МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

Кафедра ЗІ



Робота

з дисципліни «Менеджмент інформаційної безпеки»

Виконав ст. УІ-42 Симоненко Д.С.

Перевірив Ромака В.А.

ЗМІСТ

ВСТУП.................................................................................................................................................3

Розділ 1. Опис об’єкта ІБ.........................................................................................................6

* 1. Місце розташування...............................................................................................................6
  2. Опис приміщення...................................................................................................................7

1.2.1. Система електропостачання...........................................................................................7

1.2.2. Система опалення та вентиляції. ..................................................................................8

1.2.3. Корпоративна комп’ютерна мережа.............................................................................9

* 1. Загальна характеристика роботи.........................................................................................10
  2. Персонал підприємства.......................................................................................................11
     1. Посадові інструкції........................................................................................................13
  3. Інформаційна система..........................................................................................................24
     1. Програмне забезпечення...............................................................................................24
     2. Технологічний процес...................................................................................................24
     3. Резервне копіювання даних..........................................................................................26
     4. План доходів і витрат підприємства............................................................................27
  4. Реєстр інформаційних активів.............................................................................................29

Розділ 2. Методика оцінювання ризику.....................................................................30

2.1. Методика оцінки ймовірності реалізації загрози..............................................................30

2.2. Методика оцінки збитку......................................................................................................34

Розділ 3. Оцінювання ризиків...........................................................................................36

ВИСНОВОК......................................................................................................................................46  
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ..................................................................................47

ВСТУП

В часи бурхливого розвитку інформаційних технологій різні підприємства, заводи, банки та інші установи, залежать від інформаційних систем. З розвитком інформаційних технологій розвиваються і способи їх захисту, але разом з ним розвиваються методи негативного впливу на них. Підприємство є відкритою системою, що матеріальним і інформаційним потоками зв'язана з постачальниками, споживачами, експедиторами і транспортними організаціями. Такий розвиток знань та технологій дає багато різноманітних можливостей впливу на підприємство, що може призвести до порушень в його роботі або навіть до повного банкротства. Інформаційні системи займають у цих технологіях центральне положення.

Це відбувається через те що запровадженні політики інформаційної безпеки мають багато недоліків і вразливих місць, які дають змогу зловмисникам нашкодити підприємству.

Різниця між порушенням роботи персонального комп’ютера та порушенням роботи цілої мережі підприємства може бути дуже великою. Якщо порушується робота одного окремого комп’ютера то постраждає невелика кількість інформації та людей, і їх збитки від цього будуть не великими, але коли порушується робота великої компанії з величезними прибутками тоді можуть постраждати велика кількість людей, які зв’язані з цим підприємством, і загальний збиток буде дуже великим. Все це може трапитись через вразливості інформаційних систем, тому забезпечення необхідного рівня інформаційної безпеки є досить важливою задачею, що дозволить підприємству уникнути великих втрат, а також це буде стимулювати розвиток підприємства.

В умовах інформатизації, пов'язаної з формуванням інформаційної економічної системи, величезне значення набувають Інтернет-технології, впровадження яких у маркетингову діяльність підприємств дозволяє останнім адаптуватися до сучасних ринкових умов, що сприяє підвищенню ефективності їх функціонування. У цьому і полягає актуальність обраної теми.

Приклад : *Останнє десятиріччя характеризується зростанням ролі інформаційних технологій, інтелектуальних факторів у розвитку економіки і суспільства****.***Ні земля, ні капітал, ні природні ресурси не могли зрівнятися з інформацією і знаннями за рівнем впливу на суспільно-економічний розвиток. Ті країни, які визначили своїми пріоритетами інтелектуальні ресурси, інформаційно-комунікаційні технології, домоглися надзвичайно високих результатів. Почесне місце серед них займає Фінляндія, яка ще на початку XX ст. була економічно відсталою країною і могла б залишатись такою довгі роки. Але фіни знайшли в собі сили, поставили високі історичні цілі побудови передової, сучасної економіки, яка базується на інформації і знаннях, і в дуже короткий історичний термін вийшли на передові позиції у світовій економіці.

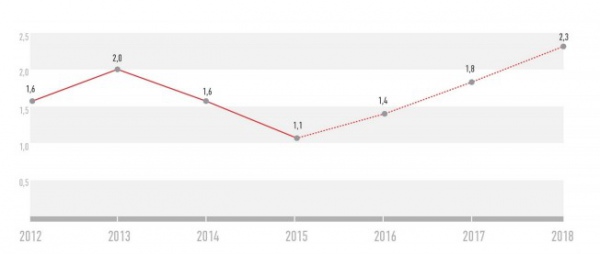
Отже, що ж становлять Інтернет-технології в маркетингу? Інтернет володіє унікальними характеристиками, які значно відрізняються від традиційних інструментів маркетингу. Однією з основних і найбільш яскравих характеристик Інтернету є гіпермедійна природа його побудови, що робить Інтернет високоефективним у поданні та засвоєнні інформації, що, в свою чергу, значно підвищує можливості маркетингу в посиленні взаємозв'язку виробників товарів та їх споживачів. Крім того, мережа Інтернет дозволяє укладати угоди, здійснювати покупки, проводити платежі, що надає Інтернету риси глобального електронного ринку. І, нарешті, Інтернет надзвичайно зближує продавців і покупців не лише в різних містах, але і на різних континентах .

Згідно із дослідженнями фахівців Intel, до 2014 року кількість користувачів Інтернету досягне 2 мільярдів, а оборот електронної комерції зросте до 1 трильйона доларів. Подібні досягнення свідчать про те, що компанія, яка не використовує **електронний бізнес** та електронну комерцію, може втратити свої позиції на ринку. Таким чином, у наш час, у тому числі завдяки маркетингу, що здійснюється через Інтернет, відбувається різке збільшення використання Інтернету, що стимулюється швидким збільшенням самих ресурсів мережі. Використання Інтернету в системі маркетингу може значно збільшити ефективність діяльності підприємства .

E-commerce в Україні: Усе більшу частину ринку електронної комерції відвойовує так звана мобільна комерція. За 2016 рік оператори обіцяють покрити 3G всю територію України, тож ще через рік проникнення мобайл очікується на рівні 50%.

Український ринок e-commerce перебуває лише на етапі становлення, водночас має значний потенціал для розвитку. Ринок електронної комерції в Україні, за даними Ekos Global, у 2014 році становив 1,6 млрд дол, у Польщі - 4,7 млрд дол, у Росії - 17,5 млрд дол. За прогнозами Української асоціації директ-маркетингу, у 2015 році обсяг ринку електронної комерції в доларах скоротиться приблизно на 45% до 1,1 млрд.

**Прогноз об’єму ринку e-commerce, мільярдів доларів**



Поряд із збільшенням ролі Інтернет-технологій у маркетингу все більш актуальною стає проблема забезпечення **інформаційної безпеки.** Заходи безпеки спрямовані на запобігання несанкціонованого отримання інформації, фізичного знищення або модифікації інформації, що захищається. Як показують зарубіжні публікації, можливості зловживання інформацією, що передається через Інтернет, розвивалися не менш інтенсивно, ніж засоби їх попередження. У цьому випадку для захисту інформації потрібно застосування не просто приватних механізмів захисту, а організація комплексу заходів із використанням спеціальних засобів, методів і заходів з метою запобігання втрати інформації .

**Під загрозою безпеки** розуміється будь-яка дія, яке може призвести до руйнування, спотворення або несанкціонованого використання інформаційних ресурсів, включаючи збережену, передану й інформацію що обробляються, а також програмні й апаратні засоби. Крім того, при розробці Інтернет-технологій виникає проблема з вирішення питання безпеки інформації, що становить комерційну таємницю, а також безпеки самих комп'ютерних інформаційних систем. Основні ознаки безпеки сучасних Інтернет-технологій

1) містять інформацію різного ступеня конфіденційності;

2) при передачі даних мають криптографічний захист інформації різного ступеня;

3) відображають ієрархічність повноважень суб'єктів, відкриваючи доступ до програм, **АРМ**,

файлів-серверів, каналів зв'язку та інформації системи;

4) оперативна зміна цих повноважень;:

5) обробка інформації у діалоговому режимі, в режимі поділу часу між користувачами і в

режимі реального часу;

6) реєструє і враховує спроби несанкціонованого доступу;

7) встановлює наявність засобів відновлення системи захисту інформації;

8) створює умови для фізичної охорони засобів обчислювальної техніки і носіїв інформації.

**Автоматизо́ване робо́че мі́сце** (*АРМ*) — індивідуальний комплекс технічних і програмних засобів, що призначений для автоматизації професійної праці фахівця і забезпечує підготовку, редагування , пошук і видачу на екран і друк  необхідних йому документів  і даних.

До основних засобів захисту відносяться такі :

1) технічні засоби становлять електричні, електромеханічні та електронні пристрої;

2) апаратні засоби становлять пристрої, що вбудовуються безпосередньо в обчислювальну

техніку;

3) фізичні засоби – це автономні пристрої та системи, наприклад, замки, ґрати, охоронна сигналізація тощо;

4) організаційні засоби захисту становлять організаційно-технічні та організаційно-правові

заходи, здійснювані в процесі створення й експлуатації обчислювальної техніки та апаратури телекомунікації;

5) морально-етичні засоби захисту реалізуються в результаті виконання різних норм і правил;

6) законодавчі засоби захисту визначаються законодавчими актами країни.

У практичній маркетинговій діяльності прийняття заходів і засобів захисту інформації включає такі самостійні напрями: *захист інформації від несанкціонованого доступу; захист інформації в системах зв'язку; захист юридичної значущості електронних документів; захист конфіденційної інформації від витоку каналами побічних електромагнітних випромінювань; захист інформації від комп'ютерних вірусів; захист від несанкціонованого копіювання програм .*

*Метою дослідження* є **аналіз ризиків** інформаційної безпеки інтернет-аукціону «Техноком», які пов’язані з використанням послуг електронної торгівлі, включаючи он-лайн угоди.

*Обєктом дослідження* є інформаційна система інтернет-аукціону «NewAuction.com.ua»

*Предметом дослідження* є ризики інформаційної безпеки,які виникають в процесі роботи інтернет-аукціону

*Для досягнення заданої мети необхідно було виконати наступні завдання:*

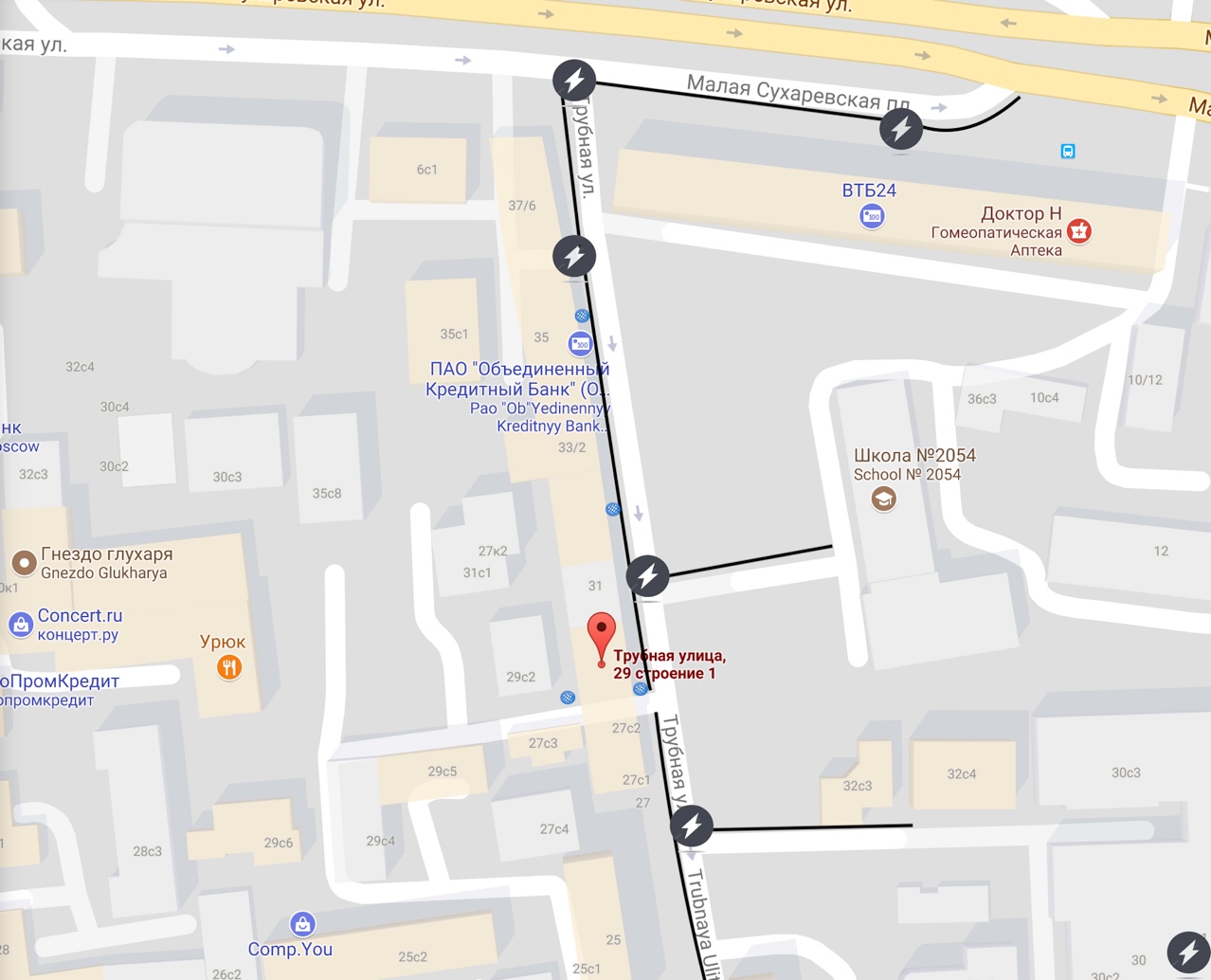
* Розглянути роботу підприємства
* Описати бізнес процес
* Ідентифікувати інформаційні активи
* Розробити методику оцінки ризику
* Дати оцінку існуючим ризикам

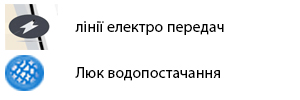
Розділ 1. Опис об’єкта ІБ

* 1. **Місце розташування.**

Приміщення інтернет-аукціону знаходиться в чотирьохповерховому будинку за адресою: Трубная вул., 29с1, Москва, Росія, 127051.Будинок має піздемну паркавку.

В цілому будинок здається під офісні приміщення. На відстанні 100 метрів знаходиться школа №2054 Ворота відчинені з 8:00 до 19:00. На об`єкті знаходиться люк водопостачання, трансформаторна підстанція, підземна парковка для працівників.





*рис.1.1 Загальна схема розміщення об’єкту та комунікацій*

* 1. **Опис приміщення.**

**1.2.1. Система електропостачання**

На територію об`єкту, до трансформаторної підстанції електроживлення підводиться з-за меж контрольованої зони (від міських ліній електропередач ПАТ «РоссЕнерго »). Від трансформаторної підстанції електромережа прокладена по периметру будинку (для забезпечення роботи освітлювальних ліхтарів, камер відео спостереження, датчиків руху та вібрації) та по периметру будівлі. Всередині будівлі електроживлення проведене по всіх кімнатах для систем освітлення та розеток. Вся проводка в приміщенні надійно заізольована та проводиться в спеціальних коробах. Для забезпечення струмовідведення у випадку короткого замикання всі електроприлади об`єднані в єдину мережу та мають надійне

заземлення (рис. 1.2).



*рис.1.2 Схема електропостачання*

**1.2.2. Система опалення та вентиляції.**

З метою забезпечення комфортних умов праці в осінню та зимову пори року, на підприємстві функціонує система опалення (рис. 1.3). Вона включає в себе котел для нагрівання води, батареї опалення та труби водопостачання. Вода з люку водопостачання через труби поступає на котел, який, гріючи воду, подає її на батареї опалення. Також будівля забезпечена системою кондиціонування для охолодження повітря в спекотний період.



*рис.1.3 Схема опалення та вентиляції*

**1.2.3. Корпоративна комп’ютерна мережа та Робочі місця**

На території об’єкту прокладено ККМ для забезпечення зв’язку між працівниками підприємства, доступу до локальної бази даних та публічного веб-сервера. Вихід в мережу Internet забезпечує інтернет-провайдер «Росс-Интернет ».

На базі роутера встановлено ПЗ проксі-сервера, який захищає локальну мережу від зовнішнього доступу.

**Персонал підприємства**

* директор (ПК 1) – очолює та координує роботу інтернет-аукціону, приймає та звільняє працівників, домовляється з постачальниками програмного забезпечення так всього що потребує офіс, керує фінансами компанії, проводить наради, видає накази та розпорядження, пов`язані з нормальним функціонуванням офісу;
* секретар (ПК 3) – відповідає на телефонні дзвінки, веде документацію підприємства.
* бухгалтер (ПК 2) – веде фінансову документацію підприємства, контролює та перевіряє законність та правильність здійснення фінансових операцій.
* системний адміністратор (ПК 8) – працівник, посадові обов’язки якого передбачають забезпечення роботи комп’ютерної техніки, комп’ютерної мережі і програмного забезпечення в організації, а також проектування та керування корпоративної бази даних.
* адміністратор веб-сервера (ПК 9) – фахівець, що займається встановленням, налаштуванням і управлінням програмного забезпечення веб-серверів.
* рекламний агент (ПК 7) – займається рекламою підприємства та продукції, після продажною роботою з клієнтами.
* менеджер з продажу (ПК 4, ПК 5) – кваліфіковані спеціалісти, в обов`язки яких входять: робота з клієнтами, оформлення замовлень, ведення документації.
* консультант (ПК 6) – відповідає на дзвінки на гарячу лінію, допомагає здійснити замовлення.
* охоронець (2 чол., приміщення охорони) – здійснюють безпосередній нагляд за безпекою організації. Контролюють стан безпеки на об`єкті.
* прибиральник (1 чол., тех.. приміщення) – займається підтримкою чистоти приміщень.

*рис.1.4 Корпоративна комп’ютерна мережа та* Робочі місця



* 1. **Загальна характеристика роботи.**

Інтернет-аукціон займається влащткванням інтернет торгів наступних товарів:

* мобільні телефони
* КПК / смартфони
* цифрова техніка
* портативне аудіо
* GPS
* ноутбуки
* портативні планшети
* ігрові консолі, ПЗ
* телевізори
* аксесуари
* карти пам'яті
* …..

Для залучення членів в інтернет-аукціон використовуються наступні методи:

* Пошукова оптимізація.

Під цим терміном мається на увазі внутрішня і зовнішня оптимізація сайту. Сторінки товарів оптимізуються під ключові запити, головна сторінка оптимізується під тип товарів, що продається в інтернет-аукціоні. Під зовнішньою оптимізацією розуміється розкрутка сайту в пошукових системах за допомогою закупівлі посилань, статей, а також інших способів.

* Реклама в соціальних мережах.

Реклама в В Контакте, Facebook, Twitter Google реклама та інших відомих сервісах.

* Реклама в газетах.

Покупець, зайшовши на сайт і ознайомившись з умовамиаукціону, починає переглядати пропонований перелік товарів. Вподобаний за ціною або технічним характеристикам продукт він заходить на аукціон та пропонує свою ставку за товар в реальному часу.

Пісял того як товар був проданий людини , яка запропонувала найвишу ставку, псля того можна приступати до оформлення замовлення. Для цього покупець повинен вказати свою поштову адресу, куди буде відправлена ​​посилка, і телефон, за яким з ним зможе зв'язатися консультант магазину для підтвердження замовлення.

Далі інтернет-аукціон підтверджує замовлення та уточнює деталі доставки за допомогою дзвінка по телефону+ e-mail повідомлення та повідомляю їх власнику товара.

Після узгодження дати доставки і способу оплати, замовлення готується до відправки. Для цього його ретельно упаковують, після чого відправляють кур’єрською службою.

Новий власник товару отримає Трекінг номер та дату доставки.

* + 1. **Посадові інструкції.**

* + - 1. **Посадова інструкція директора інтернет-аукціону**

**1. Загальні положення:**

1. Посада "Директор інтернет-аукціону" відноситься до категорії "Керівники".

2. Директор знає та застосовує у діяльності:  
      - чинне законодавство України, що регламентує підприємницьку діяльність;  
      - нормативно-правові акти та документи з державного регулювання функціонування підприємств торгівлі та організації продажу продовольчих та непродовольчих товарів;  
      - основи економіки, менеджменту, маркетингу та інш.;  
      - номенклатуру, асортимент товарів, що продаються в магазині, їх властивості та призначення;  
      - стандарти та технічні вимоги до якості товарів;  
      - правила складування та зберігання товарів;  
      - вітчизняну та зарубіжну практику з організації та технології торгівлі;  
      - види торгово-технологічного устаткування та обладнання, їх будову та правила експлуатації;  
      - завдання та обов'язки працівників магазину, їх права;  
      - основи психології та етики в торгівлі, організацію нормування та оплати праці;  
      - трудове законодавство;  
      - порядок організації та ведення обліково-звітної та іншої встановленої для торгівлі документації;  
      - правила проведення інвентаризації товарно-матеріальних цінностей;  
      - правила роботи магазину та внутрішнього трудового розпорядку;  
      - категорії і види стандартів, іншу нормативно-технічну документацію щодо сертифікації якості товарів та послуг у торгівлі;  
      - правила конкурентних взаємовідносин;  
      - правила і норми охорони праці, протипожежного захисту, виробничої санітарії та особистої гігієни.

**2. Посадові обов'язки:**

1. Керує діяльністю працівників магазину, спрямованою на забезпечення процесу обслуговування покупців.

2. Готує заявки на поставку товарів, контролює ритмічність надходження товарів та їх відповідність поданим заявкам.

3. Перевіряє наявність супровідних документів, сертифікатів відповідності, посвідчень про якість та відповідність товарів чинним стандартам та вимогам.

4. Організує вивчення попиту на види товарів та послуг, які задовольняють потреби споживачів.

5. Впроваджує прогресивні форми торгівлі та методи продажу товарів.

6. Оперативно розглядає скарги покупців і вживає заходів щодо усунення порушень та недоліків у роботі працівників магазину.

7. Організує атестацію та раціоналізацію робочих місць.

8. Організує підвищення кваліфікації персоналу.

9. Приймає пропозиції та розробляє заходи щодо поліпшення комерційної та фінансово-господарської діяльності, раціонального використання матеріальних, трудових та фінансових ресурсів, бере участь у розробленні заходів щодо економічного та соціального розвитку колективу, укладанні колективного договору.

10. Оцінює ефективність трудової діяльності працівників та вирішує питання щодо матеріального та морального їх заохочення.

11. Веде обліково-звітну, статистичну та іншу встановлену документацію, контролює складання звітності та своєчасне її подання працівниками магазину.

12. Контролює додержання працівниками підприємства правил і норм охорони праці, протипожежного захисту, виробничої санітарії та особистої гігієни, своєчасне проходження ними в установленому порядку медичного огляду.

**3. Посадові повноваження:**

**Директор магазину має право:**

1. Вживати дії для запобігання та усунення випадків будь-яких порушень або невідповідностей.

2. Знайомитися з проектами документів, що стосуються його діяльності.

3. Повідомляти про виявлені в процесі своєї діяльності порушення і невідповідності і вносити пропозиції щодо їх усунення.

* + - 1. **Посадова інструкція системного адміністратора**

**1. Загальні положення:**

1. Адміністратор системи безпосередньо підпорядковується директору організації. також використання

2. Посадова інструкція визначає посадові обов'язки, повноваження й відповідальність, а також умови роботи адміністратора системи.

3. Адміністратор системи призначається на посаду й звільняється з посади відповідно до чинного трудового законодавства розпорядженням директора організації.

4. У період тимчасової відсутності адміністратора системи його обов'язки виконує особа, призначена у встановленому порядку. Дана особа отримує відповідні права й відповідає за виконання зазначених обов'язків.

**2. Посадові обов'язки:**

1. Консультувати працівників організації з питань використання обчислювальної техніки й комп'ютерних інформаційних технологій.

2. Здійснювати інсталяцію, настроювання й оптимізацію системного програмного забезпечення, і освоєння прикладних програмних засобів.

3. Розробляти й впроваджувати прикладні програми.

4. Здійснювати підключення й заміну зовнішніх обладнань, проводити тестування засобів обчислювальної техніки.

5. Забезпечувати ведення комп'ютерних баз даних.

6. Проводити комп'ютерні антивірусні заходи.

7. Брати участь в адмініструванні локальної обчислювальної мережі організації.

8. Здійснювати тестування й ремонт окремих обладнань, засобів обчислювальної техніки, кабельних ліній локальної мережі.

9. Усувати аварійні ситуації, пов'язані з ушкодженням програмного забезпечення й баз даних.

10. Організовувати тестування й навчання співробітників організації основам

комп'ютерної грамотності й роботі із прикладними програмними засобами.

11. Забезпечувати технічний супровід застосовуваних локальних мереж і програмного забезпечення.

12. Організовувати ремонт засобів обчислювальної техніки із залученням спеціалізованих установ.

13. Здійснювати систематичний аналіз ринку апаратних засобів і програмного

забезпечення.

14. Підготовляти пропозиції про придбання, розробку або обмін апаратного забезпечення.

15. Здійснювати своєчасне повідомлення про плани модернізації апаратного й

програмного забезпечення.

16. Виконувати окремі службові доручення безпосереднього керівника.

17. Виконувати правила трудового розпорядку, прийняті в організації.

**3. Посадові повноваження:**

1. Запитувати від співробітників і керівників організації інформацію й документи, необхідні для виконання своїх посадових обов'язків.

2. Знайомитися з документами, що визначають права й обов'язки по займаній посаді, критеріями оцінки якості виконання посадових обов'язків.

3. Вносити на розгляд керівництва пропозиції з удосконалювання роботи, пов'язаної з передбаченими даною інструкцією обов'язками.

**4. Посадова відповідальність:**

Системний адміністратор несе відповідальність за:

1. Підтримання програм і баз даних в актуальному стані;
2. Виконання організаційно-технічних заходів, що забезпечують збереження інформації при збоях і відмовах комп’ютерного обладнання;
3. Обмін інформацією (в т.ч. по мережах телекомунікацій) відповідно до встановленого порядку;
4. Виконання заходів, що перешкоджають зараженню комп’ютерного обладнання комп'ютерними вірусами;
5. Виконання правил техніки безпеки при експлуатації комп’ютерного обладнання;
6. Нерозголошення відомостей, що становлять державну, службову та комерційну таємницю.
   * + 1. **Посадова інструкція адміністратора веб-сервера**

**1. Загальні положення:**

1. Адміністратор сервера підпорядковується директору підприємства.
2. Адміністратор сервера приймається на роботу і звільняється з роботи наказом директора підприємства.
3. У своїй діяльності адміністратор сервера керується:   
   - нормативними документами з питань виконуваної роботи;   
   - методичними матеріалами, що стосуються відповідних питань;   
   - статутом підприємства;   
   - правилами трудового розпорядку;   
   - наказами та розпорядженнями директора підприємства   
   - цією посадовою інструкцією.
4. Адміністратор сервера повинен знати:   
   - нормативні правові акти, інші методичні матеріали та нормативні документи, що стосуються методів програмування і застосування засобів обчислювальної техніки і комп'ютерних інформаційних технологій;   
   - протоколи та принципи функціонування Інтернету;   
   - об'єкт, якому присвячений сервер (просувати продукцію, послуги);   
   - HTML;   
   - операційну систему, під управлінням якої працює Web-сервер;   
   - основи Web-дизайну;   
   - мови програмування;   
   - основи трудового законодавства;   
   - правила і норми охорони праці та пожежної безпеки.
5. Під час відсутності адміністратора сервера його обов'язки виконує в установленому порядку призначається заступник, який несе повну відповідальність за належне виконання покладених на нього обов'язків.

**2. Посадові обов'язки:**

1. Здійснює інформаційно-технічну розробку Web-сервера (Web-вузла) і підтримує його в робочому стані.
2. Бере участь у визначенні цілей і завдань Web-проекту.
3. Здійснює проведення Web-маркетингу.
4. Розробляє гіпертекстове представлення сторінок вузла (інтерфейс Web-сервера) і концепцію подальшого розвитку Web-сервера.
5. Здійснює адміністрування Web-сервера і операційної системи, під управлінням якої працює Web-сервер.
6. Відбирає, аналізує, редагує і компонує матеріал для публікацій, розробляє анотації і визначає ключові слова.
7. Розмічає HTML-документи.
8. Налаштовує Web-сервер, організовує служби віддаленого адміністрування.
9. Організовує рекламу Web-сервера в Інтернеті.
10. Веде статистику звернень до Web-сервера, складає звіти за зверненнями з метою виявлення потенційних клієнтів і конкурентів.

**3. Посадові повноваження:**  
Адміністратор сервера має право:

1. Знайомитися з проектами рішень керівництва підприємства, що стосуються його діяльності.
2. Вносити на розгляд керівництва пропозиції щодо вдосконалення роботи, пов'язаної з обов'язками, що передбачені цією інструкцією.
3. Отримувати від керівників структурних підрозділів, фахівців інформацію та документи, необхідні для виконання своїх посадових обов'язків.
4. Залучати спеціалістів усіх структурних підрозділів підприємства для вирішення покладених на нього обов'язків (якщо це передбачено положеннями про структурні підрозділи, якщо ні - з дозволу керівника підприємства).
5. Вимагати від керівництва підприємства сприяння у виконанні своїх посадових обов'язків і прав.

**4. Посадова відповідальність:**

1. За невиконання посадових обов'язків.

2. За порушення правил внутрішнього розпорядку організації.

3. За порушення ділової етики.

4. За нераціональне використання комп'ютерної техніки.

5. За правопорушення, здійснені в процесі своєї діяльності, установлені чинним

законодавством України.

6. За розголошення інформації, що є службовою.

* + - 1. **Посадова інструкція рекламного агента**

**1. Загальні положення:**

1. Рекламний агент приймається і звільняється директором підприємства.
2. Основним завданням рекламного агента є здійснення організації роботи над проектом інтернет-аукціону, робота з клієнтами.
3. Рекламний агент безпосередньо підпорядкований директору підприємства.
4. Рекламний агент повинен знати:   
   - Процедури та іншу документацію за якістю, що відносяться до його діяльності;   
   - Основи реклами і маркетингу Інтернет проектів в Інтернеті,   
   - Принципи роботи пошукових машин, банерних мереж, каталогів web ресурсів;  
   - Володіти професійними навичками роботи і налаштування програмних продуктів MS Office, засобів доступу до ресурсів Інтернет.

**2. Посадові обов'язки:**

1. Розробка стратегії та планів розвитку інтернет-аукціону.
2. Забезпечення реалізації плану розвитку інтернет-аукціону.
3. Залучення і робота з клієнтами.
4. Аналіз відвідуваності ресурсу
5. Робота по просуванню розвитку інтернет-аукціону в Інтернеті.

**3. Посадові повноваження:**

Рекламний агент має право:

1. Приймати рішення в межах своєї компетенції.
2. Вимагати від керівництва створення нормальних умов для виконання службових обов'язків.
3. Подавати пропозиції з удосконалення своєї роботи.

**4. Посадова відповідальність:**

Рекламний агент несе відповідальність за:

1. Нечітке та несвоєчасне виконання своїх функціональних обов'язків, передбачених цією інструкцією.
2. Некоректну роботу з клієнтами.
3. Недостовірну інформацію про стан виконання, доручених йому робіт.
4. Порушення Правил внутрішнього трудового розпорядку, встановлених на підприємстві.
5. Розголошення відомостей, що становлять комерційну таємницю організації.
   * + 1. **Посадова інструкція менеджера з продажу**

**1. Загальні положення:**

1. Менеджер з продажу (далі менеджер) безпосередньо підпорядковується директору підприємства.
2. Менеджер повинен знати:  
   - порядок оформлення замовлень;  
   - час приймання і видавання замовлень;  
   - правила продажу товарів;  
   - правила експлуатації сучасних технічних засобів зв’язку;  
   - правила і норми охорони праці, протипожежного захисту, виробничої санітарії та особистої гігієни.

**2. Посадові обов’язки:**

1. Підтверджує замовлення, оформлені в інтернет магазині.
2. Оформляє замовлення із зазначенням найменування суб’єкта господарювання, назви товару, його ціни, кількості, загальної вартості товару, вартості послуг, що надаються додатково, дати (часу) виконання замовлення тощо.
3. Попереджає та пропонує споживачу, у разі відсутності якогось замовленого товару, відповідну заміну.
4. Визначає термін виконання замовлення.
5. Направляє відповідно оформлені замовлення у відділ доставки.

**3. Посадові повноваження:**  
Менеджер має право:

1. Ознайомлюватися з проектами рішень керівництва підприємства, що стосуються його діяльності.
2. Брати участь в обговоренні питань, що стосуються виконання його обов'язків.
3. Вносити на розгляд керівництва підприємства пропозиції щодо покращання роботи, пов'язаної з обов'язками, що передбачені цією інструкцією.
4. В межах своєї компетенції повідомляти керівництву підприємства про всі недоліки, виявлені в процесі його діяльності, та вносити пропозиції щодо їх усунення.
5. Вимагати від керівництва підприємства сприяння у виконанні ним посадових обов'язків.

**4. Посадова відповідальність:**  
Менеджер несе відповідальність:

1. За неналежне виконання або невиконання своїх посадових обов'язків, а також за невикористання або неповне використання своїх функціональних прав, що передбачені цією посадовою інструкцією, - в межах, визначених чинним законодавством України про працю.
2. За правопорушення, скоєні в процесі здійснення своєї діяльності, - в межах, визначених чинним адміністративним, кримінальним та цивільним законодавством України.
3. За завдання матеріальної шкоди - в межах, визначених чинним цивільним законодавством та законодавством про працю України.
   * + 1. **Посадова інструкція оператора відправки**

**1. Загальні положення:**

1. Оператор відправки (надалі - оператор) призначається на посаду і звільняється з посади наказом директора.  
2.Оператор безпосередньо підпорядковується директору.  
3. На час відсутності оператора його обов'язки виконує особа, призначена у встановленому порядку. Дана особа набуває відповідних прав і несе відповідальність за належне виконання покладених на нього обов'язків.

**2.Посадові обов’язки:**

1. Упаковка та відправлення замовлень.

2. Участь у роботі з аналізу та оцінки діяльності відділу доставки, розробка методів оптимізації процесу доставк

**3.Посадові повноваження:**

Оператор має право:  
1. Отримувати інформацію та технічну підтримку, необхідну для ефективного виконання своїх обов'язків.  
2. Знайомитися з проектами рішень керівництва підприємства, що стосуються його діяльності.  
3. Вносити на розгляд керівництва пропозиції по вдосконаленню роботи, пов'язаної з передбаченими цією посадовою інструкцій обов'язками.  
4. Повідомляти безпосередньому керівнику про всі виявлені у процесі виконання своїх посадових обов'язків невідповідності в роботі та вносити пропозиції щодо їх усунення.

**4.Посадова відповідальність:**

1. За невиконання або неналежне виконання цієї посадової інструкції.  
2. За правопорушення, скоєні в процесі здійснення своєї діяльності, в межах, визначених чинним адміністративним, кримінальним і цивільним законодавством України.  
3. За спричинення матеріального збитку - в межах, визначених чинним трудовим і цивільним законодавством України.

4. Повна матеріальна відповідальність цінності, що знаходяться під звітністю.  
5. За розголошення інформації, що становить комерційну таємницю компанії - в межах, визначених чинним трудовим і цивільним законодавством України

* + - 1. **Посадова інструкція бухгалтера**

**1. Загальні положення:**

1. Призначення на посаду бухгалтера та звільнення з неї здійснюється наказом директора підприємства з дотриманням вимог Кодексу законів про працю України.
2. Бухгалтер підпорядковується безпосередньо директору підприємства.
3. За відсутності бухгалтера його обов'язки виконує особа, при­значена у встановленому порядку), яка набуває відповідних прав та несе відповідальність за належне виконання покладених на неї обов'язків.

**2**. **Посадові обов'язки:**

1. Самостійно і в повному обсязі веде облік необоротних активів, запасів, коштів, розрахунків та інших активів, власного капіталу та зобов'язань, доходів та витрат за прийнятою на підприємстві формою бухгалтерського обліку з додержанням єдиних методологічних засад бухгалтерського обліку та з урахуванням особливостей діяльності підприємства й технології оброблення даних.
2. Забезпечує повне та достовірне відображення інформації, що міститься у прийнятих до обліку первинних документах, на рахунках бухгалтерського обліку.
3. За погодженням з власником (керівником) підприємства подає в банківські установи документи для перерахування коштів згідно з визначеними податками й платежами, а також для розрахунків з іншими кредиторами відповідно до договірних зобов'язань.
4. Бере участь у проведенні інвентаризації активів і зобов'язань, оформленні матеріалів, пов'язаних з нестачею та відшкодуванням втрат під нестачі, крадіжки й псування активів підприємства, у перевірках стану бухгалтерського обліку підприємства.
5. Готує дані для включення їх до фінансової звітності, здійснює складання окремих її форм, а також форм іншої періодичної звітності, яка грунтується на даних бухгалтерського обліку.
6. Забезпечує підготовку оброблених документів, реєстрів і звітності для зберігання їх протягом установленого терміну.
7. Постійно знайомиться та вивчає нові нормативно-методичні ти довідкові документи з питань організації та ведення бухгалтерського обліку та вносить пропозиції щодо їх впровадження на підприємстві.
8. Виконує окремі службові доручення свого безпосереднього керівника.

**3. Посадові повноваження:**

Бухгалтер має право:

1. Ознайомлюватися з проектами рішень керівництва підприємства, що стосуються його діяльності.
2. Вносити на розгляд директора пропозиції по вдосконалення роботи, пов'язаної з обов'язками, що передбачені цією інструкцією.
3. В межах своєї компетенції повідомляти безпосередньому керівнику про всі виявлені недоліки в діяльності підприємства та вносити пропозиції щодо їх усунення.
4. Вимагати та отримувати у керівника та персоналу інформацію та документи, необхідні для виконання його посадових обов'язків.
5. Вимагати від керівництва підприємства сприяння у виконанні своїх посадових обов'язків

**4. Посадова відповідальність:**

1. За неналежне виконання або невиконання своїх посадових обов'язків, що передбачені цією посадовою інструкцією, — в межах, визначених чинним законодавством України про працю.
2. За правопорушення, скоєні в процесі здійснення своєї діяльності, — в межах, визначених чинним адміністративним, кримінальним та цивільним законодавством України.
3. За завдання матеріальної шкоди — в межах, визначених чинним цивільним законодавством та законодавством про працю України
   * + 1. **Посадова інструкція завідувача складом**

**1. Загальні положення:**

1. Завідуючий складом торгового підприємства відноситься до категорії керівників.
2. Призначення на посаду завідуючого складом торгового підприємства та звільнення з неї здійснюється наказом директора підприємства.
3. Завідуючий складом торгового підприємства повинен знати:

- Нормативні та методичні матеріали з питань організації складського господарства.

- Стандарти і технічні умови на зберігання товарів.

- Види, розміри, марки, сортність та інші якісні характеристики товарів і норми їх витрати.

- Організацію вантажно-розвантажувальних робіт.

- Правила і порядок зберігання і складування товарів, положення та інструкції щодо їх обліку.

- Умови договорів на перевезення і зберігання вантажів, на оренду складських приміщень і устаткування.

- Порядок розрахунків за надані послуги та виконані роботи.

- Правила експлуатації обчислювальної техніки, комунікацій і зв'язку.

- Основи економіки, організації виробництва, праці та управління.

- Основи трудового законодавства.

- Правила внутрішнього трудового розпорядку.

- Правила і норми охорони праці, техніки безпеки, виробничої санітарії і протипожежного захисту.

1. Завідуючий складом торгового підприємства підпорядковується безпосередньо керівнику.
2. На час відсутності завідуючого складом його обов'язки виконує особа, призначена у встановленому порядку, яка набуває відповідних прав і несе відповідальність за належне виконання покладених на неї обов'язків.

**2. Посадові обов'язки:**

1. Керує роботою складу з приймання та зберігання товарів, по їх розміщенню з урахуванням найбільш раціонального використання складських площ, полегшення і прискорення пошуку необхідних товарів.
2. Забезпечує збереження складованих товарів.
3. Забезпечує дотримання режимів зберігання.
4. Організовує роботи з розпакування товарів і підготовці до продажу.
5. Готує місця для прийняття вантажів, що надійшли.
6. Організовує проведення вантажно-розвантажувальних робіт на складі з додержанням правил охорони праці, техніки безпеки, виробничої санітарії і протипожежного захисту.
7. Забезпечує збір, зберігання і своєчасне повернення постачальникам багатооборотної тари.
8. Веде облік складських операцій.
9. Забезпечує виконання правил оформлення і здачі прибутково-видаткових документів.
10. Складає встановлену звітність.
11. Бере участь у проведенні інвентаризацій товарно-матеріальних цінностей.

**3. Посадові повноваження:**

Завідуючий складом торгового підприємства має право:

1. Знайомитися з проектами рішень керівництва підприємства, що стосуються діяльності складу.
2. Вносити на розгляд керівництва пропозиції щодо вдосконалення роботи, пов'язаної з передбаченими даною інструкцією обов'язками.
3. У межах своєї компетенції повідомляти директору про всі виявлені в процесі виконання своїх посадових обов'язків недоліки в діяльності складу і вносити пропозиції щодо їх усунення.
4. Підписувати і візувати документи в межах своєї компетенції.
5. Вимагати від керівництва підприємства сприяння у виконанні своїх посадових обов'язків і прав.

**4. Посадова відповідальність:**

1. За неналежне виконання або невиконання своїх посадових обов'язків, передбачених даною посадовою інструкцією - в межах, визначених чинним трудовим законодавством України.
2. За правопорушення, скоєні в процесі здійснення своєї діяльності - в межах, визначених чинним адміністративним, кримінальним та цивільним законодавством України.
3. За завдання матеріальної шкоди - в межах, визначених чинним трудовим і цивільним законодавством України.
   * + 1. **Посадова інструкція охоронця**

**1. Загальні положення:**

1. Охоронець призначається на посаду і звільняється з посади в установленому чинним трудовим законодавством порядку наказом директора підприємства.
2. Охоронець підпорядковується безпосередньо директору.
3. У період тимчасової відсутності Охоронця, його обов'язки покладаються на тимчасово залученого на заміщення працівника.
4. У своїй роботі охоронець керується:   
   - діючими законодавчими актами України,   
   - Статутом підприємства,   
   - Правилами внутрішнього розпорядку,   
   - наказами (розпорядженнями) Генерального директора,

**2. Посадові обов'язки:**

1. Охороняє об'єкт, майно, матеріальні цінності, що знаходяться в межах будівлі.
2. Здійснює візуальний контроль за приміщеннями.
3. Разом зі змінним охоронцем перевіряє цілісність об'єкта, що охороняється, наявність замків та інших замикаючих пристосувань, неушкодженість матеріальних цінностей.
4. У разі виявлення факту псування або пошкодження обладнання, що не дозволяє прийняти об'єкт під охорону або виконувати інші функції з охорони майна, повідомляє про це директора.
5. У разі виявлення будь-яких ушкоджень в приміщеннях об'єкту, що охороняється, місць зберігання майна і матеріальних цінностей невідкладно повідомляє про це безпосередньо директора.
6. У разі відвертого шахрайства, прямого нападу на об'єкт охорони з метою розкрадання, пограбування майна та матеріальних цінностей, безпосередньої загрози життю і здоров'ю охоронця об'єкта, інших працівників та осіб, що знаходяться на території охоронюваного об'єкта, очевидних протиправних дій проти персоналу охорони під час виконання покладених на нього завдань та обов'язків, невиконання законних вимог персоналу охорони повідомляє про порушника органи правопорядку, застосовує проти порушника заходи необхідної оборони згідно з чинним законодавством.

**3. Посадові повноваження:**

Охоронець офісу має право:

1. Вносити на розгляд безпосереднього керівника компетентні та обґрунтовані пропозиції щодо поліпшення умов праці, інші раціональні пропозиції.
2. Вимагати забезпечення нормальними умовами праці (приміщенням, робочим місцем, засобами праці).
3. Користування затвердженими Генеральним директором Інструкціями, наказами, розпорядженнями, Правилами та ін. Документами, що регламентують роботу охоронця офісу.
4. Запитувати інформацію та документи, необхідні для виконання своїх посадових обов'язків.
5. Отримувати від керівництва або вповноважених осіб інформацію, матеріально-технічні та інші засоби, необхідні для здійснення своїх функціональних обов'язків.

**4. Посадова відповідальність:**

Охоронець офісу несе відповідальність:

1. За неякісне та несвоєчасне виконання завдань і обов'язків, передбачених цією Інструкцією.
2. За невикористання та / або неправомірне використання наданих цією Інструкцією прав.
3. За не дотримання законодавства України, Інструкцій, наказів, розпоряджень, Правил та ін. Документів, що регулюють роботу охоронця офісу.
4. За псування або недбале ставлення до зберігання та використання, розкрадання майна фірми.
   1. **Інформаційна система.**
      1. **Програмне забезпечення**

На комп’ютерах працівників встановлено програмний продукт «1С: Управління торгівлею» призначений для автоматизації діяльності на підприємстві. Технологічна платформа «1С: Управління торгівлею» являє собою програмну оболонку над базою даних (використовується СУБД Microsoft SQL Server), яка знаходиться на корпоративному сервері. Клієнтська частина платформи функціонує в середовищі Microsoft Windows. Серверна частина платформи в клієнт-серверному варіанті роботи функціонує на ОС Linux.

Системний адміністратор створює та видає працівникам облікові записи для доступу до системи «1С: Управління торгівлею» для виконання своїх посадових обов’язків. Всі дії користувачів в інформаційній системі, їх час та місце записуються в журнал реєстрації подій, який зберігається на корпоративному сервері, доступ до якого має лише системний адміністратор.

* + 1. **Технологічний процес**
       1. **Постачання товарів**

1. Секретар призначає зустріч з постачальником товару.  
   Директор магазину підписує договір з уповноваженим представником постачальника.
2. Одна копія договору залишається в постачальника, інша – зберігається в сейфі в кабінеті директора.
3. В обумовлений термін бухгалтер інтернет-аукціону здійснює грошовий переказ на рахунок постачальника.
4. Постачальник доставляє товар на склад магазину.
5. Завідувач складом приймає товар, про що розписується у накладній, копія якої зберігається в паперовому архіві на складі.
6. Далі завідувач складом проводить огляд товару нан наявність зовнішніх пошкоджень та заносить інформацію про товар (Назва, категорія, модель, марка, технічні характеристики) в базу даних наявних товарів, яка знаходиться на корпоративному сервері.
7. Менеджер з продажу, за погодженням з директором магазину та бухгалтером встановлює ціни на отримані товари та заносить їх в базу даних товарів.
   * + 1. **Розміщення веб-сайту**

Директор орендує сервер в компанії “DATA GROUP” для розміщення програмного забезпечення веб-сайту. Договір зберігається в сейфі директора.

Адміністратор веб-сервера через мережу Internet розміщує на сервері програмне забезпечення веб-сайту та наступну інформацію:

* найменування інернет-магазину, його місцезнаходження та порядок прийняття претензій;
* основні характеристики продукції;
* ціну, включаючи плату за доставку, та умови оплати;
* гарантійні зобов'язання та інші послуги, пов'язані з утриманням чи ремонтом продукції;
* інші умови поставки або виконання договору;
* період прийняття пропозицій;
* порядок розірвання договору.
  + - 1. **Процес покупки**

1. Клієнт заходить на веб-сайт, вибирає товар та заповнює анкету, в якій вказує свої персональні дані (ПІБ, телефон, e-mail, адреса для доставки) та здійснює оплату через систему електронних платежів. Ця інформація передається мережею Internet на локальний сервер компанії.
2. Приймальник замовлень по локальній мережі отримує доступ до інформації про замовлення, зв’язується з замовником (телефон, e-mail) для підтвердження замовлення або уточнення інформації та додає його у чергу на відправку.
   * + 1. **Доставка**

Доставку здійснює компанія «Нова Пошта». На комп’ютері оператора відправки (ПК 10) налаштовано доступ до особистого кабінету – це персональна сторінка на корпоративному сайті компанії «Нова Пошта», де Інтернет-аукціон може керувати своїми відправленнями.

Можливості кабінету дозволяють:

* Оформляти експрес-накладні (ЕН) і формувати реєстри прийому-передачі відправлень.
* Роздруковувати ЕН, маркування та реєстри відправлень.
* Контролювати вартість доставки відправлень.
* Переглядати статус відправлень.
* Знаходити ЕН за номером.
* Отримати доступ до взаємної інтеграції баз даних компанії "Нова Пошта" та Клієнта.

1. Кур’єр періодично приїжджає на склад та забирає замовлення .
2. Оператор відправки оформлює ЕН накладну, один екземпляр відправляється з замовленням, інший зберігається в архіві на складі.
3. Кур’єр розписується про отримання товару в накладній та забирає товар.
4. Інформація про час та місце доставки автоматично передається на сервер магазину.
5. Приймальник замовлень інформує замовника про час доставки товару та надсилає номер накладної для відстеження за допомогою SMS-повідомлення.
6. Покупець отримує замовлення.

В загальному процес роботи інтернет магазину можна описаний на рис. 1.6:



*рис.1.6 Схема роботи інтернет магазину*

* + 1. **Резервне копіювання даних**
       1. **Дані, які підлягають резервному копіюванню**

Резервному копіюванню підлягає вся інформація, що зберігається на корпоративному сервері (Сервер 1), а саме:

* Операційна система сервера з усіма налаштуваннями.
* Програмний комплекс 1С: Управління торгівлею.
* Інформація про наявні на складі товари.
* Електронні відомості про замовлення (П.І.Б., контактний телефон,e-mail, адреса проживання, перелік замовлених товарів ).
  + - 1. **Режим створення резервних копій**

Системний адміністратор здійснює налаштування автоматичного створення резервних копій за допомогою програми «R-Drive Image». Ця програма дозволяє здійснювати резервне копіювання у 3 режимах:

|  |  |
| --- | --- |
| Повний образ | Файл містить повний образ всього диска.  **Переваги:** ​​Для відновлення всього диска необхідний тільки цей єдиний файл.  **Недоліки:** Великий розмір. |
| Образ в диференціальному режимі | Файл містить зміни, зроблені на диску від моменту створення повного образу до поточного моменту.  **Переваги:** ​​Розмір менше розміру повного образу.  **Недоліки:** Розмір як правило більше розміру інкрементального образу. Для відновлення диска необхідний один образ в диференціальному режимі і повний образ. |
| Образ в інкрементальному режимі | Файл містить зміни, зроблені на диску від моменту створення останнього образу (повного, диференціального або інкрементального) до поточного моменту.  **Переваги:** ​​Менший розмір порівняно з диференціальним або повним образом.  **Недоліки:** Для відновлення даних можуть знадобитися інші інкрементальні / диференціальні образи крім повного образу. Якщо який-небудь з інкрементальних образів пошкоджений, то не вдасться також відновити і дані з пізніших інкрементальних копій. |

* + - 1. **План резервного копіювання**

1. Створювати повний образ першу суботу кожного місяця о 14:00.
2. Створювати образ в диференціальному режимі щосуботи о 17:00.
3. Створювати образ в інкрементальному режимі кожен робочий день о 21:00.

Резервні копії зберігаються протягом трьох місяців.

Відповідно до даного плану стан даних зберігається один раз на день, при цьому можливо здійснити відновлення даних на стан будь-якого дня протягом останніх трьох місяців. У цьому випадку максимум що може бути втрачено це зміни зроблені протягом одного дня.

Резервні копії зберігаються на орендованому сервері компанії “DATA GROUP”.  
Це вбереже сервер з резервними копіями і даними від пожежі або будь-яких інших форс-мажорних обставин, які можуть трапитися в офісі.

* + 1. **План доходів і витрат підприємства**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Показник | | Сума, грн | | |
| Місяць | Рік | По-середньому в день |
| Загальна сума від продажу товарів | | 1 310 885 | 15 730 620 | 43097 |
| Виробничі витрати | Закупівля товарів | 900 300 | 10 803 600 | 29598 |
| Оплата праці | 73 150 | 877 800 | 2404 |
| Канцелярські товари | 1 000 | 12 000 | 32 |
| Амортизація комп’ютерної техніки | 625 | 7 500 | 20 |
| Електроенергія | 780 | 9 360 | 25 |
| Витрати на рекламу | 3500 | 42 000 | 115,0685 |
| Інтернет | 200 | 2 400 | 6 |
| Орнеда сервера | 780 | 9 360 | 25 |
| Інші витрати | 850 | 10 200 | 27 |
| Всього | 981 185 | 11 774 220 | 32258,14 |
| Валовий прибуток | | 329 700 | 3 956 400 | 10839,45 |
| Податок на прибуток (5%) | | 16485 | 197820 | 541,9726 |
| Єдиний соціальний внесок | | 398 | 4776 | 13 |
| Чистий прибуток | | 312 817 | 3 753 804 | 10 284 |

**Оплата праці**

|  |  |  |  |
| --- | --- | --- | --- |
| **Посада** | Зарплата, грн | | |
| Місяць | Рік | По-середньому в день |
| директор | 23 000 | 276000 | 756 |
| секретар | 4 500 | 54000 | 147 |
| бухгалтер | 5 500 | 66000 | 180 |
| системний адміністратор | 10 000 | 120000 | 328 |
| адміністратор веб-сервера | 10 000 | 120000 | 328 |
| менеджер з продажу | 3 500 | 42000 | 115 |
| приймальник замовлень | 2 500 | 30000 | 82 |
| консультант | 2 500 | 30000 | 82 |
| оператор відправки | 3 500 | 42000 | 115 |
| завідувач складу | 3 500 | 42000 | 115 |
| вантажник | 2 500 | 30000 | 82 |
| прибиральник | 2 150 | 25800 | 70 |
| **Вьсого** | 73 150 | 877800 | 2404 |

* 1. **Реєстр інформаційних активів.**

|  |  |  |  |
| --- | --- | --- | --- |
| Опис активу | | | |
| Актив | Власник | Місце розташування | Категорія активу |
| Електронний каталог товарів (містить інформацію про технічні характеристики продукції, її  ціну, включаючи плату за доставку, та умови оплати) | Адміністратор веб-сервера | Дата центр  Компанії «Data group» | БД |
| Програмне забезпечення інтернет магазину | Адміністратор веб-сервера | Дата центр  Компанії «Data group» | ПЗ |
| Інформація в електронному вигляді про наявні на складі товари (Назва, категорія, модель, марка, технічні характеристики, ціна для продажу) | Завідувач складом | Сервер 1 | БД |
| Електронні відомості про замовлення (П.І.Б., контактний телефон,e-mail, адреса проживання, перелік замовлених товарів ) | Консультант | Сервер 1 | БД |
| Сервер 1 | Системний адміністратор | Серверна | КТ |
| Локальна мережа передавання даних (комутатор, лінії передавання даних) | Системний адміністратор | Офіс | МО |

БД- база даних, КТ- комп’ютерна техніка, ВІ – віртуальна інформація, МО - мережне обладнання, ПД – паперові документи.

Розділ 2. Методика оцінювання ризику

Щоби оцінити ризик, зручно використовувати простий і зрозумілий метод розрахунку. Саме простота дає змогу достовірно оцінити ризики і за необхідності корегувати їх значення. Найпростішою є формула:

*Ризик=Ймовірність\*Збиток*

**2.1. Методика оцінки ймовірності реалізації загрози.**

Оцінка ймовірності реалізації загрози здійснюється за непрямим показниками, а саме:

* можливість виникнення джерела ,що визначає міру доступності до можливості використати фактор (уразливість) (для антропогенних джерел), віддаленість від фактора (уразливості) (для техногенних джерел) або особливості обстановки (для випадкових джерел);
* готовність джерела , що визначає міру кваліфікації та привабливість здійснення діяння з боку джерела загрози (для антропогенних джерел) або наявність необхідних умов (для техногенних та стихійних джерел);
* фатальність , що визначає міру непереборності наслідків реалізації загрози.

Кожний показник оцінюється експертно-аналітичним методом за п'ятибальною системою. Коефіцієнт  для окремого джерела можна визначити як відношення добутку наведених вище показників до максимального значення 125:



*Табл. 2.1*

**Характеристика міри доступності об'єкта**

|  |  |  |
| --- | --- | --- |
| **Міра доступності** | **X** | **Характеристика** |
| Висока ступінь доступності | 5 | Антропогенне джерело загроз має повний доступ до персональних комп'ютерів працівників, до інтерфейсу управління веб-сторінки магазину, та до мережевого та серверного обладнання (роутер, комутатор, сервер, локальна обчислювальна мережа) за рахунок виконання своїх посадових обов’язків. (Джерела: системний адміністратор, адміністратор веб-сервера) |
| Ступінь доступності вище середньої | 4 | Антропогенне джерело загроз має можливість опосередкованого, не визначеного функціональними обов’язками доступу до персональних комп'ютерів працівників та до мережевого та серверного обладнання за рахунок несанкціонованого доступу до привілейованих робочих місць, та наявності каналу витоку інформації через локальну мережу та мережу інтернет (Джерела: працівники, хакери) |
| Середня ступніть доступності | 3 | Антропогенне джерело загроз має обмежену можливість доступу до інформації, що зберігається на сервері та окремих персональних комп’ютерах працівників через використання політики безпеки, яка обмежує випадковий доступ до даних. (Джерела: менеджер з продажу, бухгалтер, системний адміністратор, хакери, працівники компанії «Київстар») |
| Низька ступінь доступності | 2 | Антропогенне джерело має дуже обмежену можливість доступу до персональних комп'ютерів працівників та до мережевого та серверного обладнання. (Джерела: хакери). |
| Відсутність доступності | 1 | Антропогенне джерело загроз не має доступу до технічних пристроїв компанії |

*Табл. 2.2*

**Характеристика міри віддаленості об'єкта**

|  |  |  |
| --- | --- | --- |
| **Міра віддаленості** | **X** | **Характеристика** |
| Співпадаючі об'єкти | 5 | Персональні комп'ютери працівників, які містять інформацією, що підлягає захисту, мережеве та серверне обладнання самі містять джерела техногенних загроз і їхній територіальний поділ неможливий. |
| Близько розташовані об'єкти | 4 | Персональні комп'ютери працівників, які містять інформацією, що підлягає захисту, мережеве та серверне обладнання знаходяться в безпосередній близькості від техногенних джерел загроз, прояв яких може суттєво вплинути на ці об'єкти захисту. |
| Середньовіддалені об'єкти | 3 | Персональні комп'ютери працівників, які містять інформацією, що підлягає захисту, мережеве та серверне обладнання знаходяться на віддаленні від джерел техногенних загроз при якому їх прояв спричиняє лише несуттєвий вплив. |
| Віддалено розташовані об'єкти | 2 | Персональні комп'ютери працівників, які містять інформацією, що підлягає захисту, мережеве та серверне обладнання знаходяться на віддаленні від джерел техногенних загроз яке виключає його прямий вплив. |
| Значно віддалені об'єкти | 1 | Персональні комп'ютери працівників, які містять інформацією, що підлягає захисту, мережеве та серверне обладнання розташовуються на значній відстані від джерела техногенних загроз, що повністю виключає будь-які впливи, в тому числі вторинні. |

*Табл. 2.3*

**Особливості оточення об'єкта**

|  |  |  |
| --- | --- | --- |
| **Особливості оточення** | **X** | **Характеристика** |
| Дуже небезпечні умови | 5 | Персональні комп'ютери працівників, які містять інформацією, що підлягає захисту, мережеве та серверне обладнання та паперові документи розташовані в зоні дії природних катаклізмів. |
| Небезпечні умови | 4 | Персональні комп'ютери працівників, які містять інформацією, що підлягає захисту, мережеве та серверне обладнання та паперові документи розташовуються в зоні, де прогнозується поява природних катаклізмів |
| Помірно небезпечні умови | 3 | Персональні комп'ютери працівників, які містять інформацією, що підлягає захисту, мережеве та серверне обладнання розміщені в зоні, в якій за тривалими спостереженнями відсутні прояви природних катаклізмів, але існує можливість появи стихійних джерел загроз в самому технічному обладнанні (персональні комп'ютери, принтери, сервер, роутер) |
| Слабо небезпечні умови | 2 | Персональні комп'ютери працівників, які містять інформацією, що підлягає захисту, мережеве та серверне обладнання розміщені в зоні, в якій не спостерігаються прояви природних катаклізмів, але існує можливість прояви стихійних джерел загрозах в певному технічному обладнанні (персональні комп'ютери, принтери, сервер, роутер) |
| Безпечні умови | 1 | Персональні комп'ютери працівників, які містять інформацією, що підлягає захисту, мережеве та серверне обладнання розміщені поза межами дії природних катаклізмів і не існує передумов прояви стихійних джерел загроз |

*Табл. 2.4*

**Характеристика можливості взаємодії з інформаційними активами (мережі зв'язку)**

|  |  |  |
| --- | --- | --- |
| **Можливості** | **X** | **Характеристика** |
| Четвертий рівень | 5 | Повний обсяг можливостей суб'єктів, займаються розробкою програмного забезпечення, проектуванням і ремонтом персональних комп'ютерів та принтерів, сегментів локальної мережі з можливістю включення до її складу власних технічних пристроїв, (рівень розробника та комп’ютерного інженера) |
| Третій рівень | 4 | Можливість керування інформаційними процесами в мережі, впливу на конфігурацію та склад наявного в мережі програмного забезпечення (рівень системного адміністратора) |
| Другий рівень | 3 | Створення й запуск в мережі передавання даних власних утиліт і програм з новими функціями обробки інформації (рівень програміста, кваліфікованого користувача ) |
| Перший рівень | 2 | Запуск лише обмеженого набору програм для обробки інформації (рівень некваліфікованих користувача). |
| Нульовий рівень | 1 | Відсутність можливості будь-якого використання встановлених програм. |

*Табл. 2.5*

**Характеристика привабливості здійснення діяння з боку джерела загроз**

|  |  |  |
| --- | --- | --- |
| **Привабливість** | **X** | **Характеристика** |
| Особливо привабливий рівень | 5 | Інформаційні ресурси, які підлягають захисту, містять інформацію втрата якої зумовить непоправні збитки та призведе до краху організації. |
| Привабливий рівень | 4 | Інформаційні ресурси, які підлягають захисту, містять інформацію яка може бути використана на користь джерела загрози або третіх осіб |
| Помірно привабливий рівень | 3 | Інформаційні ресурси, які містять інформацію, розголошення якої може нанести шкоду окремим особам. |
| Привабливий рівень | 2 | Інформаційні ресурси, які містять інформацію, системне накопичення та узагальнення якої в результаті може завдати збитку. |
| Непривабливий рівень | 1 | Інформаційні ресурси, які містять інформацію, яка не представляє інтересу для джерела загрози. |

*Табл. 2.6*

**Характеристики умови готовності джерела**

|  |  |  |
| --- | --- | --- |
| **Готовність** | **X** | **Характеристика** |
| Загроза реалізована | 5 | Умови сприятливі або можуть бути сприятливі для реалізації загрози. |
| Загроза помірно реалізована | 4 | Сприятливі умови для реалізації загрози, але неможливість її активізації . |
| Загроза слабо реалізована | 3 | Існують об’єктивні причини на самому об’єкті або його оточенні, що перешкоджають реалізації загрози. |
| Загроза майже не реалізована | 2 | Майже не існує передумов для реалізації передбачуваної події. |
| Загроза не реалізована | 1 | Відсутні передумови для реалізації передбачуваної події. |

*Табл. 2.7*

**Міра непереборності наслідків загрози**

|  |  |  |
| --- | --- | --- |
| **Готовність** | **X** | **Характеристика** |
| Непереборні наслідки | 5 | Результат прояву загрози може призвести до повного знищення персональних комп'ютерів працівників та паперових документів, що призведе до непоправних втрат та неможливість доступу до інформації, що підлягає захисту. |
| Практично непереборні наслідки | 4 | Результат прояву загрози може призвести до повного знищення персональних комп'ютерів працівників та паперових документів, що призведе до значних втрат на відновлення і як наслідок до суттєвого обмеження часу доступу до інформації. |
| Частково непереборні наслідки | 3 | Результат прояву загрози приводить до часткового пошкодження інформаційних ресурсів або суттєвого довготривалого обмеження доступу до об'єктів захисту і потребує значних затрат (матеріальних, час) на відновлення цих об'єктів |
| Переборні наслідки | 2 | Результат прояву загрози приводить до часткового пошкодження інформаційних ресурсів і не потребує значних затрат (матеріальних, час) на відновлення цих об'єктів. |
| Відсутність наслідків | 1 | Результат прояву загрози не впливають на діяльність об'єктів захисту |

**2.2. Методика оцінки збитку.**

Розмір збитку відображає в грошовому еквіваленті втрати, які понесе організація внаслідок реалізації загрози. Цим збитком може бути вартість конфіденційної інформації, фінансові витрати на відновлення роботи інформаційної системи, втрата прибутку через порушення технологічного процесу.

Наприклад, якщо у результаті нападу на веб-сервер інтернет-аукціону він перестав обслуговувати клієнтів, безпосереднім збитком може бути:

1. Втрата чи пошкодження інформації.
2. Витрати на відновлення нормального функціонування сервера (витрати робочого часу, придбання нового ПЗ)
3. Втрата доходу внаслідок неможливості обслуговування клієнтів протягом часу, необхідного для відновлення роботи ураженого веб-серверу (падіння продажів, втрата репутації та довіри клієнтів).

Для оцінювання значення можливого збитку може бути використана п’ятибальна шкала якісного аналізу. Для того, щоб оцінка збитку містила економічний зміст, якісну шкалу можна пов’язати зі значенням безпосередніх фінансових втрат організації.

*Табл. 2.2*

**Шкала оцінювання збитку**

|  |  |  |
| --- | --- | --- |
| **Значення збитку** | **Збиток комерційним інтересам організації** | **Фінансові втрати, грн** |
| 1 | Незадоволення з боку клієнтів, незначна затримка в роботі ІС. | Менше 2 000 |
| 2 | Зниження рівня довіри до компанії, часткове пошкодження інформаційних ресурсів. | Від 2 000 до 5 000 |
| 3 | Втрата декількох потенційних клієнтів, короткочасна зупинка роботи ІС. | Від 5 000 до 15 000 |
| 4 | Розповсюдження негативних відгуків про організацію, довготривала зупинка роботи ІС. | Від 15 000 до 200 000 |
| 5 | Втрата довіри з боку значної частини клієнтів, втрата основної частки ринку | Понад 200 000 |

Розділ 3. Оцінювання ризиків.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Електронний каталог товарів (містить інформацію про технічні характеристики продукції, її  ціну, включаючи плату за доставку, та умови оплати) | | | | | | | | | | | |
| Загроза | Власник | Місце розташування | Категорія активу | Джерело | Механізм реалізації загрози | К1 | К2 | К3 | Кзаг | Збиток | Ризик (%) |
| Доступності | Адміністратор веб-сервера | Дата центр  Компанії «Data group» | БД | Хакер | DDoS-напад на сервер, що містить інформацію через *відсутність фільтрації трафіку.* | 5 | 4 | 2 | 0,32 | 1 | 13 |
| Знищення інформації за рахунок XSS-нападу на ПЗ веб-сайту через *відсутність екранування вхідних даних* | 2 | 4 | 4 | 0,25 | 4 | 39 |
| Системний адміністратор | Знищення інформації за рахунок використання робочого місця адміністратора веб-сервера через *відсутність виходу з системи, коли залишається робоче місце* | 4 | 4 | 4 | 0,51 | 4 | 80 |
| Цілісності | Системний адміністратор | Модифікація інформації про ціну товару за рахунок використання робочого місця адміністратора веб-сервера через *відсутність виходу з системи, коли залишається робоче місце* | 4 | 3 | 2 | 0,19 | 2 | 15 |
| Хакер | Модифікація інформації про ціну товару за рахунок XSS-нападу на ПЗ веб-сайту через *відсутність екранування вхідних даних* | 5 | 4 | 4 | 0,64 | 4 | 100 |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Програмне забезпечення інтернет магазину | | | | | | | | | | | |
| Загроза | Власник | Місце розташування | Категорія активу | Джерело | Механізм реалізації загрози | К1 | К2 | К3 | Кзаг | Збиток | Ризик (%) |
| Доступність | Адміністратор веб-сервера | Дата центр Компанії «Data group» | ПЗ | Хакер | DDoS-напад на сервер, що містить ПЗ через відсутність фільтрації трафіку. | 5 | 4 | 2 | 0,32 | 1 | 13 |
| Системний адміністратор | Видалення ПЗ за рахунок використання робочого місця адміністратора веб-сервера через відсутність виходу з системи, коли залишається робоче місце | 4 | 4 | 4 | 0,51 | 4 | 80 |
| Цілісність | Хакер | Модифікація ПЗ за рахунок XSS-нападу на ПЗ веб-сайту через відсутність екранування вхідних даних | 5 | 4 | 4 | 0,64 | 4 | 100 |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Електронні відомості про замовлення (П.І.Б., контактний телефон,e-mail, адреса проживання, перелік замовлених товарів ) | | | | | | | | | | | |
| Загроза | Власник | Місце розташування | Категорія активу | Джерело | Механізм реалізації загрози | К1 | К2 | К3 | Кзаг | Збиток | Ризик (%) |
| Доступність | Консультант | Сервер 1 | БД | Основний персонал компанії | Знищення інформації за рахунок привласнення ідентифікатора системного адміністратора, який необхідний для роботи з системою 1С через *ненадійність ідентифікатора системного адміністратора (мала довжина, використання стандартних комбінацій)* | 3 | 3 | 2 | 0,14 | 3 | 16 |
| Блокування доступу інших користувачів до інформації за рахунок видалення або зміни їх облікових записів для доступу до системи 1с шляхом привласнення ідентифікатора системного адміністратора, який необхідний для роботи з обліковими записами користувачів в системі 1С через  *ненадійність ідентифікатора системного адміністратора (мала довжина, використання стандартних комбінацій)* | 3 | 2 | 2 | 0,09 | 1 | 4 |
| аміністартор веб-сервера | Знищення інформації за рахунок використання робочого місця системного адміністратора через *відсутність виходу з системи, коли залишається робоче місце* | 4 | 3 | 2 | 0,19 | 3 | 22 |
| Блокування доступу інших користувачів до інформації за рахунок видалення або зміни їх облікових записів для доступу до ситеми 1С шляхом використання робочого місця системного адміністратора через *відсутність виходу з системи, коли залишається робоче місце.* | 4 | 3 | 2 | 0,19 | 1 | 7 |
| Хакер | Знищення інформації за рахунок проникнення в мережу через *наявність незахищених облікових записів для адміністрування маршрутизатора* (backdoor-уразливостей) | 2 | 4 | 2 | 0,12 | 3 | 14 |
| Блокування доступу інших користувачів до інформації за рахунок видалення або зміни їх облікових записів для доступу до ситеми 1С шляхом проникнення в мережу через *наявність незахищених облікових записів для адміністрування маршрутизатора* (backdoor-уразливостей) | 2 | 3 | 2 | 0,09 | 1 | 4 |
| Лінія електроживлення | Знищення інформації за рахунок виходу з ладу сервера внаслідок перепаду напруги через *відсутність стабілізатора напруги* | 4 | 3 | 4 | 0,38 | 4 | 59 |
| Блокування доступу до інформації, за рахунок відсутності електроживлення сервера через *відсутність джерела безперебійного живлення* | 4 | 2 | 2 | 0,13 | 1 | 5 |
| Пожежа | Знищення інформації через фізичне знищення сервера внаслідок пожежі, яка виникла через  *відсутність пожежної сигналізації.* | 3 | 2 | 4 | 0,19 | 4 | 30 |
| Цілісніть | Основний персонал компанії | Модифікація інформації за рахунок привласнення ідентифікатора менеджера з продажу, який необхідний для роботи з системою 1С через *ненадійність ідентифікатора (мала довжина, використання стандартних комбінацій)* | 3 | 4 | 3 | 0,29 | 2 | 23 |
| Хакер | Віддалена модифікація інформації за рахунок проникнення в мережу через *наявність незахищених облікових записів для адміністрування маршрутизатора* (backdoor-уразливостей) | 2 | 4 | 3 | 0,19 | 2 | 15 |
| Конфіденційність | Основний персонал компанії | Копіювання інформації на сторонні носії через *відсутність обмеження на використання стороніх носіїв інформації* | 4 | 3 | 1 | 0,09 | 5 | 18 |
| Працівники компанії «Київстар» | Перехоплення інформації яка надходить з веб-сайту через мережу інтернет за рахунок *незахищеного з’єднання.* | 2 | 2 | 1 | 0,03 | 5 | 6 |
| Хакер | Викрадення інформації за рахунок проникнення в мережу через *наявність незахищених облікових записів для адміністрування маршрутизатора* (backdoor-уразливостей)*.* | 2 | 4 | 1 | 0,06 | 5 | 12 |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Інформація в електронному вигляді про наявні на складі товари (Назва, категорія, модель, марка, технічні характеристики) | | | | | | | | | | | |
| Загроза | Власник | Місце розташування | Категорія активу | Джерело | Механізм реалізації загрози | К1 | К2 | К3 | Кзаг | Збиток | Ризик (%) |
| Доступність | Оператор поштового відділу | Сервер 1 | БД | Хакер | Зараження корпоративного сервера вірусом-шифрувальником через *відсутність брандмауера для захисту локальної мережі від шкідливого трафіку.* | 3 | 3 | 2 | 0,14 | 2 | 11 |
| Цілісність | Персонал підприємства | Внесення змін в інформацію про товари, які суперечать посадовим інструкціям через *відсутність політики розмежування доступу.* | 4 | 2 | 2 | 0,13 | 2 | 10 |
| Хакер | Модифікація інформації про товари через *відсутність брандмауера для захисту локальної мережі від шкідливого трафіку.* | 3 | 3 | 2 | 0,14 | 2 | 11 |
| Конфіденційність | Хакер | Копіювання інформації з сервера через  *відсутність брандмауера для захисту локальної мережі від шкідливого трафіку.* | 3 | 4 | 3 | 0,29 | 1 | 11 |
| Персонал підприємства | Копіювання інформації на сторонні носії зберігання данних через  *відсутність обмеження на використання стороніх носіїв інформації.* | 4 | 3 | 3 | 0,29 | 1 | 11 |
| Системний адміністатор | Надання доступу до інформації стороннім особам через зміну *конфігурації мережного обладнання.* | 5 | 4 | 3 | 0,48 | 1 | 19 |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Сервер 1 | | | | | | | | | | | |
| Загроза | Власник | Місце розташування | Категорія активу | Джерело | Механізм реалізації загрози | К1 | К2 | К3 | Кзаг | Збиток | Ризик (%) |
| Доступність | Системний адміністратор | Серверна | КТ | Хакер | Зараження корпоративного сервера вірусним ПЗ через *відсутність антивірусного захисту,* яке спричиняє збої в роботі сервера. | 3 | 4 | 3 | 0,29 | 2 | 23 |
| Система кондціонування | Знищення інформації через перегрівання сервера за рахунок *виходу з ладу системи кондиціонування* | 3 | 3 | 4 | 0,29 | 4 | 45 |
| Лінія електроживлення | Знищення інформації за рахунок виходу з ладу сервера внаслідок перепаду напруги через *відсутність стабілізатора напруги* | 4 | 3 | 4 | 0,38 | 4 | 59 |
| Блокування доступу до інформації, за рахунок відсутності електроживлення сервера через *відсутність джерела безперебійного живлення* | 4 | 2 | 2 | 0,13 | 1 | 5 |
| Пожежа | Знищення інформації через фізичне знищення сервера внаслідок пожежі, яка виникла через  *недотримання правил пожежної безпеки та відсутність пожежної сигналізації.* | 3 | 2 | 4 | 0,19 | 4 | 30 |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Локальна мережа передавання даних | | | | | | | | | | | |
| Загроза | Власник | Місце розташування | Категорія активу | Джерело | Механізм реалізації загрози | К1 | К2 | К3 | Кзаг | Збиток (грн.) | Ризик (%) |
| Доступність | Системний адміністратор | Офіс | МО | Комутатор | Затримка в обміні інформації через переповнення таблиці MAC-адрес комутатора через *використання динамічної таблиці MAC-адрес* | 5 | 5 | 2 | 0,4 | 1 | 16 |
| Лінія електроживлення | Затримка в обміні інформації через відсутність електроживлення комутатора через *відсутність джерела безперебійного живлення* | 4 | 2 | 2 | 0,13 | 1 | 5 |
| Пожежа | Відсутність обміну інформації між вузлами мережі через фізичне знищення комутатора та ліній зв’язку внаслідок пожежі, яка виникла через  *недотримання правил пожежної безпеки та відсутність пожежної сигналізації.* | 3 | 2 | 4 | 0,19 | 3 | 22 |
| Конфіденційність | Основний персонал компанії | Перехоплення інформації , яка передається по мережі за допомогою нападу ARP-spoofing який можливий через *використання динамічної таблиці MAC-адрес та відсутність шифрування даних в мережі* | 4 | 3 | 3 | 0,29 | 3 | 34 |

висновок

У даній роботі я провів опис об’єкта, ідентифікував найбільш критичні інформаційні активи, провів оцінку імовірності реалізації загроз, уразливостей.

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

список використаної літератури

1. Ромака В.А., Корж Р.О., Гарасим Ю.Р. «Менеджмент у сфері захисту інформації» - Львів, 2013
2. УДК 004.056:061.68 Студ. А.І. Кунинець, магістрант; проф. Ю.І. Грицюк, д-р техн. наук – Львівський ДУ БЖД
3. Чашкин, Ю. Р. Математическая статистика. Анализ и обработкаданных: учеб. пособие для студентоввузов / Ю. Р. Чашкин. - Ростов н/Д. : Феникс, 2010. - 240 с.
4. Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдін. – К. : «МК-Прес», 2005. –600 с
5. Малюк, А. А. Информационнаябезопасность: концептуальные и методологическиеосновызащитыинформации: учебноепособие для вузов / А. А. Малюк. - М. : Горячаялиния-Телеком, 2004. - 208 с.
6. Степанов, Е. А. Информационнаябезопасность и защитаинформации [Текст] : учебноепособие / Е. А. Степанов, И. К. Корнеев. - М. : Инфра-М, 2001. - 304 с.