контроль над власними персональними даними, і на спрощення нормативної бази для

міжнародних економічних відносин шляхом уніфікації регулювання в рамках ЄС.

Компанії яким потрібно впроваджувати GDPR:

– мають постійне представництво в ЄС;

– не мають постійного представництва, але обробляють персональні дані людей (суб'єктів персональних даних), які знаходяться в одній з країн ЄС і можуть мати громадянство іншої держави;

– співпрацюють з організаціями, які вже імплементували GDPR і для збереження свого статусу зобов'язані вибирати підрядника за тим же принципом.

Ключові принципи GDPR:

– Законність, справедливість і прозорість - повинні бути легальні підстави в рамках GDPR для збору і використання даних, непорушення будь-яких законів, відкритість, чесність від початку і до кінця про використання персональних даних;

– Конкретні цілі - все конкретні завдання повинні бути закріплені в політиці конфіденційності і повинні чітко дотримуватися;

– Мінімізація використаних даних - використання адекватної кількості даних для виконання поставлених цілей обмежених тільки необхідною кількістю;

– Точність - персональні дані повинні бути точними і не повинні вводити в оману; виправлення неправильних;

– Обмеження зберігання даних - не зберігати дані довше ніж потрібно, періодично проводити аудит даних і видаляти невикористовувані;

– Цілісність і конфіденційність / безпеку - зберігати дані в безпечному місці і приділяти достатню увагу збереження даних;

– Підзвітність - відповідальність за обробку персональних даних та

виконання всіх інших принципів GDPR включаючи записи про конфіденційність; захисту, використання, перевірки даних; призначення посадової особи щодо захисту даних

2.2. Розробка рекомендацій щодо проведення аудиту об’єктів электронной комерції.

Основними цілями проведення робіт з аудиту ІБ є:

– Незалежна оцінка поточного рівня захищеності інформаційної інфраструктури для прийняття рішення про її модернізації;

– Ідентифікація та оцінка вразливостей;

– Визначення відповідності СУІБ завданням і бізнес-цілям компанії;

– Відповідність вимогам чинного законодавства України і міжнародних стандартів;

– Мінімізація ризиків ІБ.

Завданнями аудиту інформаційної безпеки об’єктів електронної коммерції є:

– аналіз наявних нормативних і організаційно-розпорядчих документів про порядок функціонування інформаційної системи (ІС) і захисту інформації об’єкту електронної коммерції;

– аналіз структури, складу, принципів функціонування ІС і існуючої системи захисту інформації;

– оцінка ефективності існуючої системи захисту ІС із застосуванням спеціалізованих інструментаріїв і експертних оцінок за існуючими методиками;

– аналіз загроз безпеки інформації;

– оцінка показників захищеності об’єкту електронної коммерції;

–розробка інструкцій по здійсненню внутрішнього аудиту інформаційної безпеки

– вироблення конкретних рекомендацій з розробки політики безпеки і

варіантів її практичної реалізації комплексом організаційних заходів, програмно-апаратних, технічних та інших засобів.

Для проведення аудиту безпеки об’єктів електронної коммерції рекомендована наступна программа аудиту.

Етап I.

Планування робіт:

- визначення меж проведення аудиту;
- визначення робочої групи проекту;
- розробка календарного плану проведення аудиту та ін.

Етап II.

Обстеження і збір інформації:

- запит необхідної інформації;
- проведення анкетування;
- проведення інтерв'ювання;
- аналіз бізнес-процесів і цілей компанії; виділення основних інформаційних активів;
- ідентифікація основних інформаційних потоків;
- обстеження IT-інфраструктури та наявних механізмів захисту інформації;

Етап III.

Аналіз і оцінка отриманих даних:

- аналіз повноти і змісту існуючої організаційно-розпорядчої документації, вимогам щодо захисту інформації;
- визначення рівня захищеності IT-інфраструктури;
- аналіз і оцінка ризиків, пов'язаних із загрозами безпеці інформаційних ресурсів тощо.

Етап IV.

Розробка рекомендацій та Звіту аудиту:

- розробка рекомендацій щодо мінімізації ризиків виявлених загроз ІБ;

– розробка рекомендацій щодо вдосконалення системи інформаційної безпеки;

– розробка рекомендацій по налаштування та конфігурації IT-рішень і засобів захисту;

– розробка рекомендацій та звіту аудиту.

Рекомендовано проводити аудит інформаційної безпеки об’єктів електронної коммерції відповідно до:

1) Міжнародних, національних та галузевих стандартів

ISO 27001. Інформаційні технології. Методи захисту. Системи менеджменту захисту інформації. Вимоги.

ISO 27005. Інформаційна технологія - Методи і засоби забезпечення безпеки - Менеджмент ризику інформаційної безпеки.

ISO 27002. Інформаційні технології. Звід правил по управлінню захистом інформації, зокрема про сервіси електронної коммерції (розділ 10)

Повинні бути розглянуті наслідки для безпеки і вимоги до механізмів контролю, пов'язані з використанням сервісів електронної комерції, включаючи онлайнові транзакції. Також слід розглянути питання забезпечення цілісності та доступності інформації, що публікується в електронній формі через загальнодоступні системи.

Інформація, яка використовується в електронній комерції і передається через мережі загального користування, повинна бути захищена від шахрайських дій, заперечування договору, а також від несанкціонованого розкриття та модифікації.

Керівництво по впровадженню

Аналіз факторів безпеки для електронної комерції повинен включати в себе наступне:

– рівень довіри, який потрібно для підтвердження автентичності кожної зі сторін, наприклад, шляхом аутентифікації;

– процеси авторизації, що стосуються того, хто уповноважений

встановлювати ціни, випускати або підписувати ключові комерційні документи;

– надання гарантій того, що торгові партнери повністю інформовані про свої авторизації;

– визначення і виконання вимог до конфіденційності, цілісності, підтвердження відправки та отримання ключових документів, неможливості відмови від договірних зобов'язань, наприклад, пов'язаних з тендерними або договірними процесами;

– необхідний рівень довіри до цілісності рекламованих прайс-листів;

– конфіденційність будь-яких чутливих даних або інформації;

– конфіденційність і цілісність будь-яких транзакцій, пов'язаних із замовленнями, інформації про оплату, адреси доставки та підтвердження отримання;

– ступінь контролю, необхідна для перевірки платіжної інформації, отриманої від покупця;

– вибір найбільш підходящої для захисту від шахрайства форми платежу;

– рівень захисту, необхідний для забезпечення конфіденційності і цілісності інформації про замовлення;

– резервне копіювання інформації в транзакціях;

– відповідальність за будь-які шахрайські транзакції;

– вимоги по страхуванню.

Багато з перерахованих вище завдань можуть бути вирішені шляхом застосування криптографічних методів, беручи до уваги дотримання вимог законодавства.

Угоди про електронну комерцію між торговими партнерами повинні бути підкріплені письмовим договором, в якому обидві сторони погоджуються з умовами торгівлі, включаючи деталі авторизації. Також можуть бути необхідні інші угоди з провайдерами інформаційних сервісів і мережевими провайдерами.

Загальнодоступні торгові системи повинні публікувати умови надання послуг для клієнтів.

Необхідно приділити увагу забезпеченню стійкості вузла, використовуваного для електронної комерції, до атак і вплив на безпеку будь-яких мережевих з'єднань, необхідних для реалізації сервісів електронної комерції.

Додаткова інформація

Електронна комерція вразлива до великої кількості мережевих загроз, які можуть привести до шахрайства, розбіжностей за контрактом, а також до розкриття або модифікації інформації.

В електронній комерції можуть застосовуватися безпечні методи аутентифікації, наприклад, використання криптографії з відкритими ключами або цифрових підписів для зменшення ризиків. Також там, де такі сервіси потрібні, можуть використовуватися довірені треті сторони.

Онлайнові транзакції

Інформація, залучена в онлайнові транзакції, повинна бути захищена з метою запобігання незавершеною передачі, неправильної маршрутизації, несанкціонованого зміни переданих повідомлень, несанкціонованого розкриття вмісту, дублювання або повторної відправки повідомлень.

Керівництво по впровадженню

Розглянуті аспекти безпеки онлайнових транзакцій повинні включати в себе наступне:

– використання електронних підписів усіма сторонами, які беруть участь в транзакції;

– всі аспекти транзакції, наприклад, надання гарантій того, що:

– призначені для користувача повноваження всіх учасників перевірені і мають силу;

– транзакція залишається конфіденційною; і зберігається конфіденційність персональних даних учасників;

– канал зв'язку між усіма учасниками зашифрований;

– протоколи, використовувані для взаємодії між усіма учасниками, захищені;

– надання гарантій того, що зберігання деталей транзакції здійснюється поза будь-якої середовища загального доступу, наприклад, на платформі зберігання, існуючої в Інтранет мережі організації, і деталі транзакції не потрапляють на носій даних, до якого є прямий доступ з Інтернет;

– там, де використовується довірена особа (наприклад, для випуску і підтримки цифрових підписів і / або цифрових сертифікатів), безпека інтегрована і вбудована в процес управління сертифікатами / підписами.

Загальнодоступна інформація

Слід подбати про забезпечення цілісності інформації в системах загального доступу, для запобігання несанкціонованої модифікації.

Програмне забезпечення, дані та інша інформація, для якої потрібне забезпечення високого рівня цілісності, розміщена в загальнодоступних системах, повинна бути захищена відповідними механізмами, наприклад, цифровими підписами. Загальнодоступна система повинна тестуватися на уразливості і відмови, перш ніж до інформації буде надано доступ.

Повинен існувати процес формальної авторизації, перш ніж інформація буде зроблена загальнодоступною. Крім того, всі вхідні дані, що надаються системі ззовні, повинні перевірятися і затверджуватися.

Системи електронних публікацій, особливо допускають зворотний зв'язок і пряме введення інформації, повинні ретельно контролюватися таким чином, щоб:

– інформація добувалася у відповідності з усіма законодавчими актами про захист даних;

– інформація, що вводиться або обробляється в системах електронних публікацій, оброблялася своєчасно, з необхідною точністю і повнотою;

– забезпечувався захист конфіденційної інформації в процесі її

накопичення і зберігання;

– доступ до системи електронних публікацій, не допускав ненавмисного доступу до мереж, до яких вона підключена.

Додаткова інформація

Інформація в загальнодоступній системі, наприклад, інформація на Web-сервері, доступному через мережу Інтернет, повинна відповідати законам, правилам і постановам в тій юрисдикції, в якій знаходиться система, здійснюється комерційна діяльність або знаходиться власник (и) системи. Несанкціонована модифікація інформації, що публікується інформації може зашкодити репутації організації, яка її публікує.

Стандарт безпеки інфраструктури платіжних карт - PCI DSS.

PCI DSS визначає наступні шість областей контролю і 12 основних вимог з безпеки.

А саме:

Побудова і супровід захищеної мережі

Вимога 1: установка та забезпечення функціонування міжмережевих екранів для захисту даних власників карток.

Вимога 2: невикористання виставлених за замовчуванням виробниками системних паролів та інших параметрів безпеки.

Захист даних власників карток

Вимога 3: забезпечення захисту даних власників карток в ході їх зберігання.

Вимога 4: забезпечення шифрування даних власників карток при їх передачі через загальнодоступні мережі.

Підтримка програми управління уразливими

Вимога 5: використання і регулярне оновлення антивірусного програмного забезпечення.

Вимога 6: розробка та підтримка безпечних систем і додатків.

Реалізація заходів по строгому контролю доступу

Вимога 7: обмеження доступу до даних власників карток відповідно зі службовою необхідністю.

Вимога 8: присвоєння унікального ідентифікатора кожному особі, яка має доступ до інформаційної інфраструктури.

Вимога 9: обмеження фізичного доступу до даних власників карток.

Регулярний моніторинг і тестування мережі

Вимога 10: контроль і відстеження всіх сеансів доступу до мережевих ресурсів і даних власників карток.

Вимога 11: регулярне тестування систем і процесів забезпечення безпеки.

Підтримка політики інформаційної безпеки

Вимога 12: розробка, підтримка та виконання політики інформаційної безпеки.

НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

2 Також рекомендовано проводити аудит інформаційної безпеки об’єктів електронної коммерції відповідно до законодавчої бази:

– Закону України «Про захист персональних даних»;

– Закону України «Про інформацію»;

– Закону України «Про наукову і науково-технічну діяльність»;

– Закону України « Про доступ до публічної інформації»;

– Закону України «Про електронні документи та електронний документообіг»;

– Закону України «Про електронний цифровий підпис»;

– Закону України «Про захист інформації в інформаційно телекомунікаційних системах»;

3 Внутрішньо організаційно-розпорядчих документів компанії.

2.3. Аудит об’єктів електронної комерції на прикладі інтернет магазину.

2.3.1 Загальні відомості про організацію

У роботі розглянуто товариство з обмеженою відповідальністю «Авалон Днепр», яке займається оптовим та роздрібним продажем кави, чаю, та кавового обладнання через Інтернет – магазин, та через магазин у місті. Фірма здійснює доставку продукції по всій території України.

Повна назва підприємства: Товариство з обмеженою відповідальністю «Авалон Днепр».

Адреса: м. Дніпро, вул. Богдана Хмельницького 152. Форма власності: приватна власність.

2.3.2 Організаційна структура підприємства

Підприємство працює кожен день з 9.00 – 19.00.

Оформити замовлення на сайті, можливо в будь-який час.

Графік роботи співробітників:

Директор, заступник директора, бухгалтер, системний адміністратор – 9.00 – 19.00 у будні дні. Перерва з 12.00 – 12.30.

Охоронці (по одному на зміну) - 08.00-16.00, 16.00-24.00, 24.00-08.00

Прибирання приміщення проводиться кожного буднього дня з 9.30 до 10.00.

Завідуючі складом, Продавці, Відділ продажу - 7-денний робочий тиждень, по одному на зміну: 09.00-19.00, вихідні за розкладом в різні дні. Перерва встановлюється за індивідуальним графіком.

Штатна чисельність співробітників:

- директор – 1 людина;
- заступник директора – 1 людина;
- бухгалтер – 1 людина;
- відділ продажу (співробітники Call –центру) – 5 чоловік;
- охоронці – 2 людини;
- системний адміністратор – 1 людина;

- завідуючі складом – 2 людини;
- продавці – 2 людини;
- прибиральниця – 2 людини;

Всього – 17 чоловік;

2.3.3 Обстеження об’єкта інформаційної діяльності

Об'єкт знаходиться в двоповерховій будівлі, розташованій на вулиці із середнім рівнем руху транспортних засобів в спальному районі.

Офіс підприємства знаходиться на першому поверсі. На першому поверсі знаходяться офіси підприємств, що займаються діяльністю в сфері продажів та приватні приміщення.

На другому поверсі знаходяться приватні приміщення. Контрольована зона (КЗ) визначена наказом керівника підприємства №1 від 17.03.2009 р і обмежена

- з східної сторони знаходиться завод «Полімермаш».
- з західної і північної сторони знаходиться двоповерховий будинок .
- з північної сторони від знаходиться проспект Богдана Хмельницького.
- з західної сторони від знаходиться трансформаторна підстанція.
- з західно-південної сторони знаходиться двоповерховий будинок.

На ситуаційному плані підприємства показано місце розташування ОІД та розташовані навколо нього об’єкти.

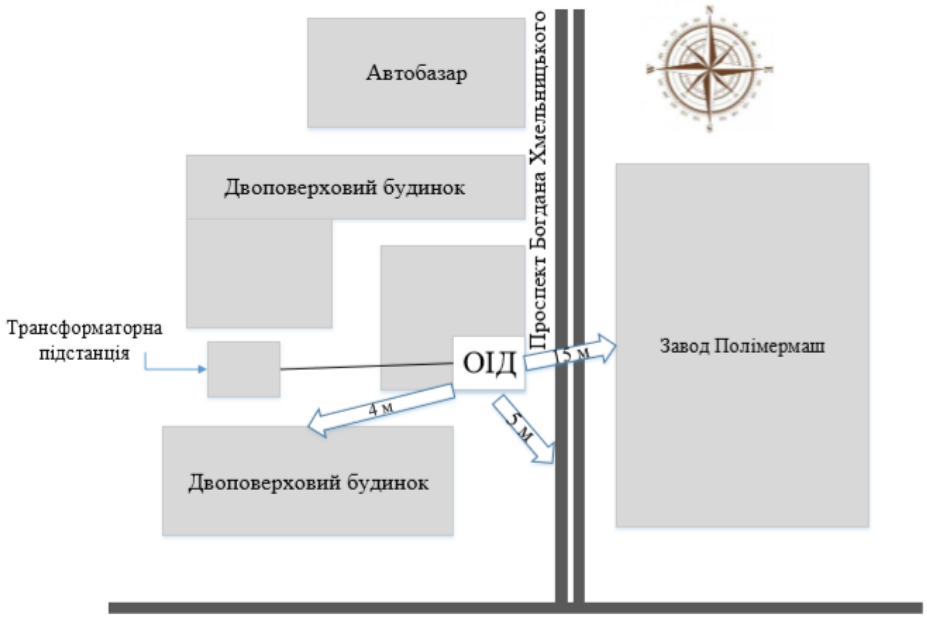

Рисунок 2.1 - Ситуаційний план підприємства

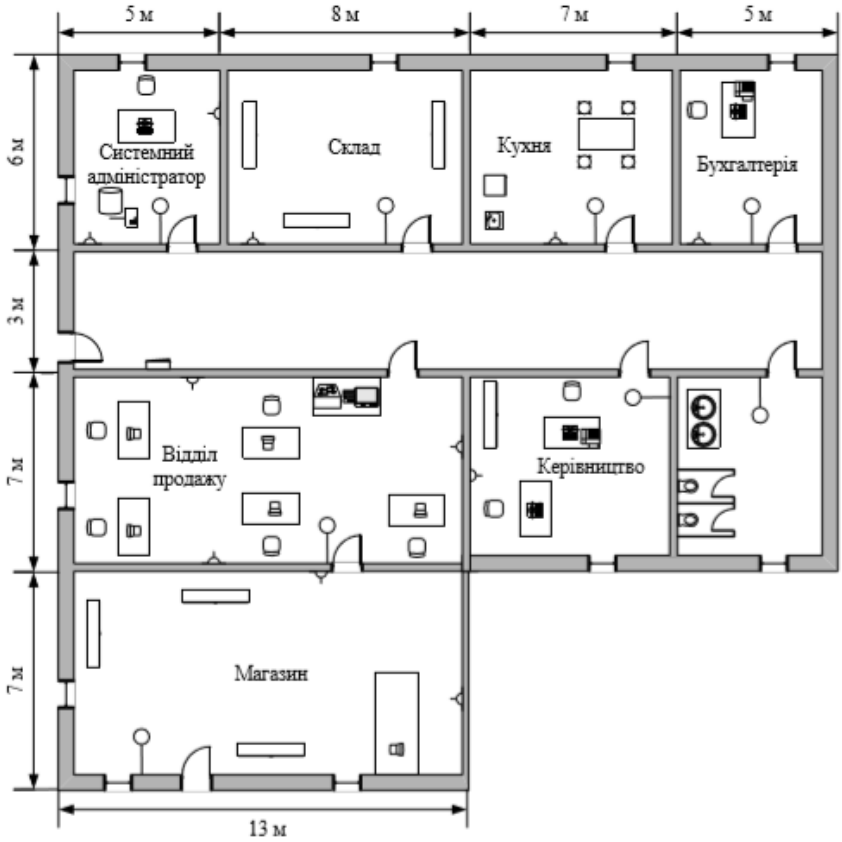

Рисунок 2.2 - Генеральний план ТОВ «Авалон Днепр»

Фізична характеристика об’єкта інформаційної діяльності:

- товщина несучих стін - 0,5 м;

- товщина перегородки - 0,25 м;
- склад стін - залізобетонні конструкції, висота перекриттів 2,6 м;
- склад перегородок - цегла, утеплений гіпсокартоном;
- стеля - залізобетонна монолітна заливна товщиною 150 мм;
- підлога - монолітна бетонна стяжка товщиною 100 мм;
- покриття підлоги – лінолеум 10 мм;
- вікна – 11 штук, зроблені з металопластику, розмірами 1400мм*1250мм, з 2камерним склопакетом;
- внутрішні двері – 8 штук, зроблені з ламінованого МДФ, розміром 1200 мм * 2000мм;
- зовнішні двері – 2 штуки, зроблені зі звареної листової сталі, оздоблені замком, розміром 1200 мм * 2000мм;
- електропостачання здійснюється через підключення до трансформаторної підстанції, виходить за межі контрольованої зони, розетки і вимикачі - 220 В;
- система опалення підключена до міської мережі опалення, знаходиться за межами КЗ (пластикові труби, однотрубна вертикальна система опалення);
- на об’єкті є Інтернет і телефонний зв'язок;
- підприємство обладнано системою контролю доступу. Режим доступу здійснюється через контрольно-пропускний пункт (тобто вхід в будівлю здійснюється за пропусками та через охорону).

2.3.4 Обстеження обчислювальної системи ТОВ «Авалон Днепр»

На території об’єкту знаходиться 10 комп’ютерів, у співробітників Call – центру – 5, по одному у директора, заступника директора, системного адміністратора, на складі, та у продавців (у магазині). Також у офісі є принтери, МФУ, стаціонарний та мобільний телефони. На усіх пристроях на підприємстві встановлено ліцензоване програмне забезпечення.

Мережу поділено на мережеві (робочі) групи – директор, заступник директора, системний адміністратор, бухгалтер, інші користувачі. Кожна з

цих мережевих груп має доступ лише до певної інформації та програм. У кожного працівника підприємства є свій обліковий запис, доступ до якого має лише він. Забезпеченням роботи комп'ютерної техніки, комп'ютерної мережі і програмного забезпечення в організації займається системний адміністратор. Використовувати зовнішні носії мають право лише директор, заступник директора та системний адміністратор. Усі співробітники мають доступ до Інтернету, але з обмеженням доступу до соціальних мереж. Усі співробітники мають доступ до факсу та принтеру.

Вихід комп'ютерів до мережі Інтернет забезпечується через кабель. На рисунку 2.3 зображена схема мережі інформаційно-телекомунікаційної системи ТОВ «Авалон Днепр».

Рисунок 2.3 - Структурна схема мережі інформаційно-телекомунікаційної системи ТОВ «Авалон Днепр».

У таблицях 2.2 і 2.3 представлений перелік апаратного і програмного забезпечення мережі ТОВ «Авалон Днепр».

Таблиця 2.1 – Апаратне забезпечення системи

№	Найменування	Характеристика	Кількість
1	Робоча станція	Модель: ASUS M52AD	5
2	Комутатор	Модель: D-Link DES-1016C	1
3	Принтер	Модель: HP LaserJet M127fw with Wi-Fi (CZ183A)	2
4	Сервер	Patriot Tower E3-1220V3: Intel Xeon Quad-Core E3-1220 v3 (3.1 ГГц)/ 8 ГБ/ 2 x Seagate ST500NM0011 500 ГБ, 64 МБ, Constellation ES, Serial ATA 6 Гбіт/с	1
5	Wi-Fi роутер	Модель: TP-LINK TLWR940N	1
6	Монітор	Модель: 23.8" LG 24MP58VQ-P	5
7	Ноутбук	Модель: Acer Aspire ES1-533P2WF	5
8	Клавіатура	Модель: Roccat Isku USB (ROC-12-731)	5
9	Мишка	Модель: Asus Strix Claw (90YH00C1-BAUA00)	5
10	МФУ	Модель: Canon i-SENSYS MF4410	1

Таблиця 2.2 – Програмне забезпечення системи

№	Тип програмного забезпечення	Найменування
1	2	3
1	Операційна система	Windows 7

Продовження таблиці 2.2

	2	3
	Прикладне ПЗ	Microsoft Office 2010
		Opera
		Avast Internet Security (антівірус)
		WinRaR (архіватор)
3	Бухгалтерія	1С: Підприємство 7.7, 8.0 (управління підприємством, бухоблік)
4	Склад	1С: Предприятие 7.7 Работа с торговым оборудованием
5	ПЗ для роботи операторів	Skype
		WebPhone
6	Операційна система (сервіс)	Microsoft Windows Server 2003 SP1 R2 Standard Edition Rus VLC

2.3.5 Аналіз загроз інформації

Загроза інформації — будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації або нанесення збитків автоматизованій системі.

Для виявлення порушників та загроз, які вони можуть реалізовувати щодо інформації, особливо з обмеженим доступом, на підприємствах роблять аналіз загроз та модель порушника.

Загроза інформації, що циркулює в інформаційній системі, залежить від її структури та конфігурації, технології оброблення інформації в ній, стану навколишнього фізичного середовища, а також дій персоналу. Зазвичай загроза є наслідком наявності вразливих місць у захисті інформаційних систем.

До найбільш важливих властивостей загрози відносяться вибірковість, передбачуваність та шкідливість. Вибірковість характеризує націленість загрози на нанесення шкоди тим чи іншим конкретним властивостям об'єкта безпеки. Передбачуваність характеризує наявність ознак виникнення загрози, що дозволяють заздалегідь прогнозувати можливість появи загрози і визначати конкретні об'єкти безпеки, на які вона буде спрямована. Шкідливість характеризує можливість нанесення шкоди різної тяжкості об'єкту безпеки. Шкода, як правило, може бути оцінена вартістю витрат на ліквідацію наслідків прояви загрози або на запобігання її появи.

Носіями загроз безпеці інформації є джерела загроз. Всі джерела загроз безпеці інформації, що циркулює в корпоративній мережі можна розділити на три основні групи:

- загрози, обумовлені діями суб'єкта (антропогенні загрози);
- загрози, обумовлені технічними засобами (техногенні загрози);
- загрози, обумовлені стихійними джерелами.

1 Антропогенними джерелами загроз виступають суб'єкти, дії яких можуть бути кваліфіковані як навмисні або випадкові злочини. Антропогенні загрози також поділяють на зовнішні і внутрішні.

Зовнішні джерела можуть бути випадковими або навмисними і мати різний рівень кваліфікації. До них відносяться дії кримінальних структур; рецидивістів і потенційних злочинців; партнерів; конкурентів; політичних супротивників.

Внутрішні суб'єкти (джерела), як правило, представляють собою висококваліфікованих спеціалістів у галузі розробки та експлуатації

програмного забезпечення та технічних засобів, які знайомі зі специфікою завдань, що вирішуються, структурою та основними функціями та принципами роботи програмно-апаратних засобів захисту інформації, та які мають можливість використання штатного обладнання та технічних засобів мереж. До них відносяться:

- основний персонал (користувачі, системний адміністратор, керівники);
- допоміжний персонал (прибиральники, охорона).

2 Техногенні загрози визначаються технократичною діяльністю людини та розвитком цивілізації. Загрози, пов’язані з втратою або псуванням інформації внаслідок виходу з ладу обладнання, які важко спрогнозувати и майже неможливо попередити. До цієї групи входять як зовнішні так і внутрішні джерела.

3 Стихійні джерела потенційних загроз інформаційній безпеці, як правило, є зовнішніми по відношенню до об'єкта захисту. Під ними розуміють, насамперед, природні катаклізми. Такі джерела загроз абсолютно не піддаються прогнозуванню, і тому заходи захисту від них повинні застосовуватися завжди.

Аналіз загроз наведен у таблиці 2.6

Таблиця 2.3 – Аналіз загроз

№	Джерело загрози	Вразливість	Загроза
1	2	3	4
Антропогенні			
1	Персонал підприємства	Вільний доступ співробітників до чужих робочих місць	Перегляд інформації співробітниками, які не допущені до обробки інформації з обмеженим доступом

Продовження таблиці 2.3

1	2	3	4
2	Персонал підприємства	Відсутність зобов'язання про нерозголошення інформації	Розголошення інформації, модифікація, знищення співробітниками допущеними до її обробки
3	Персонал підприємства (системний адміністратор)	Несвоєчасне оновлення системи антивірусного захисту	Модифікація інформації, знищення інформації
4	Персонал підприємства	Необізнаність в питаннях безпеки	Помилки персоналу при роботі з інформацією
Техногенні (внутрішні)			
1	Зовнішні (засоби зв'язку, мережі інженерних комунікації). Внутрішні (неякісні технічні та програмні засоби обробки інформації)	Відсутність резервного копіювання	Втрата або модифікація інформації через вихід з ладу апаратно-програмних засобів
2		Неякісні апаратне та програмні засоби, кидки напруг.	
3		Нестабільне електропостачання.	
4		Дія на обладнання коливань напруги.	

Продовження таблиці 2.3

1	2	3	4
Стихійні			
1	Пожежі		
2	Землетруси		
3	Підтоплення		

2.3.5 Модель порушника

Модель порушника – абстрактний формалізований або неформалізований опис порушника.

Порушники бувають внутрішні (ті, що працюють в організації) та зовнішні (наприклад, постачальники послуг). Порушниками можуть бути: - персонал підприємства;

- постачальники товарів;
- відвідувачі магазину;
- конкуренти;
- кримінальні структури;
- персонал, що обслуговує комунікації (наприклад, Internet, лінії телефонного зв’язку).

Згідно НД ТЗІ 1.4-001-200 порушник класифікується за різними рівнями (рівнем можливостей, рівнем знань, за використовуваними методами і способами, за місцем здійснення дії)

За рівнем можливостей порушники поділяються на:

1 Найнижчий рівень можливостей користування АС, можливість запуску визначеного набору програм, що виконують заздалегідь передбачені функції обробки інформації.

2 Можливість запускати і створювати власні програми, які можуть виконувати нові функції обробки інформації.

3 Можливість управління програмним забезпеченням АС.

4 Можливість здійснювати проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення АС, а також включення до складу АС власних засобів з новими функціями обробки інформації.

За рівнем знань порушники поділяються на:

1 Не володіють інформацією про АС.

2 Знають функціональні особливості АС, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами.

3 Мають високий рівень знань і досвід роботи з технічними засобами системи.

4 Володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації АС.

5 Володіють інформацією про функції та механізм дії засобів захисту.

За використовуваними методами і способами порушники поділяються на:

1 Використовують лише агентурні методи одержання інформації.

2 Використовують технічні засоби для перехоплення інформаційних сигналів.

3 Використовують недоліки проектування КСЗІ або штатні засоби АС для реалізації спроб несанкціонованого доступу.

4 Використовують способи і засоби активного впливу на АС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ тощо).

За місцем дії порушники можуть класифікуватися як:

1 Не мають доступу на контрольовану територію, та не мають доступу до АС.

2 Мають доступ на контрольовану територію, але не мають доступу до АС.

3 Мають доступ до робочих місць користувачів АС.

4 Мають доступ до місць накопичення і зберігання даних.

5 Мають доступ до засобів керування КСЗІ і до засобів адміністрування АС. Після аналізу можливих порушників було складено модель порушника, яка наведена у таблиці 2.7

Таблиця 2.4 – Модель порушника

№	Порушник	За рівнем можливостей	За рівнем знань	За використовуваними методами і способами	За місцем дії
1	2	3	4	5	6
Внутрішні					
1	Директор	3	4	3	5
2	Заступник директора	2	4	3	4
3	Бухгалтер	2	4	3	4
4	Відділ продажу	1	2	3	3
5	Охоронці	1	1	2	2
6	Системний адміністратор	4	5	3	5
7	Завідуючий складом	1	3	3	3
8	Продавці	1	2	2	3
9	Прибиральниці	1	1	1	2

Продовження таблиці 2.4

Зовнішні					
1	Відвідувачі	1	1	1	2
2	Конкуренти	1	1	1	2
3	Кримінальні структури	1	1	1	2
4	Персонал, що обслуговує комунікації	1	1	1	2
5	Постачальники товару	1	1	1	2

2.3.6 Аналіз ризиків

Згідно з ISO/IEC 27000 аналіз ризику це - процес розуміння характеру ризику і визначення рівня ризику.

В якості критеріїв оцінки ступеню небезпеки виберемо:

Можливість виникнення джерела (К1) - визначає ступінь доступності до об’єкта захисту (для антропогенних джерел), віддаленість від об'єкта, що захищається (для техногенних джерел) або особливості обстановки (для випадкових джерел).

Готовність джерела (К2) - визначає ступінь кваліфікації і привабливість здійснення діянь з боку джерела загрози (для антропогенних джерел), або наявність необхідних умов (для техногенних і стихійних джерел).

Фатальність (К3) і - визначає ступінь непереборності наслідків реалізації загрози. Кожний показник оцінюється від 1 до 5. Причому, 1 відповідає мінімальному обсязі впливу оцінюваного показника на небезпеку використання джерела, а 5 - максимальному.

Загальну оцінку для окремого джерела (К) можна визначити як відношення вищенаведених показників до максимального значення (125).

$$К = \frac{К1 * К2 * К3}{125} \quad (2.1)$$

Таблиця 2.5 – Аналіз ризиків

№	Загроза	К1	К2	К3	К
1	2	3	4	5	6
1	Перегляд інформації співробітниками, які не допущені до обробки інформації з обмеженим доступом	4	3	3	0.288
2	Розголошення інформації, модифікація, знищення співробітниками допущеними до її обробки	4	2	3	0.192
3	Модифікація інформації, знищення інформації	4	3	3	0.288
4	Помилки персоналу при роботі з інформацією	4	3	4	0.384
5	Втрата або модифікація інформації через вихід з ладу апаратно-програмних засобів	4	3	4	0.384
6	Стихійні лиха	1	1	1	0.008

2.3.7 Профіль захищеності WEB-сторінки

Згідно з нормативними документами НД ТЗІ 2.5-010-03 потрібно визначити критерії захищеності даної WEB-сторінки. Так як, WEB-сервер розміщується у оператора, а робочі станції – на території власника WEB-сторінки, взаємодія яких з WEB-сервером здійснюється з використанням мереж передачі даних (технологія Т2), мінімально необхідний функціональний профіль визначається:

КА-2, КВ-1,

ЦА-1, ЦО-1, ЦВ-1,

ДВ-1, ДР-1,

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

Результати попереднього обстеження наведені в таблиці 2.6

Таблиця 2.6. – Виконання критеріїв профілю

№	Позначення профілю	Значення	Виконання (+/-)
1	КА-2	Базова адміністративна конфіденційність	+
2	КВ-1	Конфіденційність при обміні	+
3	ЦА-1	Мінімальна адміністративна цілісність	+
4	ЦО-1	Відкат	-
5	ЦВ-1	Цілісність при обміні	-
6	ДВ-1	Відновлення після збоїв	+
7	ДР-1	Використання ресурсів	+
8	НР-2	Реєстрація	+
9	НИ-2	Ідентифікація і автентифікація	+
10	НК-1	Достовірний канал	+
11	НО-1	Розподіл обов’язків	-
12	НЦ-1	Цілісність комплексу засобів захисту	+
13	НТ-1	Самотестування	+
14	НВ-1	Ідентифікація і автентифікація при обміні	-

1 Базова адміністративна конфіденційність

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об’єкта. Доступ до загальнодоступної інформації встановлюється для користувачів усіх категорій. Призначення атрибутів доступу користувачам і процесам до захищених об'єктів

здійснюється адміністратором безпеки на основі аналізу функціональних та службових обов'язків окремих користувачів.

КЗЗ повинен надавати тільки адміністратору безпеки права доступу до технологічної інформації КСЗІ та процесів, що забезпечують її актуалізацію, супроводження та аналіз. Доступ до процесів, що забезпечують ведення системних процесів з адміністрування й забезпечення функціонування АС в цілому, окремих її компонентів та сервісів, а також до технологічної інформації щодо управління АС повинен надаватись тільки користувачам, які мають відповідні повноваження.

Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністратора безпеки.

Так як в системі, адміністратор безпеки та користувачі, яким надані повноваження щодо супроводження WEB-сторінки проходять процедури ідентифікації і автентифікації, можно зробити висновок, що ця послуга реалізується.

2 Конфіденційність при обміні

КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об’єкті, який передається.

КЗЗ повинен забезпечувати можливість реєстрації подій, які призвели або можуть призвести до порушення конфіденційності інформації, що міститься в об’єктах, які передаються.

Ця послуга реалізується. В системі реалізується шифрування файлів перед їх передачею каналами зв'язку.

3 Мінімальна адміністративна цілісність

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувачів і захищених об’єктів. Розмежування доступу здійснюється на рівні надання (встановлення заборони) користувачеві прав модифікувати об’єкт.

Право визначати множину об'єктів АС, цілісність яких забезпечується КЗЗ, надається адміністратору безпеки.

КЗЗ повинен надавати можливість адміністратору безпеки для кожного захищеного об’єкта визначити домен, якому повинні належати ті користувачі і/або групи користувачів, що мають право модифікувати об’єкт. Тільки йому надається право включати і вилучати користувачів та об'єкти до/з конкретних доменів.

Користувачі не мають права модифікувати об’єкти, тому ця послуга реалізується.

4 Відкат

Ця послуга забезпечує можливість відмінити окрему операцію або послідовність операцій і повернути захищений об'єкт після внесення до нього змін до попереднього наперед визначеного стану.

Політика обмеженого відкату стосується користувачів, яким надано право супроводження КСЗІ та управління АС; об’єктів, які містять публічну інформацію; функціонального програмного забезпечення, що використовується для актуалізації, захисту публічної інформації та супроводження WEB-сторінки; створеної в процесі супроводження WEB-сторінки технологічної інформації КСЗІ та технологічної інформації щодо управління АС. Якщо стосовно якогось з об’єктів зазначених категорій в процесі обробки не передбачається можливості його модифікації, політика послуги на нього не розповсюджується.

Ця послуга не реалізована в системі. Для задоволення вимоги ЦО-1 функціонального профілю захищеності можна скористатися засобами резервного копіювання.

5 Цілісність при обміні

КЗЗ повинен забезпечувати контроль за цілісністю інформації в повідомленнях, які передаються, а також бути здатним виявляти факти їх несанкціонованого видалення або дублювання.

КЗЗ повинен забезпечувати можливість реєстрації подій, які призвели до порушення цілісності повідомлень, їх несанкціонованого видалення або дублювання.

Ця послуга не реалізована в системі. Для задоволення вимоги ЦВ-1 функціонального профілю захищеності цінні документи при передачі через незахищене середовище повинні завірятися ЕЦП.

6 Відновлення після збоїв

Політика відновлення після збоїв, що реалізується КЗЗ, стосується: системного та функціонального програмного забезпечення; засобів захисту інформації та засобів управління КСЗІ; засобів адміністрування та управління обчислювальною системою АС – і гарантує повернення АС у відомий захищений стан після відмов або переривання обслуговування, спричинених помилковими діями користувачів, неврахованою функціональною недостатністю програмного та апаратного забезпечення (наприклад, можливою наявністю не виявлених під час проектування незадекларованих функцій), іншими непередбачуваними ситуаціями.

Можна створити контрольні точки відновлення системи та відстежити, які файли буде видалено або додано після відновлення комп'ютера. Можна використати функцію «Відновлення системи».

Ця послуга реалізована.

7 Використання ресурсів

КЗЗ повинен реалізувати рівень ДР-1.

Ця послуга дозволяє керувати використанням користувачами послуг та ресурсів.

Політика використання ресурсів, що реалізується КЗЗ, стосується: користувачів загальнодоступної інформації; адміністратора безпеки та користувачів, яким надано повноваження щодо управління АС; файлової системи; системного та функціонального програмного забезпечення; технологічної інформації щодо управління АС; окремих периферійних

пристроїв (принтерів, накопичувачів інформації і т.ін.); обчислювальних ресурсів АС і передбачає можливість встановлення обмежень на їх використання.

Обмеження щодо використання окремим користувачем та/або процесом обсягів обчислювальних ресурсів АС або кількості об'єктів встановлюються адміністратором безпеки, тому ця послуга реалізована.

8 Реєстрація

Послуга дозволяє контролювати небезпечні відповідно до політики безпеки WEB-сторінки дії користувачів всіх категорій із захищеними об'єктами.

Політика реєстрації стосується: користувачів усіх категорій; публічної інформації WEB-сторінки; системного та функціонального програмного забезпечення, що використовується для актуалізації, захисту публічної інформації та супроводження WEB-сторінки; створеної в процесі супроводження WEB-сторінки технологічної інформації КСЗІ та технологічної інформації щодо управління АС.

КЗЗ повинен забезпечувати реєстрацію всіх подій, які мають безпосереднє відношення до безпеки.

Ця послуга реалізується.

9 Ідентифікація і автентифікація

КЗЗ повинен однозначно ідентифікувати категорії користувачів WEB-сторінки і за атрибутами кожної з цих категорій визначати послуги, що їм доступні. Ідентифікація здійснюється на підставі особистого імені та/або IP-адреси користувача.

КЗЗ повинен автентифікувати адміністратора WEB-сторінки, співробітників СЗІ та користувачів, які мають повноваження щодо управління АС, з використанням захищеного механізму на підставі особистого пароля. Автентифікація користувачів, що мають виключне право доступу тільки до публічної інформації, не здійснюється.

Дозвіл на виконання будь-яких дій з інформацією та обладнанням WEB-сторінки, що контролюються КЗЗ, надається користувачу тільки після успішного завершення процедур ідентифікації та/або автентифікації його КЗЗ відповідно до категорії користувача.

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

Користувачі, перед тим, як скористатися своїм обліковім записом, вводять ім’я і пароль, які зберігаються в базі у адміністратора. Отже, ця послуга реалізована.

10 Достовірний канал

Ця послуга повинна гарантувати користувачу будь-якої категорії можливість безпосередньої взаємодії з КЗЗ, а також те, що ніяка взаємодія користувача з АС не може бути модифікованою іншим користувачем або процесом. Послуга визначає вимоги до механізму встановлення достовірного зв'язку між користувачем і КЗЗ.

Політика достовірного каналу стосується користувачів усіх категорій та компонентів системного та функціонального програмного забезпечення, які задіяні для реалізації механізмів КЗЗ.

Ця умова виконується, так як забезпечується засобами операційної системи серверу.

11 Розподіл обов’язків

Ця послуга дозволяє розмежувати повноваження користувачів, визначивши категорії користувачів з певними і притаманними для кожної з категорій функціями (ролі). Послуга призначена для зменшення потенційних збитків від навмисних або помилкових дій користувачів і обмеження авторитарності керування АС.

Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Умова не виконується, оскільки немає окремих адміністратора безпеки та

системного адміністратора. Для задоволення вимоги, НО-2 функціонального профілю захищеності було вирішено призначити заступника директора виконувати обов’язки менеджера з інформаційної безпеки.

12 Цілісність комплексу засобів захисту

КЗЗ повинен реалізувати рівень НЦ-1.

Ця послуга визначає міру здатності КЗЗ WEB-сторінки захищати себе і гарантувати свою спроможність керувати захищеними об’єктами.

Політика цілісності КЗЗ повинна визначати склад КЗЗ, механізми контролю цілісності його компонентів та порядок їх використання.

Ця послуга реалізована.

13 Самотестування

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій захисту WEB-сторінки.

Політика самотестування поширюється на адміністратора безпеки, компоненти системного та функціонального програмного забезпечення, які задіяні для реалізації механізмів КЗЗ, засоби захисту інформації.

До складу КЗЗ повинна входити множина тестових процедур, яка враховує особливості функціонування компонентів конкретної WEB-сторінки і достатня для оцінки правильності виконання всіх критичних для безпеки публічної та технологічної інформації КСЗІ функцій, а сам КЗЗ повинен бути здатним контролювати їх виконання.

Ця послуга реалізована.

14 Ідентифікація і автентифікація при обміні

Ця послуга дозволяє у разі використання технології Т2 компонентам КЗЗ WEB-сервера і віддаленої робочої станції здійснити взаємну ідентифікацію, перш ніж розпочати взаємодію.

Послуга ідентифікації і автентифікації при обміні стосується адміністратора безпеки та користувачів, яким надані повноваження щодо супроводження WEB-сторінки, технологічної інформації КСЗІ.

КЗЗ повинен надавати доступ до процесів, що забезпечують ініціалізацію обміну даними, тільки адміністратору безпеки і користувачам, яким надано повноваження щодо супроводження WEB-сторінки.

Ця послуга не реалізована. Для реалізації цієї послуги потрібно виключити можливість несанкціонованого зовнішнього підключення та встановити між мережевий екран.

2.3.8 Рекомендації щодо підвищення рівня інфомаційної безпеки

Згідно з ISO/IEC 27002 рекомендується

– Забезпечити рівень довіри, який потрібно для підтвердження автентичності кожної зі сторін, наприклад, шляхом аутентифікації;

– Встановити процеси авторизації, для директора, заступника директора, бухгалтера;

– Надання гарантій того, що торгові партнери повністю інформовані про свої авторизації;

– Визначення і виконання вимог до конфіденційності, цілісності, підтвердження відправки та отримання ключових документів, неможливості відмови від договірних зобов'язань, наприклад, пов'язаних з тендерними або договірними процесами;

– Забезпечити необхідний рівень довіри до цілісності рекламованих прайс-листів;

– Забезпечити конфіденційність і цілісність будь-яких транзакцій, пов'язаних із замовленнями, інформації про оплату, адреси доставки та підтвердження отримання;

– Ступінь контролю, необхідна для перевірки платіжної інформації, отриманої від покупця;

– Вибір найбільш підходящої для захисту від шахрайства форми платежу;

– Забезпечити рівень захисту, необхідний для забезпечення конфіденційності і цілісності інформації про замовлення;

Рекомендації щодо онлайнових транзакції:

– Використання електронних підписів усіма сторонами, які беруть участь в транзакції;

– Транзакція залишається конфіденційною; і зберігається конфіденційність персональних даних учасників;

– Канал зв'язку між усіма учасниками зашифрований;

– Протоколи, використовувані для взаємодії між усіма учасниками, захищені;

Рекомендації щодо загальнодоступної інформації.

Системи електронних публікацій, особливо допускають зворотний зв'язок і пряме введення інформації, повинні ретельно контролюватися таким чином, щоб:

– інформація добувалася у відповідності з усіма законодавчими актами про захист даних;

– інформація, що вводиться або обробляється в системах електронних публікацій, оброблялася своєчасно, з необхідною точністю і повнотою;

– забезпечувався захист конфіденційної інформації в процесі її накопичення і зберігання;

Рекомендується отримати сертифікат відповідності стандарту безпеки даних індустрії платіжних карт PCI DSS.

Так як, ТОВ “Авалон Днепр” обробляє до 20 000 транзакцій у рік, необхідний 4 рівень сертифікації.

Вимоги до сертифікації:

– рекомендована щорічна самооцінка відповідності із заповненням опитувального листа;

– рекомендовано щоквартальне ASV-сканування;

– вимоги визначаються банком-еквайром.

Згідно стандарту необхідно забезпечити:

– установка та забезпечення функціонування міжмережевих екранів для захисту даних власників карток.

– невикористання виставлених за замовчуванням виробниками системних паролів та інших параметрів безпеки.

– забезпечення захисту даних власників карток в ході їх зберігання.

– забезпечення шифрування даних власників карток при їх передачі через загальнодоступні мережі.

– використання і регулярне оновлення антивірусного програмного забезпечення.

– розробка та підтримка безпечних систем і додатків.

– обмеження доступу до даних власників карток відповідно зі службовою необхідністю.

– присвоєння унікального ідентифікатора кожному особі, яка має доступ до інформаційної інфраструктури.

– обмеження фізичного доступу до даних власників карток.

– контроль і відстеження всіх сеансів доступу до мережевих ресурсів і даних власників карток.

– регулярне тестування систем і процесів забезпечення безпеки.

2.3.9 Аналіз ризиків після впровадження рекомендацій

У таблиці 2.10 проаналізовані рівень ризику після впровадження політики безпеки. Отже, можна зробити висновок, що після проведення аудиту ступінь небезпеки загроз була зменшена.

Таблиця 2.10 - Аналіз ризиків після впровадження рекомендацій

№	Загроза	К1	К2	К3	К
1	2	3	4	5	6
1	Перегляд інформації співробітниками, які не допущені до обробки інформації з обмеженим доступом	2	1	1	0.128
2	Розголошення інформації, модифікація, знищення співробітниками допущеними до її обробки	2	1	2	0.128
3	Модифікація інформації, знищення інформації	2	1	1	0.016
4	Помилки персоналу при роботі з інформацією	2	1	2	0.128
5	Втрата або модифікація інформації через вихід з ладу апаратно-програмних засобів	2	1	1	0.016
6	Стихійні лиха	1	1	1	0.008

2.4 Висновки

В другому розділі проаналізовані стандарти, згідно яких проводиться аудит інформаційної безпеки. Для проведення аудиту інформаційної безпеки об’єктів електронної коммерції рекомендовано використати: міжнародний стандарт ISO 27001:2013, стандарт PCI DSS, Закони України, нормативно-правові акти.

На прикладі інтернет-магазину ТОВ «Авалон Днепр», визначено, що аудит проведений згідно з цими рекомендаціями є ефективним.

РОЗДІЛ 3.ЕКОНОМІЧНА ЧАСТИНА

3.1.Розрахунок вартості проведення аудиту

Метою даного розділу є обґрунтування економічної доцільності проведення аудиту інтернет магазину ТОВ «Авалон Днепр»

Для визначення ефективності необхідно розрахувати:

1) витрати на проведення аудиту;

2) оцінку можливого збитку від атаки (злому) на вузол або сегмент мережі;

3) економічну доцільність проведення аудиту в організації

Витрати на проведення аудиту $К_{пб}$ складаються з часу, який витрачається на проведення аудиту в рік t, вартості одної години машинного часу ПК $С_{мч}$ та річного фонду заробітної плати інженерно-технічного персоналу , що обслуговує систему інформаційної безпеки $С_{з}$:

$$К_{пб} = t(С_{мч} + С_{з}) \quad (3.1)$$

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = P \cdot C_{e} + \frac{Ф_{перв} \cdot Н_{а}}{F_{р}} + \frac{К_{лпз} \cdot Н_{апз}}{F_{р}}, \frac{грн}{год}, \quad (3.2)$$

де Р – встановлена потужність ПК, кВт;

$С_{е}$ – тариф на електричну енергію, грн/кВт·година;

$Ф_{перв}$ – первісна вартість на ПК на початок року, грн;

$Н_{а}$– річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$– річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$– вартість ліцензійного програмного забезпечення, грн.;

$F_{р}$– річний фонд робочого часу (за 40-годинного робочого тижня Fр = 1920 год).

Заробітної плата за годину інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки $С_{з}$, складає:

$$С_з = \frac{(З_{осн}+З_{дод})\cdot 1,22}{160} \text{ грн,} \qquad (3.3)$$

де $З_{осн}$, $З_{дод}$ – основна і додаткова заробітна плата відповідно, грн. на рік.

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

У таблиці 3.1. наведено час t, який витрачається на реалізацію рекомендацій.

Таблиця 3.1 – Час на проведення аудиту

№	Задачі	t, год/рік
1	Планування робіт	15
2	Обстеження і збір інформації	75
3	Аналіз і оцінка отриманих даних	75
4	Розробка рекомендацій та Звіту аудиту	50

Отже, загальний час на проведення аудиту – 215 годин на рік.

Дані для розрахунку вартості 1 години машинного часу $С_{мч}$:

Р=0, 25 кВт;

$С_в$=1,68 грн/кВт·годин

Первісна вартість на ПК $Ф_{перв}$: 5628 грн.

Вартість ліцензійного програмного забезпечення $К_{лпз}$:

Таблиця 3.2 - Вартість ліцензійного програмного забезпечення

№	Найменування	Ціна
1	ABC Backup Pro	780 грн.
2	Avast Endpoint Security	560 грн.
3	AIDA64	1040 грн.
Всього $К_{лиз}$		2380 грн.

$$Н_а = \frac{1}{Т} = \frac{1}{4} = 0,25$$

$Н_{апз} = \frac{1}{Т} = \frac{1}{2} = 0,5$

$F_р$=1920 год;

$$С_{мч} = 0,25 \cdot 1,68 + \frac{5628 \cdot 0,25}{1920} + \frac{2380 \cdot 0,5}{1920} = 1,7 \text{ грн/год}$$

Дані для розрахунку заробітної плати інженерно-технічного персоналу $С_з$:

$З_{осн}$ системного адміністратора = 6700 грн. на місяць;

$З_{дод}$ системного адміністратора = 536 грн. на місяць;

$З_{осн}$менеджера з інформаційної безпеки = 6500 грн. на місяць;

$З_{дод}$ менеджера з інформаційної безпеки = 520 грн. на місяць.

Заробітна плата за годину системного адміністратора:

$$C_з = \frac{(З_{осн} + З_{дод}) * 1,22}{160} = \frac{7236 * 1,22}{160} = 55, 17 \text{ грн. / год}$$

Заробітна плата за годину менеджера з інформаційної безпеки:

$$C_з = \frac{(З_{осн} + З_{дод}) * 1,22}{160} = \frac{6500 * 1,22}{160} = 49, 56 \text{ грн. / год}$$

$$К_{пб} = 215(1,7+55,17+49,56) = 22\ 882 \text{ грн}$$

Таким чином, час на проведення аудиту становить 92 години на рік, а витрати на проведення аудиту 22 882 грн.

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пб} + К_{пз} + К_{навч} \qquad (3.4)$$

де $К_{пб}$ – витрати на проведення аудиту, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн

$К_{навч}$ –витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн;

К = 22 882 + 2380 + 5000 + 30 262 грн.

3.2 Розрахунок експлуатаційних витрат

Річні експлуатаційні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к , \text{ тис. грн.,} \quad (3.5)$$

де $С_в$ - витрати на Upgrade-відновлення й модернізацію системи інформаційної безпеки;

$С_к$ - витрати на керування системою інформаційної безпеки;

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{єв} + С_{ел} + С_{тос}, \text{ грн.,} \quad (3.6)$$

де $С_н$ - витрати на навчання адміністративного персоналу;

$С_а$ - річний фонд амортизаційних відрахувань;

$С_з$ - річний фонд заробітної плати інженерно-технічного персоналу;

$С_{єв}$ - розмір єдиного внеску (22% від фонду ЗП);

$С_е$ - вартість електроенергії;

$С_{тос}$ - витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки.

Річний фонд амортизаційних відрахувань (Са) визначається за видами основних засобів

Апаратне забезпечення

Програмне забезпечення

$$С_а = К_{пз} = 2380/2 = 1\ 190 \text{ грн.} \quad (3.7)$$

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

$$С_з = (З_{зп} + 22\%) * N * m = 17392*12 = 208707 \text{ грн.} \quad (3.8)$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($С_{тос}$) у відсотках від вартості капітальних витрат (1-3%).

Витрати на керування системою інформаційної безпеки складають:

$$С_к = 3000+1\ 190+208707+3136+806,4+1635=218\ 474 \text{грн}$$

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

$$С = 5000 + 218\ 474 = 223\ 474 \text{ грн.}$$

3.3 Оцінка можливого збитку від атаки (злому) на вузол або сегмент мережі

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = (П_п + П_в) \sum i \sum n \quad , \quad (3.9)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки:

$$П_П = \frac{\sum Зс}{F} \cdot t_П \quad , \qquad (3.10)$$

де F – місячний фонд робочого часу (становить 160 ч);

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн на місяць;

tп–час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин.

$$П_п = \sum 17392*6/160 \cdot 4 = 2608 \text{ грн.}$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \qquad (3.11)$$

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

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

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

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ВИ} = \frac{\sum Зс}{F} \cdot t_{ВИ} \quad , \qquad (3.12)$$

де $t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин;

$$П_{ви} = \sum 17392 \cdot 6/160 \cdot 12 = 7826 \text{ грн.}$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{ПВ} = \frac{\sum Зо}{F} \cdot t_В \quad , \tag{3.13}$$

де $t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

$$П_{пв} = \sum 17392 \cdot 6/160 \cdot 8 = 5217 \text{ грн.}$$

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

$$U = (2608+7826+5217+5000) \cdot 6 \cdot 10 = 1\ 239\ 184 \text{ грн.}$$

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C, \tag{3.14}$$

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

$$E = 1\ 239\ 184 \cdot 0.4 - 233725 = 261\ 948 \text{ грн.}$$

3.3 Оцінка економічної ефективності системи захисту інформації

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

б) коефіцієнт повернення інвестицій (ROSI) (Return on Investment for Security);

в) термін окупності капітальних інвестицій T_o.

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

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

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,} \qquad (3.15)$$

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

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

ROSI = 223 474/22 882 = 9,7

При цьому проект визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта:

$$ROSI\ (N_{деп} - N_{інф})/100), \qquad (3.16)$$

де $N_{деп}$ – річна депозитна ставка або прибутковість альтернативного варіанту вкладення коштів, 18%;

$N_{інф}$ – річний рівень інфляції, 13,7%.

9,7 (18-13,7)/100

9,7 0,041

Для вибраного варіанта визначається розрахунковий строк окупності капітальних інвестицій T_o.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки

$$T_O = \frac{K}{E} = \frac{1}{ROSI} \quad (3.17)$$

T_o=0,1=36 днів

3.4 Висновки до третього розділу

Витрати на проведення аудиту складають 22 882 грн.

Збиток від простою атакованого вузла або сегмента корпоративної мережі складається з оплачуваних втрат робочого часу та простою співробітників атакованого вузла або сегмента корпоративної мережі і вартості відновлення працездатності вузла або сегмента корпоративної мережі.

Загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складає 223 474 грн.

Термін окупності капітальних інвестицій складає 36 днів.

ВИСНОВКИ

Під час виконання дипломної роботи було проаналізовано проблеми інформаційної безпеки об’єктів електронної коммерції, методи проведення аудиту інформаційної безпеки, стандарти, згідно критеріїв яких проводиться аудит інформаційної безпеки. Також було розглянуто особливості проведення аудиту інформаційної безпеки, проаналізовано нормативно-правову базу України в області захисту інформації.

В спеціальній частині були розроблені рекомендації щодо проведення аудиту інформаційної безпеки об’єктів електронної коммерції, була запропонована програма проведення аудиту об’єктів електронної коммерції, наведені критерії, згідно яких потрібно проводити аудит.

На прикладі інтернет магазину ТОВ “Авалон Днепр” перевірено ефективність аудиту.

В економічному розділі розраховані витрати на впровадження рекомендацій.

ПЕРЕЛІК ПОСИЛАНЬ

1. Цивільний Кодекс України - Стаття 505 ЦКУ від 16.01.2003 № 435
2. Закон України «Про доступ до публічної інформації» - Ст. 7
3. ISO/IEC TR 18044:2004 «Менеджмент інцидієнтів інформаційної безпеки» - ст. 27
4. ISO/IEC 27001
5. Кримінальний Кодекс України - Стаття 231 із змінами, внесеними згідно із Законом N 2252-IV від 16.12.2004
6. Кримінальний Кодекс України, Стаття 232
7. Кримінальний Кодекс України, ст. 362
8. Адміністративний Кодекс України, ст.212
9. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» - Чинний від 2000-12-15 - ДСТСЗІ СБ України - ст. 17
10. Закон України "Про захист інформації в інформаційно телекомунікаційних системах"
11. Закон України «Про державну таємницю»
12. Закон України «Про захист персональних даних»
13. НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»
14. 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”
15. Закон України «Про інформацію»
16. НД ТЗІ 1.1-003-99 “Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу”

17. НД ТЗІ 1.1-005-07 “Захист інформації на об’єктах інформаційної діяльності.Створення комплексу технічного захисту інформації. Передпроектні роботи”
18. НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі"
19. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»
20. Шваб Л. Основи підприємництва: Навч. посібник/ Людмила Іллівна Шваб,.– К.: Каравела, 2006. - 343 с.
21. Шипицына, И.В. Технологии электронной коммерции: Учеб. Пособие И.В.
22. 104. Электронная коммерция : метод. указания / сост. : Н.В. Молоткова, М.А.
23. 105. Электронная коммерция: уч. пособие / под ред. проф. Брагина –
24. 106. Электронная коммерция: уч. пособие / под ред. проф. Брагина –
25. 107. Электронная коммерция: Учебное пособие / В.В. Ежунинов– ДУЭП, 2005.

ДОДАТОК А. Відомість матеріалів дипломного проекту

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	20	
6	А4	2 Розділ	41	
7	А4	3 Розділ	8	
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 файлів на електронному носії

1 Пояснювальна_записка_Скворцова_125м-17-2.docx

2 Презентація_до_диплома__Скворцова_125м-17-2.pptx

ДОДАТОК В. Відгук керівника економічного розділу

Керівник: _____ к.е.н., доц. Пілова Д.П.
(підпис)

ДОДАТОК Г. Відгук

на дипломний проект бакалавра

студентки групи УБіт-13-1

Скворцової Дар’ї Андріївни

на тему: «Аудит об’єктів електронної коммерції»

Метою роботи є підвищення ефективності інформаційної безпеки об’єктів інформаційної безпеки за допомогою проведення аудиту інформаційної безпеки.

Тема дипломної роботи безпосередньо пов’язана з об’єктом діяльності фаху 125 “Кібербезпека”. Для досягнення поставленої мети в дипломному проекті вирішуються наступні задачі: розглянуто особливості проведення аудиту інформаційної безпеки, розроблено рекомендації щодо проведення аудиту інформаційної безпеки об’єктів електронної комерції; визначено ефективність проведення аудиту, на прикладі інтернет-магазину. Практична цінність полягає у розробці рекомендації щодо підвищення рівня інфомаційної безпеки об’єктів електронної комерції.

Оформлення пояснювальної записки до дипломної роботи виконано з деякими відхиленнями від стандартів.

За час дипломування Скворцова Д.А. проявила себе фахівцем, здатним самостійно вирішувати поставлені задачі.

Оцінка роботи_____

Керівник дипломної роботи,

д.т.н., проф кафедри БІТ, _____ Корнієнко В.І.

Керівник спеціальної частини,

ст. викл. кафедри БІТ, _____ Галушко С.О.