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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Храмова Миколи Олеговича*

академічної групи *125-19-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка політики безпеки інформаційно-комунікаційної системи підприємства з продажу побутової техніки*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Магро В.І.			
розділів:				
спеціальний	ст. викл. Мєшков В.І.			
економічний	к.е.н., доц. Романюк Н.М.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2023

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Храмову Миколі Олеговичу* **академічної групи** *125-19-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка політики безпеки інформаційно-комунікаційної системи підприємства з продажу побутової техніки***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № 350-с

Розділ	Зміст	Термін виконання
Розділ 1	Визначити актуальність розробки засобів захисту інформаційних ресурсів з обмеженим доступом, виконати опис виду діяльності підприємства, проаналізувати типову інформаційну систему підприємства з продажу побутової техніки	29.03.2023
Розділ 2	Розробити модель загроз та модель порушника, визначити критерії захищеності та надати рекомендацій щодо реалізації системи захисту ІКС підприємства. Розробити політику безпеки захисту від несанкціонованого доступу ІКС підприємства з продажу побутової техніки.	24.05.2023
Розділ 3	Виконати розрахунки економічних показників та довести економічну доцільність розробки.	09.06.2023

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

Дата видачі: 09.01.2023р.

Дата подання до екзаменаційної комісії: 09.06.2023р.

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

РЕФЕРАТ

Пояснювальна записка: __ с., __ рис., _ табл., __ додатка, __ джерел.

Мета роботи – розробити стратегію захисту інформаційної системи підприємства з продажу побутової техніки від можливих загроз та створення політики безпеки, що дозволить запобігти несанкціонованому доступу до даних та мінімізувати можливі наслідки випадкових чи зловісних дій.

Об’єкт дослідження – інформаційна система підприємства з продажу побутової техніки.

Предмет дослідження – заходи захисту інформаційної системи підприємства з продажу побутової техніки.

У першому розділі роботи визначена актуальність розробки засобів захисту інформаційних ресурсів з обмеженим доступом, виконано опис виду діяльності підприємства, визначені посадові обов'язки персоналу підприємства з продажу побутової техніки та розглянута типова інформаційна система підприємства з продажу побутової техніки.

У другому розділі роботи розроблена модель загроз та модель порушника, визначено критерії захищеності та надані рекомендацій щодо реалізації системи захисту ІКС підприємства. Розроблено детальну політику безпеки захисту від несанкціонованого доступу ІКС підприємства з продажу побутової техніки.

У третьому розділі роботи проведено розрахунки економічних показників та доведена економічна доцільність розробки.

Практичне значення роботи полягає у можливості застосування розробленої політики безпеки як типової для інформаційної системи підприємства з продажу побутової техніки.

ПОЛІТИКА БЕЗПЕКИ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ.

ABSTRACT

Explanatory note: ___ pp., ___ pic., ___ table, ___ app, ___ sources.

The purpose of the study is to develop a strategy for protecting the information system of a household appliances sales company from possible threats and to create a security policy that will prevent unauthorized access to data and minimize the possible consequences of accidental or sinister actions.

The object of research is the information system of an enterprise selling household appliances.

The subject of the study is the measures to protect the information system of an enterprise selling household appliances.

The first section of the paper defines the relevance of developing means of protecting information resources with limited access, describes the type of activity of the enterprise, defines the job responsibilities of the personnel of the enterprise selling household appliances and considers a typical information system of the enterprise selling household appliances.

The second section of the paper develops a threat model and an intruder model, defines security criteria and provides recommendations for implementing a system for protecting the enterprise's ICS. A detailed security policy for protection against unauthorized access to the ICS of an enterprise selling household appliances has been developed.

In the third section of the paper, economic indicators are calculated and the economic feasibility of the development is proved.

The practical significance of the work lies in the possibility of applying the developed security policy as a typical one for the information system of an enterprise selling household appliances.

SECURITY POLICY, THREAT MODEL, INTRUDER MODEL, INFORMATION SYSTEM, CYBERSECURITY, INFORMATION SECURITY MANAGEMENT.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС	–	автоматизована система;
ІКС	–	інформаційно-комунікаційна система;
ОС	–	операційна система;
НСД	–	несанкціонований доступ;
ПЗ	–	програмне забезпечення;
BI	–	Business Intelligence;
CRM	–	Customer Relationship Management;
ERP	–	Enterprise Resource Planning;
SCM	–	Supply Chain Management;
TMS	–	Transportation Management System.

ЗМІСТ

с.

ВСТУП

В сучасному світі, коли обмін інформацією є невід'ємною частиною життя, інформаційні технології стали надзвичайно важливим інструментом для бізнесу та різних галузей економіки. Інформаційні системи стали ключовим елементом бізнес-процесів, оскільки вони забезпечують швидкий та ефективний обмін даними, допомагають вирішувати проблеми та оптимізувати роботу підприємств.

Однак, зростання використання інформаційних технологій також призводить до збільшення кількості загроз для інформаційної безпеки, таких як несанкціонований доступ, віруси, соціальний інжиніринг та інші. У зв'язку з цим, забезпечення безпеки інформаційних систем стало особливо важливою задачею.

Мета роботи – розробити стратегію захисту інформаційної системи підприємства з продажу побутової техніки від можливих загроз та створення політики безпеки, що дозволить запобігти несанкціонованому доступу до даних та мінімізувати можливі наслідки випадкових чи зловісних дій.

Об’єкт дослідження – інформаційна система підприємства з продажу побутової техніки.

Предмет дослідження – заходи захисту інформаційної системи підприємства з продажу побутової техніки.

Завдання роботи:

- провести аналіз загроз, що ставлять під загрозу інформаційну систему підприємства з продажу побутової техніки.
- розробити модель загроз та модель порушника для інформаційної системи підприємства.
- визначити критерії захищеності для автоматизованої системи класу 3.
- розробити політику безпеки для інформаційної системи підприємства.
- розробити рекомендації щодо захисту від несанкціонованого доступу, вторгнень, витоку інформації.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Актуальність розробки засобів захисту інформаційних ресурсів з обмеженим доступом

Розробка засобів захисту інформаційних ресурсів з обмеженим доступом інформаційно-комунікаційної системи (ІКС) є важливою задачею для забезпечення безпеки даних та захисту від несанкціонованого доступу до них.

Основні кроки при розробці засобів захисту інформаційних ресурсів з обмеженим доступом ІКС:

1. Аналіз загроз та ризиків – оцінка потенційних загроз безпеці даних та ризиків їхньої реалізації. За результатами аналізу ризиків потрібно визначити заходи забезпечення безпеки.

2. Визначення обмеженого доступу – встановлення механізмів, що обмежують доступ до конфіденційної інформації. Це може бути досягнуто за допомогою контролю доступу, шифрування, ідентифікації користувачів, контролю цілісності даних та ін.

3. Захист від несанкціонованого доступу – встановлення заходів, що мінімізують можливість несанкціонованого доступу до даних. Це може бути досягнуто за допомогою мережевого брандмауера, антивірусного програмного забезпечення, механізмів виявлення інтрузій та ін.

4. Моніторинг системи – встановлення механізмів моніторингу стану системи та виявлення можливих загроз. Це може бути досягнуто за допомогою систем логування та аудиту.

5. Тестування та аналіз результатів – тестування засобів захисту та аналіз результатів може виявити можливі проблеми та допомогти вдосконалити систему.

Загальний підхід до розробки засобів захисту інформаційних ресурсів з обмеженим доступом ІКС полягає в поєднуванні технічних та організаційних заходів для забезпечення безпеки інформації. Це можуть бути заходи забезпечення фізичної безпеки, які забезпечують фізичний захист пристроїв і обладнання ІКС від несанкціонованого доступу.

Також можуть бути встановлені заходи забезпечення криптографічної безпеки, які забезпечують захист даних від проникнення зловмисника за допомогою різних методів шифрування.

Важливою складовою є заходи забезпечення безпеки мережі, такі як налаштування мережевих з'єднань, ідентифікація користувачів, використання мережевих брандмауерів і систем виявлення інтрузій, що забезпечують захист від зовнішніх атак на мережу.

Для забезпечення організаційної безпеки слід встановлювати процедури управління доступом, політики щодо користування даними, а також правила поведінки користувачів під час роботи з даними.

Нарешті, регулярні аудити безпеки допоможуть виявляти можливі загрози та слабкі місця в системі та вчасно приймати заходи для забезпечення безпеки.

Розробка засобів захисту інформаційних ресурсів з обмеженим доступом ІКС є дуже важливим етапом у забезпеченні безпеки даних і захисту від несанкціонованого доступу до них. Для успішної розробки таких засобів слід враховувати різноманітні загрози, встановлювати необхідні технічні та організаційні заходи, проводити тестування та моніторинг системи, а також регулярно проведення аудиту безпеки.

У розробці засобів захисту інформаційних ресурсів з обмеженим доступом ІКС також важливо враховувати законодавчі вимоги та рекомендації щодо захисту даних. Зокрема, в багатьох країнах існують закони, які регулюють захист конфіденційної інформації та вимагають встановлювати відповідні заходи для її захисту. Також існують рекомендації та стандарти щодо захисту інформації, такі як ISO/IEC 27001, які містять рекомендації щодо захисту інформації від різних загроз.

У розробці засобів захисту інформаційних ресурсів з обмеженим доступом ІКС важливо також враховувати специфіку конкретної системи та її потреби. Наприклад, система, яка зберігає медичну інформацію, може потребувати більш жорсткого захисту даних, ніж система, яка зберігає загальну інформацію. Також варто враховувати можливість відновлення даних в разі їх

втрати чи пошкодження, а також встановлювати механізми резервного копіювання та відновлення даних.

У цілому, розробка засобів захисту інформаційних ресурсів з обмеженим доступом ІКС є складним та відповідальним процесом, який вимагає спеціалізованих знань та досвіду. Однак, правильно розроблені та встановлені заходи захисту даних допоможуть зберегти конфіденційність та цілісність інформації, що зберігається в ІКС, та зменшити ризик несанкціонованого доступу до неї.

1.1.1 Аналіз загроз та ризиків

Аналіз загроз та ризиків – це перший етап розробки засобів захисту інформаційних ресурсів з обмеженим доступом ІКС. Цей етап передбачає виявлення потенційних загроз безпеці даних та оцінку ризиків їхньої реалізації. Аналіз загроз та ризиків допомагає визначити пріоритетні напрями захисту, а також встановити необхідні заходи для забезпечення безпеки даних.

Для проведення аналізу загроз та ризиків слід виконати такі дії:

1. Визначення інформаційних ресурсів та їх значущості – необхідно визначити, які дані є конфіденційними та критичними для діяльності компанії, і встановити, які ресурси та обладнання відповідають за зберігання та обробку цих даних.

2. Визначення загроз – необхідно визначити потенційні загрози, які можуть призвести до витоку або пошкодження конфіденційної інформації. Це можуть бути зовнішні або внутрішні загрози. Зовнішні загрози можуть включати хакерські атаки, віруси та інші види кібератак. Внутрішні загрози можуть включати недбале ставлення до конфіденційної інформації з боку співробітників, витік даних в результаті помилок або недостатнього контролю доступу.

3. Оцінка ризиків – необхідно оцінити рівень ризику від кожної загрози та визначити можливі наслідки їх реалізації. Рівень ризику може бути визначений на основі імовірності виникнення загрози та можливих наслідків. Наприклад, ризик витоку конфіденційної інформації може мати серйозні

наслідки для діяльності компанії, тому його рівень ризику повинен бути визначений високим.

4. Визначення заходів захисту – на основі оцінки ризиків необхідно визначити необхідні заходи захисту та плани надзвичайних ситуацій для відповідного впровадження. Це можуть бути технічні заходи, такі як шифрування, контроль доступу, системи виявлення інтрузій та інші, або організаційні заходи, такі як політики безпеки, процедури резервного копіювання, процедури перевірки досвіду та ін.

5. Планування та реалізація – після визначення заходів захисту необхідно скласти план реалізації та впровадження цих заходів. У плані повинні бути визначені терміни впровадження, бюджет та інші важливі деталі.

Аналіз загроз та ризиків є важливим етапом розробки засобів захисту інформаційних ресурсів з обмеженим доступом ІКС. Він допомагає визначити пріоритетні напрями захисту та необхідні заходи для забезпечення безпеки даних. Після аналізу загроз та ризиків можуть бути виявлені необхідні зміни в існуючій системі безпеки, які допоможуть забезпечити надійний захист інформації від різноманітних загроз.

Після проведення аналізу загроз та ризиків, важливо регулярно моніторити безпеку інформаційних ресурсів та вживати необхідних заходів для запобігання ризикам.

Наприклад, можуть бути встановлені системи виявлення інтрузій та інших загроз, що сповіщають про можливі атаки на систему. Для моніторингу безпеки можуть використовуватись спеціальні інструменти, такі як системи журналювання подій, які дозволяють відслідковувати дії користувачів у системі та виявляти можливі аномалії.

Важливо проводити регулярні оновлення та патчі для програмного забезпечення та операційної системи, що зменшує ризик використання програмних вразливостей зловмисниками.

Також можуть бути встановлені технічні засоби контролю доступу, такі як карти доступу, або біометричні системи ідентифікації, що дозволяють контролювати доступ до конфіденційної інформації.

У кожній організації повинен бути розроблений план надзвичайних ситуацій, що містить в собі процедури дій в разі виявлення загроз та інцидентів в області інформаційної безпеки.

Нарешті, слід пам'ятати про необхідність навчання персоналу, який працює з інформаційними ресурсами, щодо правил та процедур безпеки, щоб забезпечити свідоме та відповідальне ставлення до інформації.

У цілому, проведення аналізу загроз та ризиків є важливим етапом розробки засобів захисту інформаційних ресурсів з обмеженим доступом ІКС. Для успішного впровадження заходів захисту необхідно проводити регулярну моніторинг та оновлення системи безпеки, використовуючи сучасні технології та засоби захисту. Також важливо мати план надзвичайних ситуацій та план дій в разі виявлення загроз та інцидентів в області інформаційної безпеки. Для успішного захисту даних необхідно мати свідомий та відповідальний підхід до безпеки інформації, що включає в собі навчання персоналу та впровадження ефективних процедур безпеки.

Нарешті, важливо пам'ятати, що загрози безпеці інформації постійно змінюються, тому аналіз загроз та ризиків необхідно проводити регулярно, а заходи захисту оновлювати та адаптувати до нових потенційних загроз. Тільки так можна забезпечити надійний та ефективний захист інформаційних ресурсів з обмеженим доступом ІКС.

1.1.2 Визначення обмеженого доступу

Визначення обмеженого доступу є другим етапом розробки засобів захисту інформаційних ресурсів з обмеженим доступом ІКС. Цей етап передбачає визначення прав доступу користувачів до інформаційних ресурсів та обладнання системи. Визначення обмеженого доступу має на меті забезпечення контролю доступу до конфіденційної інформації та запобігання можливим загрозам безпеці даних.

Для визначення обмеженого доступу до інформаційних ресурсів слід виконати наступні дії:

1. Визначення ролей користувачів – необхідно визначити різні ролі користувачів системи та їхні права доступу до інформаційних ресурсів. Наприклад, адміністратор системи має повний доступ до всіх інформаційних ресурсів, тоді як звичайні користувачі можуть мати доступ лише до певних ресурсів, що необхідні для виконання їх робочих обов'язків.

2. Встановлення політик доступу – необхідно встановити правила та процедури доступу до інформаційних ресурсів, що відповідають визначеним ролям користувачів. Це може включати політику паролів, обмеження доступу до конфіденційних даних, контроль доступу до мережі та інше.

3. Встановлення системи авторизації та аутентифікації – необхідно встановити систему авторизації та аутентифікації, яка дозволить ідентифікувати користувачів та надавати їм відповідні права доступу до інформаційних ресурсів. Це може включати використання паролів, карт доступу, біометричних систем та інших технічних засобів ідентифікації.

4. Встановлення системи контролю доступу – необхідно встановити систему контролю доступу, яка дозволить контролювати доступ користувачів до інформаційних ресурсів. Це може включати системи контролю доступу на рівні мережі, операційної системи та додатків.

5. Визначення прав доступу – необхідно визначити права доступу користувачів до інформаційних ресурсів відповідно до їхніх ролей та профілю робочих обов'язків. Наприклад, звичайний користувач може мати доступ лише до певних ресурсів, тоді як адміністратор має повний доступ до всіх ресурсів системи.

6. Встановлення системи моніторингу доступу – необхідно встановити систему моніторингу доступу, яка дозволить відслідковувати дії користувачів у системі та виявляти можливі аномалії. Це допоможе виявити можливі загрози безпеці даних та запобігти їх виникненню.

7. Встановлення системи аудиту доступу – необхідно встановити систему аудиту доступу, яка дозволить відслідковувати всі дії користувачів у системі та зберігати цю інформацію для подальшого аналізу. Це може допомогти виявити можливі загрози безпеці даних та виявити потенційні проблеми у системі безпеки.

Визначення обмеженого доступу до інформаційних ресурсів є важливим етапом розробки засобів захисту інформаційних ресурсів з обмеженим доступом ІКС. Цей етап дозволяє забезпечити контроль доступу до конфіденційної інформації та запобігти можливим загрозам безпеці даних. Після визначення прав доступу необхідно перевірити їх ефективність та адаптувати за необхідності для забезпечення максимальної безпеки даних.

1.1.3 Захист від несанкціонованого доступу

Захист від несанкціонованого доступу є третім етапом розробки засобів захисту інформаційних ресурсів з обмеженим доступом ІКС. Цей етап передбачає впровадження заходів захисту, що дозволяють запобігти несанкціонованому доступу до інформаційних ресурсів.

Для захисту від несанкціонованого доступу слід виконати наступні дії:

1. Встановлення захисту пароля – необхідно встановити політику паролів, що відповідає вимогам безпеки, а також використовувати сучасні алгоритми хешування та шифрування паролів.

2. Встановлення фізичного захисту – необхідно встановити фізичний захист для серверних приміщень, дата-центрів та іншого обладнання, що забезпечує роботу ІКС. Це може включати використання систем контролю доступу, відеоспостереження та інших засобів захисту.

3. Встановлення системи захисту мережі – необхідно встановити систему захисту мережі, що дозволяє контролювати доступ до мережевих ресурсів та запобігати несанкціонованому доступу до інформаційних ресурсів.

4. Встановлення системи шифрування – необхідно встановити систему шифрування для захисту конфіденційної інформації в мережі, базах даних та інших інформаційних ресурсах.

5. Встановлення системи виявлення інтрузій – необхідно встановити систему виявлення інтрузій, яка дозволяє відслідковувати незвичайну активність та виявляти можливі атаки на систему.

6. Встановлення системи захисту від вірусів та інших шкідливих програм – необхідно встановити систему захисту від вірусів та інших шкідливих програм, що дозволяє запобігати можливій інфікуванню системи та поширенню шкідливих програм.

7. Встановлення системи резервного копіювання – необхідно встановити систему резервного копіювання, що дозволяє зберігати копії даних на випадок втрати чи пошкодження оригінальних даних.

8. Встановлення системи аудиту – необхідно встановити систему аудиту, що дозволяє відслідковувати всі дії користувачів та зберігати цю інформацію для подальшого аналізу. Це допоможе виявити можливі загрози безпеці даних та виявити потенційні проблеми у системі безпеки.

9. Визначення системи захисту даних – необхідно визначити систему захисту даних, що дозволяє захистити конфіденційну інформацію від несанкціонованого доступу та зберігати її в захищеному вигляді.

10. Встановлення процедур безпеки – необхідно встановити процедури безпеки для користувачів системи, які дозволяють забезпечити безпеку даних та запобігти можливим загрозам. Це може включати процедури зміни паролів, використання сильних паролів, процедури заборони використання певних додатків та інші.

Встановлення заходів захисту від несанкціонованого доступу є важливим етапом розробки засобів захисту інформаційних ресурсів з обмеженим доступом ІКС. Цей етап дозволяє забезпечити максимальний захист від можливих загроз та інцидентів, що можуть виникнути в процесі роботи системи. Після встановлення заходів захисту необхідно перевірити їх ефективність та адаптувати за необхідності для забезпечення максимальної безпеки даних і системи в цілому. Також необхідно регулярно проводити аудит

безпеки, щоб переконатися у тому, що заходи захисту працюють ефективно та відповідають вимогам безпеки.

Загальною метою заходів захисту від несанкціонованого доступу є забезпечення безпеки інформації, що зберігається в ІКС. Це дозволяє забезпечити конфіденційність, цілісність та доступність інформації, що є важливими для бізнесу та громадської безпеки. Оскільки загрози безпеці даних постійно змінюються та розвиваються, необхідно регулярно оновлювати заходи захисту, щоб забезпечувати максимальний рівень безпеки інформації в ІКС.

1.1.4 Моніторинг системи

Моніторинг системи є четвертим етапом розробки засобів захисту інформаційних ресурсів з обмеженим доступом ІКС. Цей етап передбачає встановлення системи моніторингу, що дозволяє відслідковувати стан системи та виявляти можливі проблеми та загрози безпеці даних.

Для ефективного моніторингу системи слід виконати наступні дії:

1. Визначення ключових параметрів системи – необхідно визначити ключові параметри системи, які необхідно моніторити для виявлення можливих проблем та загроз безпеці даних. Це може включати моніторинг обсягу пам'яті, робочого процесора, обсягу дискового простору та інших параметрів.

2. Встановлення системи моніторингу – необхідно встановити систему моніторингу, що дозволяє відслідковувати стан системи та ключових параметрів. Це може включати використання спеціальних програмних засобів, які збирають дані про стан системи та надсилають їх на сервер моніторингу.

3. Встановлення системи оповіщення – необхідно встановити систему оповіщення, яка дозволяє отримувати повідомлення про незвичайні стани системи або можливі загрози безпеці даних. Це може включати використання електронної пошти, SMS-повідомлень та інших засобів оповіщення.

4. Визначення порогових значень – необхідно визначити порогові значення для кожного з ключових параметрів системи. Це дозволяє визначити межі, поза якими вважатиметься, що система знаходиться в небезпечному стані.

5. Визначення процедур реагування – необхідно визначити процедури реагування на виявлені проблеми та загрози безпеці даних. Це може включати автоматичне відновлення системи, заблокування користувачів, що порушують правила безпеки, та інші заходи.

6. Встановлення засобів збереження даних моніторингу – необхідно встановити засоби збереження даних моніторингу, що дозволяють зберігати історію стану системи та ключових параметрів. Це допомагає відслідковувати тенденції в розвитку проблем та загроз безпеці даних, що може допомогти в запобіганні подібних інцидентів у майбутньому.

7. Використання аналітичних засобів – необхідно використовувати аналітичні засоби для аналізу зібраних даних моніторингу. Це дозволяє виявляти тенденції та знаходити причини проблем та загроз безпеці даних.

8. Встановлення системи захисту від вторгнень – необхідно встановити систему захисту від вторгнень, що дозволяє виявляти та запобігати спробам несанкціонованого доступу до системи.

9. Встановлення системи моніторингу та аудиту – необхідно встановити систему моніторингу та аудиту, що дозволяє відслідковувати дії користувачів та виявляти можливі загрози безпеці даних.

Моніторинг системи допомагає забезпечити максимальний рівень безпеки даних та зменшити ризик виникнення проблем у майбутньому. Дані, що збираються системою моніторингу, можуть допомогти виявити потенційні загрози безпеці даних та вчасно вжити заходи для їх запобігання. Крім того, моніторинг системи допомагає виявляти проблеми у процесах роботи системи, що може допомогти в запобіганні відмовам та відновленні роботи системи у разі її збою. За результатами моніторингу можуть бути внесені зміни до процедур безпеки та до заходів захисту, що дозволяє покращити рівень безпеки системи в цілому.

1.1.5 Тестування та аналіз результатів

Тестування та аналіз результатів є п'ятим етапом розробки засобів захисту інформаційних ресурсів з обмеженим доступом ІКС. Цей етап передбачає

виконання тестів з метою перевірки ефективності та правильності роботи засобів захисту та аналіз результатів тестування.

Для ефективного тестування та аналізу результатів слід виконати наступні дії:

1. Визначення тестових випадків – необхідно визначити тестові випадки, які дозволять перевірити ефективність та правильність роботи засобів захисту. Це може включати випадки з несанкціонованим доступом до системи, спробами атак з мережі, відправлення шкідливого програмного коду та інших можливих загроз.

2. Виконання тестів – після визначення тестових випадків необхідно виконати тести для перевірки ефективності та правильності роботи засобів захисту. Тести можуть бути виконані за допомогою спеціальних програмних засобів, що дозволяють імітувати можливі загрози безпеці даних.

3. Аналіз результатів – після виконання тестів необхідно проаналізувати отримані результати та визначити ефективність та правильність роботи засобів захисту. Це може включати оцінку рівня захисту від можливих загроз, визначення проблем та слабких місць у системі захисту, а також визначення рівня ефективності виявлення та блокування можливих загроз.

4. Внесення змін – після аналізу результатів можуть бути внесені зміни до засобів захисту та процедур безпеки. Це може включати встановлення нових заходів захисту, зміну параметрів системи, яка відповідає захисту, а також внесення змін до процедур безпеки, що дозволить покращити рівень захисту та зменшити ризик виникнення можливих загроз.

5. Повторне тестування – після внесення змін необхідно повторно виконати тестування для перевірки ефективності та правильності роботи засобів захисту. Це дозволяє переконатися у тому, що внесені зміни спрацювали ефективно та відповідають вимогам безпеки.

6. Документування результатів – після тестування та аналізу результатів необхідно документувати отримані результати. Це допоможе зберегти

інформацію про ефективність та правильність роботи засобів захисту, що може бути корисним для подальшого покращення системи захисту.

Тестування та аналіз результатів є важливим етапом розробки засобів захисту інформаційних ресурсів з обмеженим доступом ІКС. Це дозволяє перевірити ефективність та правильність роботи засобів захисту, виявити можливі проблеми та слабкі місця в системі захисту, а також внести зміни для покращення рівня захисту та зменшення ризиків безпеки даних. Тестування та аналіз результатів є важливою частиною процесу підтримки безпеки даних в ІКС, що дозволяє забезпечити надійний захист даних та інформаційних ресурсів в цілому.

1.2 Опис виду діяльності підприємства

Підприємство з продажу побутової техніки займається роздрібною торгівлею побутовою технікою та іншими товари для дому. Ця діяльність включає в себе наступні етапи:

Закупівля товарів – підприємство закуповує товари від виробників або дистриб'юторів, зазвичай з оптової бази. Закупівля може бути здійснена з деякою періодичністю, або при необхідності поповнення асортименту.

Складський облік – після отримання товару, його слід прийняти на склад і здійснити його облік. Це включає в себе ідентифікацію товару, оцінку його якості, визначення місця для зберігання та внесення до складської книги.

Продаж – підприємство здійснює продаж побутової техніки відвідувачам свого магазину або онлайн. Перед продажем, продавець повинен показати товар покупцеві, пояснити його особливості та відповісти на всі питання. Після того, як покупець обрав товар, він оформляє замовлення та проводить оплату.

Після продажне обслуговування – після продажу, підприємство забезпечує після продажне обслуговування, що може включати в себе встановлення товару, налаштування, гарантійне та післягарантійне обслуговування.

Реклама та маркетинг – підприємство здійснює рекламу та маркетингову діяльність для залучення покупців, зокрема розміщення реклами в ЗМІ та

соціальних мережах, проведення рекламних кампаній та акцій, знижки, програми лояльності та інше.

Аналіз продажів та звіти – підприємство проводить аналіз продажів, щоб визначити найбільш популярні товари, ефективність маркетингових кампаній, обсяги продажів та інші показники. Це допомагає підприємству виявляти тенденції ринку та виробляти стратегічні рішення.

Управління запасами – підприємство веде управління запасами для планування закупівлі товарів та управління їх рухом на складі. Для цього використовуються різноманітні програмні засоби, що дозволяють автоматизувати процеси управління запасами та складського обліку.

Обслуговування сайту та Інтернет-магазину – здійснює обслуговування сайту та Інтернет-магазину, оновлює каталог товарів, додає описи та фото товарів, забезпечує безпеку оплати та інше.

Підприємство з продажу побутової техніки має ряд викликів, зокрема конкуренцію на ринку, швидкий розвиток технологій та зміну попиту на товари. Однак, здійснення всіх етапів діяльності та використання сучасних технологій дозволяє підприємству зберегти свої позиції на ринку та задовольнити потреби своїх клієнтів.

1.3 Посадові обов'язки персоналу підприємства з продажу побутової техніки

На підприємстві визначені наступні посади: директор підприємства, заступник директора, менеджер з закупівлі товарів, спеціаліст з логістики, менеджер з продажу, спеціаліст сервісного центру, маркетолог, бухгалтер, бізнес аналітик, контент-менеджер сайту підприємства, системний адміністратор, охоронець, прибиральниця.

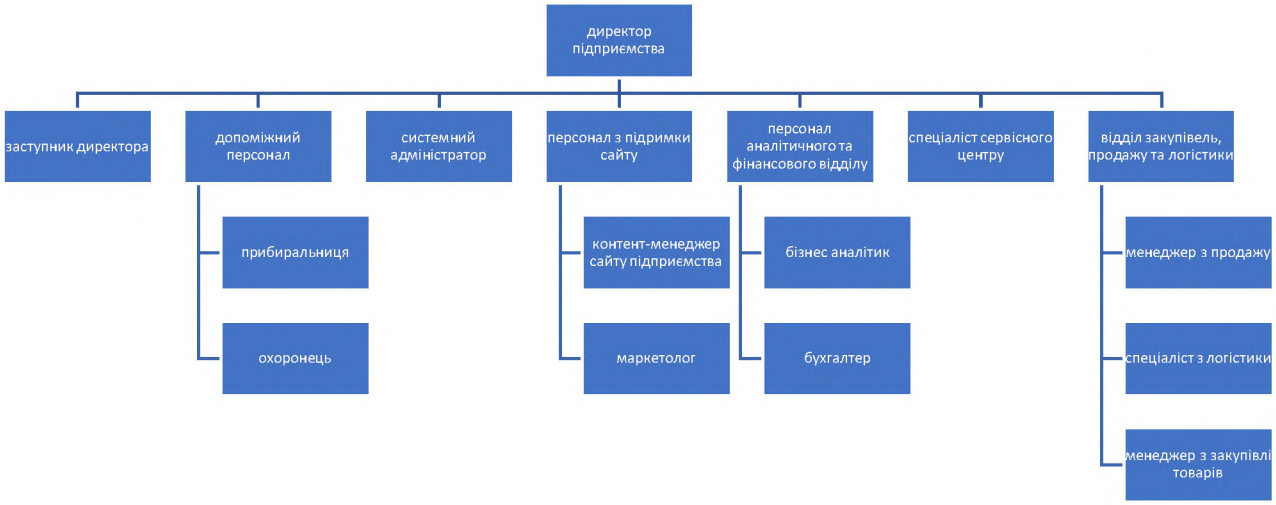

Рисунок 1.1 – Організаційна структура

Директор підприємства:

– Визначає стратегію розвитку підприємства та встановлює мету і завдання для керівництва та персоналу;

– Керує роботою підприємства, контролює діяльність всіх підрозділів;

– Приймає рішення з питань фінансової та економічної діяльності підприємства;

– Установлює зв'язки з постачальниками та клієнтами, розвиває нові напрями бізнесу;

– Веде переговори з партнерами та інвесторами;

– Організовує роботу з управління персоналом та забезпечує виконання вимог стандартів якості та безпеки.

Заступник директора:

– Виконує обов’язки директора підприємства в його відсутності;

– Відповідає за планування та реалізацію проектів;

– Координує діяльність всіх підрозділів;

– Забезпечує дотримання процедур та стандартів якості та безпеки.

Менеджер з закупівлі товарів:

– Відповідає за закупівлю та забезпечення асортименту товарів;

– Аналізує ринок та вибирає постачальників;

– Планує та контролює витрати на закупівлю товарів.

Спеціаліст з логістики:

– Відповідає за організацію перевезення товарів від постачальника до складу та від складу до клієнтів;

– Відповідає за оптимізацію логістичних процесів та зниження витрат на доставку товарів.

Менеджер з продажу:

– Відповідає за продаж товарів в магазині або через інтернет-магазин;

– Забезпечує високий рівень обслуговування клієнтів та розвиток взаємин відносин з ними;

– Планує та контролює роботу менеджерів з продажу;

– Аналізує продажі та розробляє стратегію продажів.

Спеціаліст сервісного центру:

– Відповідає за прийом та обробку заявок на гарантійний та післягарантійний ремонт товарів;

– Координує роботу технічних спеціалістів та контролює якість виконання ремонтних робіт.

Маркетолог:

– Розробляє маркетингові стратегії та рекламні кампанії;

– Вивчає попит на товари та аналізує конкуренцію;

– Планує та контролює бюджет маркетингових заходів;

– Розробляє рекламні матеріали та контент для рекламних кампаній.

Бухгалтер:

– Відповідає за ведення бухгалтерського обліку та звітності підприємства;

– Планує та контролює фінансову діяльність підприємства;

– Розробляє бюджет та фінансові плани.

Бізнес аналітик:

– Аналізує економічну та фінансову діяльність підприємства;

– Розробляє стратегію розвитку та оптимізації бізнес-процесів;

– Вивчає ринок та конкурентів;

– Розробляє рекомендації для підвищення ефективності діяльності підприємства.

Контент-менеджер сайту підприємства:

– Розробляє та оновлює контент на сайті підприємства;

– Розробляє стратегію просування сайту та контенту в соціальних мережах;

– Аналізує показники відвідуваності та ефективності сайту.

Системний адміністратор:

– Відповідає за налагодження, підтримку та безпеку IT-інфраструктури підприємства;

– Забезпечує роботу комп'ютерів, програмного забезпечення та інших технічних засобів;

– Контролює захист інформації на серверах та інших пристроях;

– Забезпечує безперебійну роботу мережі інтернет та локальної мережі підприємства.

Охоронець:

– Відповідає за забезпечення безпеки підприємства та його майна;

– Контролює доступ на територію підприємства;

– Забезпечує порядок та безпеку на території підприємства;

– Реагує на випадки порушень правил поведінки на території підприємства.

Прибиральниця:

– Відповідає за прибирання та збереження чистоти на території підприємства;

– Забезпечує порядок у приміщеннях підприємства.

Кожен з перелічених співробітників відповідає за власний розділ діяльності на підприємстві та співпрацює з іншими підрозділами. Успішна робота підприємства залежить від ефективності роботи кожного співробітника.

1.4 Інформація яка циркулює в ІКС підприємства

В інформаційній системі підприємства між зазначеними користувачами можуть циркулювати різні види інформації. Основні види інформації, що можуть оброблятися в інформаційній системі підприємства та циркулювати між користувачами, включають:

- Інформація про клієнтів: дані про клієнтів, їхні замовлення, контактні дані та інші характеристики.
- Інформація про товари: дані про асортимент товарів, його опис, вартість, кількість на складі та інші характеристики.
- Інформація про виробництво: дані про процес виробництва, використання матеріалів та обладнання, забезпечення якості продукції.
- Фінансова інформація: дані про бухгалтерський облік, доходи та витрати підприємства, фінансові показники та звіти.
- Інформація про персонал: дані про співробітників, їхні трудові угоди, відомості про заробітну плату та соціальні виплати.
- Інформація про логістику: дані про процес доставки товарів та контроль їхнього руху від постачальника до клієнта.
- Інформація про маркетинг: дані про стратегії маркетингу, проведені рекламні кампанії, аналітику ринку та конкурентів.
- Інформація про безпеку: дані про захист інформації, фізичну та технічну безпеку на підприємстві.

Ці види інформації можуть бути обмінювані між різними користувачами інформаційної системи підприємства в режимі онлайн або офлайн. Важливим елементом цього процесу є забезпечення безпеки даних та контроль доступу до них, щоб запобігти несанкціонованому доступу до конфіденційної інформації. Інформаційна система підприємства повинна забезпечувати можливість обміну

даними між користувачами на різних рівнях доступу, забезпечувати автоматичну інтеграцію даних з різних джерел, автоматизувати процеси аналізу та обробки інформації, а також забезпечувати збереження та архівування даних.

Крім того, інформаційна система підприємства може включати різні модулі, що забезпечують різноманітні функції, такі як:

Модуль управління продажами: забезпечує можливість планування, контролю та аналізу продажів, керування запасами та взаємодію з клієнтами.

Модуль управління виробництвом: забезпечує можливість контролю та аналізу процесу виробництва, планування використання матеріалів та обладнання, а також забезпечує якість продукції.

Модуль управління персоналом: забезпечує можливість керування трудовими відносинами, планування кадрових ресурсів та зарплат, аналізу ефективності праці та контролю за дотриманням законодавства.

Модуль управління фінансами: забезпечує можливість контролю та аналізу фінансової діяльності, планування та контролю витрат, управління податками та іншими фінансовими аспектами.

Модуль управління складом: забезпечує можливість контролю та аналізу запасів на складі , їхньої руху, планування та контролю поставок та забезпечення доступу до інформації про наявність товарів.

Модуль управління логістикою: забезпечує можливість контролю та аналізу доставки товарів, відслідковування маршрутів транспорту та забезпечення взаємодії з постачальниками та перевізниками.

Модуль управління маркетингом: забезпечує можливість аналізу ринку та конкурентів, планування та контролю маркетингових акцій, збору та аналізу відгуків клієнтів.

Модуль управління інформацією: забезпечує можливість збору, аналізу та обробки різноманітної інформації, в тому числі текстової, графічної, відео- та аудіоінформації, а також забезпечує її збереження та архівування.

Модуль управління безпекою: забезпечує можливість захисту конфіденційної інформації, контролю доступу до даних та забезпечення фізичної та технічної безпеки на підприємстві.

Модуль управління взаємодією з клієнтами: забезпечує можливість взаємодії з клієнтами через різні канали комунікації, включаючи телефон, електронну пошту, чат, соціальні мережі та інші.

Модуль управління контентом: забезпечує можливість створення та редагування контенту на сайті підприємства, його оптимізацію та просування в Інтернеті.

Кожен з цих модулів може мати власну базу даних та користувацький інтерфейс для керування функціями та доступом до даних. Наприклад, директор підприємства може мати доступ до всіх модулів та функцій інформаційної системи, в той час як менеджер з продажу може мати доступ тільки до модулю управління продажами та обміну даними з модулем управління персоналом. Бізнес-аналітик може мати доступ до модулів управління фінансами та складом для аналізу показників ефективності підприємства.

Таким чином, інформаційна система підприємства забезпечує можливість обробки та аналізу великої кількості даних, взаємодії різних підрозділів та співробітників, а також забезпечує ефективну управлінську діяльність підприємства.

Таблиця видів інформації, що циркулюють в різних модулях інформаційної системи підприємства:

Таблиця 1.1 – Види інформації які циркулюють на підприємстві

Користувач ІКС	Вид інформації	Режим доступу	Вид модуля управління
Директор підприємства	Фінансові звіти, стратегічні дані, плани	З обмеженим доступом	Модуль управління фінансами
Заступник	Дані про кадри, трудові	З обмеженим	Модуль

Користувач ІКС	Вид інформації	Режим доступу	Вид модуля управління
директора	договори, звіти	доступом	управління персоналом
Менеджер з закупівлі	Дані про постачальників, замовлення	З обмеженим доступом	Модуль управління складом
Спеціаліст з логістики	Дані про доставку товарів, склад запасів	З обмеженим доступом	Модуль управління логістикою
Менеджер з продажу	Звіти про продажі, клієнтська база	З обмеженим доступом	Модуль управління продажами
Спеціаліст сервісного центру	Дані про ремонт, гарантії, сервісні центри	З обмеженим доступом	Модуль управління сервісом
Маркетолог	Дані про конкурентів, ринок, маркетингові акції	З обмеженим доступом	Модуль управління маркетингом
Бухгалтер	Дані про оплату, звіти про доходи та витрати	З обмеженим доступом	Модуль управління фінансами
Бізнес-аналітик	Аналітичні дані про ефективність роботи підприємства	З обмеженим доступом	Модуль управління фінансами, модуль управління складом
Контент-менеджер сайту	Контент сайту підприємства	Відкритий доступ	Модуль управління контентом
Охоронець	Дані про безпеку на території підприємства, відеоспостереження	З обмеженим доступом	Модуль управління безпекою
Прибиральниця	Дані про розміщення обладнання та матеріалів	Відкритий доступ	Модуль управління складом
Системний	Дані про налаштування	З обмеженим	Модуль

Користувач ІКС	Вид інформації	Режим доступу	Вид модуля управління
адміністратор	та підтримку інформаційної системи	доступом	управління інформацією, модуль управління безпекою

1.5 Типова інформаційна система підприємства з продажу побутової техніки

Інформаційна система підприємства з продажу побутової техніки може містити різноманітне обладнання та програмне забезпечення для забезпечення роботи різних модулів та користувачів.

Для забезпечення роботи модулів управління, таких як управління продажами, управління складом, управління персоналом та фінансове управління, можуть використовуватися такі програмні засоби:

– ERP-системи, такі як Oracle, SAP, Microsoft Dynamics. Вони дозволяють автоматизувати бізнес-процеси інтеграцією різних функцій і модулів, таких як управління продажами, складом, фінансами та кадрами.

– CRM-системи, такі як Salesforce, Zoho CRM, Bitrix24. Вони дозволяють управляти клієнтською базою, контактами та продажами.

– Бухгалтерські програми, такі як 1С, QuickBooks, Xero. Вони дозволяють вести облік доходів та витрат, складання фінансових звітів та податкової звітності.

Для забезпечення безпеки та захисту інформації в інформаційній системі підприємства можуть використовуватися такі програмні та апаратні засоби:

– Антивірусне програмне забезпечення, таке як McAfee, Norton. Воно дозволяє захистити систему від вірусів, троянів та інших загроз.

– Firewall, такий як Cisco, Fortinet, SonicWall. Він дозволяє захистити мережу від несанкціонованого доступу та заблокувати небезпечний трафік.

– Системи резервного копіювання, такі як Veeam, Acronis, Backup Exec. Вони дозволяють зберегти резервну копію даних та відновити їх у разі втрати або пошкодження.

Для користувачів, які працюють з інформаційною системою підприємства, можуть використовуватися такі програмні та апаратні засоби:

– робочі станції. Вони можуть бути звичайними ПК або ноутбуками, що мають встановлене необхідне програмне забезпечення та підключені до локальної мережі.

– монітори. Вони дозволяють відображати інформацію, що обробляється в інформаційній системі, та робити різні операції з даними.

– принтери та сканери. Вони дозволяють друкувати та сканувати документи, які зберігаються в інформаційній системі.

– мережеві пристрої. Вони дозволяють підключати робочі станції та інші пристрої до локальної мережі, що забезпечує обмін даними та спільний доступ до ресурсів.

– Активна мережева апаратура, така як комутатори та маршрутизатори, дозволяють підключати комп'ютери до мережі та забезпечувати безперебійну роботу мережі.

– VPN-з'єднання та інші засоби забезпечення віддаленого доступу до інформаційної системи.

– Клавіатури та миші, які дозволяють користувачам взаємодіяти з інформаційною системою.

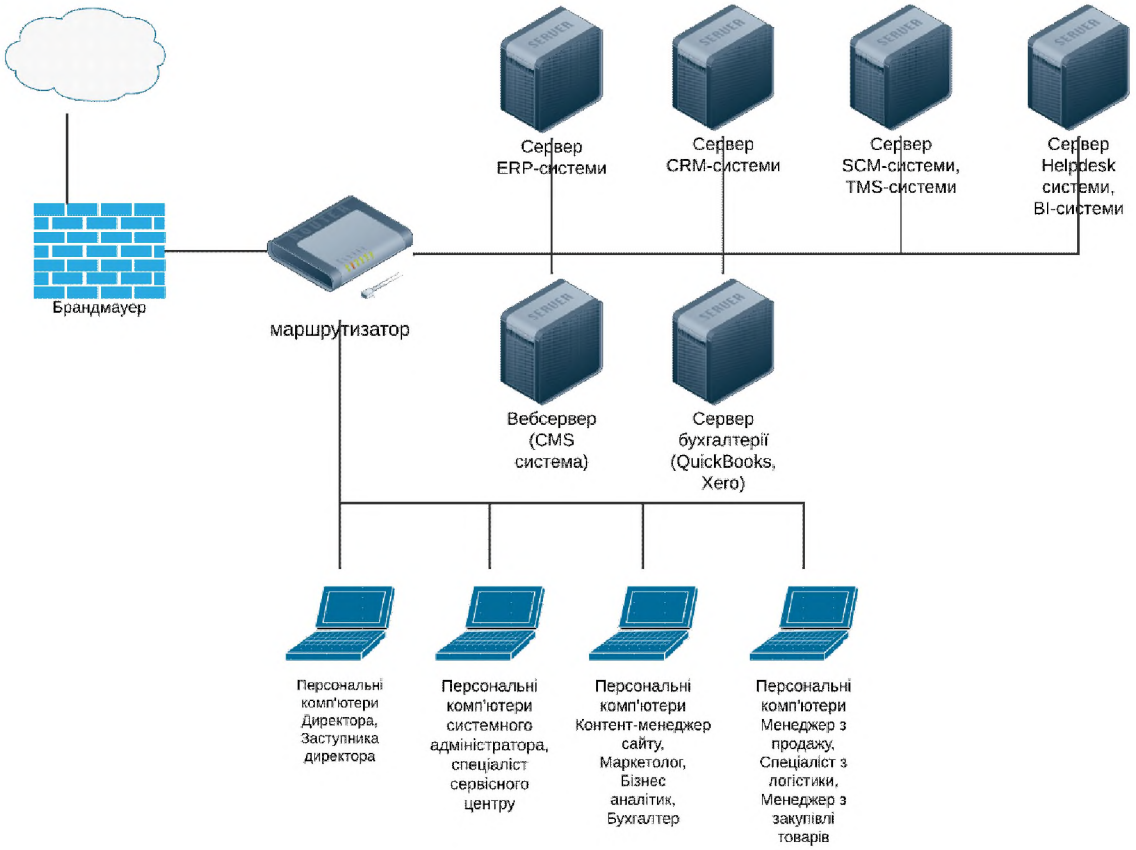

Рисунок 1.2 – Інформаційна система підприємства

Враховуючи специфіку роботи різних користувачів та модулів управління, можуть використовуватися різні обладнання та програмне забезпечення. Наприклад, менеджер з продажу може працювати з CRM-системою, яка дозволяє керувати продажами та клієнтською базою, тоді як спеціаліст з сервісного центру може використовувати програмні засоби для керування ремонтом та гарантією на побутову техніку. Директор підприємства може використовувати ERP-систему для контролю фінансової діяльності та керування бізнес-процесами, а бізнес-аналітик може використовувати програмне забезпечення для аналізу даних та формування звітності.

Для забезпечення безпеки даних та захисту від несанкціонованого доступу можуть використовуватися різні програмні та апаратні засоби, такі як

антивірусне програмне забезпечення, фаєрволи, системи резервного копіювання та інші.

Для моніторингу та аналізу роботи інформаційної системи можуть використовуватися спеціальні програмні засоби, такі як системи моніторингу мережі, системи логування подій та інші. Ці засоби дозволяють відстежувати роботу різних модулів, перевіряти виконання правил доступу до даних та забезпечувати безпеку та надійність роботи інформаційної системи.

Окрім того, для забезпечення роботи сайту підприємства можуть використовуватися такі програмні засоби, як система управління контентом (CMS), система аналітики вебтрафіку, програми для оптимізації SEO та інші. Ці засоби дозволяють керувати контентом сайту, аналізувати його відвідуваність та підвищувати його рейтинг в пошукових системах.

Зокрема, для підтримки взаємодії з клієнтами та забезпечення їхнього зручного обслуговування на сайті підприємства може бути встановлено спеціальну систему онлайн-консультацій або чат-бот, які дозволяють швидко та ефективно відповідати на запитання клієнтів та вирішувати їхні проблеми.

Загалом, обладнання та програмне забезпечення інформаційної системи підприємства з продажу побутової техніки залежать від потреб та особливостей діяльності підприємства. Важливо забезпечити ефективну роботу різних модулів управління та забезпечити безпеку та надійність даних, що обробляються в інформаційній системі.

Нижче подано таблицю, яка відображає залежність між користувачами ІКС, модулями управління та програмним забезпеченням, що використовуються в інформаційній системі підприємства з продажу побутової техніки.

Таблиця 1.2 – Програмне забезпечення модулів управління інформаційної системи підприємства

Користувач ІКС	Вид модуля управління	Програмне забезпечення
Директор	ERP-система	Oracle, SAP, Microsoft Dynamics

Користувач ІКС	Вид модуля управління	Програмне забезпечення
Заступник директора	CRM-система	Salesforce, Microsoft Dynamics
Менеджер з закупівлі товарів	SCM-система	SAP Ariba, Oracle, Coupa
Спеціаліст з логістики	TMS-система	Oracle Transportation Management
Менеджер з продажу	CRM-система	Salesforce, Microsoft Dynamics
Спеціаліст сервісного центру	Helpdesk система	Zendesk, Jira Service Desk
Маркетолог	CMS система	WordPress, Drupal, Joomla
Бізнес-аналітик	BI-система	Tableau, Power BI, QlikView
Бухгалтер	Бухгалтерський ПЗ	1С, QuickBooks, Xero
Контент-менеджер сайту підприємства	CMS система	WordPress, Drupal, Joomla
Системний адміністратор	системи безпеки IT	Symantec, McAfee

Відповідно до специфіки діяльності та потреб різних модулів управління використовуються різні програмні засоби. Для директора та заступника директора важливо мати доступ до ERP- та CRM-систем, відповідно. Менеджер з закупівлі товарів використовує SCM-систему для керування поставками та закупівлями, а спеціаліст з логістики використовує TMS-систему для керування транспортними ресурсами. Менеджер з продажу використовує CRM-систему для керування клієнтською базою та продажами, а спеціаліст сервісного центру використовує Helpdesk систему для керування запит ками на обслуговування.

Маркетолог використовує CMS-систему для керування контентом на сайті підприємства, а бізнес-аналітик використовує BI-систему для аналізу даних та формування звітності. Бухгалтер використовує спеціалізоване програмне забезпечення для обліку фінансів та податків, а контент-менеджер сайту підприємства використовує CMS-систему для керування контентом на сайті.

Нарешті, системний адміністратор забезпечує безпеку та надійність даних, використовуючи спеціалізовані програмні та апаратні засоби, такі як антивірусне програмне забезпечення та фаєрволи. Він також керує роботою

систем моніторингу та логування подій, що дозволяє відслідковувати роботу різних модулів управління та забезпечувати безпеку роботи інформаційної системи підприємства.

Отже, використання різних програмних засобів дозволяє різним користувачам ІКС виконувати свої функції та забезпечувати ефективну роботу інформаційної системи підприємства з продажу побутової техніки.

1.5.1 ERP-система

ERP-система (Enterprise Resource Planning) - це комп'ютерна програма для планування та управління різними процесами в підприємстві, такими як фінансове управління, управління персоналом, виробничий менеджмент, управління закупівлями та логістикою, управління проектами та ін.

ERP-система забезпечує інтеграцію та автоматизацію різних функцій та процесів, що забезпечує ефективну роботу всієї компанії та дозволяє зменшити витрати на управління та оптимізувати роботу підприємства.

У системі ERP використовуються централізовані бази даних, що дозволяє забезпечити єдиний доступ до інформації для всіх користувачів системи. Вона дозволяє керувати різними процесами, такими як управління запасами, виробництвом, продажами та маркетингом, фінансовим управлінням, звітністю та іншими.

Основною перевагою ERP-системи є можливість координації різних бізнес-процесів, які раніше працювали незалежно один від одного, тим самим зменшуючи витрати на робочу силу та збільшуючи продуктивність. ERP-системи дозволяють вирішувати більш складні задачі, такі як оптимізація ланцюга постачань, планування продажів та виробництва, управління взаємовідносинами з клієнтами та ін.

Серед популярних ERP-систем можна відзначити Oracle, SAP, Microsoft Dynamics, та інші. Ці системи можуть бути налаштовані під специфіку діяльності конкретного підприємства, що забезпечує максимальну ефективність та продуктивність управління різними процесами в підприємстві.

1.5.2 CRM-система

CRM-система (Customer Relationship Management) – це програмне забезпечення, яке допомагає підприємствам керувати взаємовідносинами з клієнтами. Основна мета CRM-системи полягає в зборі, аналізі та використанні даних про клієнтів з метою поліпшення їхнього досвіду з обслуговування та підвищення ефективності продажів.

CRM-система забезпечує можливість зберігати інформацію про клієнтів, їх контактні дані, історію спілкування з підприємством, замовлення та оплати, пропозиції та підказки щодо покупок. Вона також дозволяє керувати комунікацією з клієнтами, забезпечувати персоналу доступ до цієї інформації, а також робити аналіз даних та формувати звіти.

CRM-система може бути налаштована під специфіку діяльності конкретного підприємства, що дозволяє забезпечити максимальну ефективність та продуктивність управління взаємовідносинами з клієнтами. Наприклад, для торгових компаній це може бути система для відстеження продажів та керування контактами з клієнтами, а для сервісних компаній – система для відстеження запитів та підтримки клієнтів.

Серед популярних CRM-систем можна відзначити Salesforce, Microsoft Dynamics CRM, Zoho CRM, та інші. Окрім того, деякі підприємства можуть використовувати спеціалізовані CRM-системи, розроблені для конкретної галузі, такі як система керування відносинами з клієнтами для готелів, ресторанів, медичних закладів та ін.

1.5.3 SCM-система

SCM-система (Supply Chain Management) – це програмне забезпечення, яке допомагає підприємствам керувати логістичними процесами, поставками та інвентаризацією, які є частиною поставкового ланцюга. Основна мета SCM-системи полягає в управлінні всім процесом від постачальників до кінцевого споживача з метою оптимізації витрат та підвищення продуктивності.

SCM-система забезпечує можливість керувати процесами, пов'язаними з виробництвом та постачанням товарів, включаючи контроль запасів, координацію поставок та виробництва, відстеження доставок, аналіз даних та формування звітності. Вона також дозволяє підприємству працювати з постачальниками, управляти контрактами, робити планування та прогнозування попиту, вести облік інвентаря та відстеження витрат.

SCM-система може бути налаштована під специфіку діяльності конкретного підприємства, що дозволяє забезпечити максимальну ефективність та продуктивність управління поставковим ланцюгом. Наприклад, для виробничих компаній це може бути система для керування виробництвом та логістикою, а для торгових компаній - система для керування запасами та поставками.

Серед популярних SCM-систем можна відзначити SAP SCM, Oracle SCM, Microsoft Dynamics 365 Supply Chain Management, та інші. Окрім того, деякі підприємства можуть використовувати спеціалізовані SCM-системи, розроблені для конкретної галузі, такі як системи керування логістикою для готелів, ресторанів, медичних закладів та ін.

1.5.4 TMS-система

TMS-система (Transportation Management System) – це програмне забезпечення, яке допомагає підприємствам керувати логістичними процесами, пов'язаними з транспортуванням товарів та матеріалів. Основна мета TMS-системи полягає в підвищенні ефективності та оптимізації процесів транспортування з метою зменшення витрат та підвищення якості обслуговування.

TMS-система забезпечує можливість керувати процесами, пов'язаними з перевезенням товарів, включаючи планування маршрутів, вибір перевізника, відстеження вантажу, управління контрактами та платежами, аналіз даних та формування звітності. Вона також дозволяє керувати комунікацією з перевізниками та контролювати їх виконання договірних умов.

TMS-система може бути налаштована під специфіку діяльності конкретного підприємства, що дозволяє забезпечити максимальну ефективність та продуктивність управління транспортуванням. Наприклад, для логістичних компаній це може бути система для керування транспортом та маршрутами, а для виробничих компаній – система для керування доставкою сировини та готової продукції.

Серед популярних TMS-систем можна відзначити Oracle Transportation Management, SAP Transportation Management, MercuryGate TMS, та інші. Окрім того, деякі підприємства можуть використовувати спеціалізовані TMS-системи, розроблені для конкретної галузі, такі як системи керування транспортом для готелів, ресторанів, медичних закладів та ін.

1.5.5 Helpdesk система

Helpdesk-система (іноді також називається сервіс-деском або службою підтримки) – це програмне забезпечення, що допомагає організувати та керувати процесом надання технічної підтримки користувачам, які мають проблеми з використанням продуктів або послуг компанії.

Основна мета Helpdesk-систем полягає в тому, щоб забезпечити якісну та ефективну підтримку клієнтів, знизити час відгуку на запити, забезпечити швидке вирішення проблем, збільшити рівень задоволеності клієнтів і підвищити репутацію компанії.

Для досягнення цих цілей Helpdesk-система забезпечує такі можливості:

– реєстрація запитів та заявок від користувачів, надання інформації про статус запиту;

– керування розподілом та призначенням запитів на відповідальних співробітників;

– моніторинг виконання запитів та контроль якості наданої підтримки;

– аналіз запитів та статистичної інформації для покращення процесу надання підтримки та підвищення рівня задоволеності клієнтів.

Серед функцій, які надає Helpdesk-система можна виділити:

– систему тікетів для реєстрації запитів користувачів та їхнього моніторингу;

– систему електронної пошти та сповіщень для повідомлення клієнтів про стан їхнього запиту;

– систему бази знань, що містить інформацію про часті запити та їх рішення;

– інструменти для аналізу та звітування про роботу служби підтримки.

Серед популярних Helpdesk-систем можна виділити такі програмні продукти, як Freshdesk, Zendesk, Jira Service Desk, Salesforce Service Cloud та інші.

Helpdesk-система може бути використана на підприємствах будь-якої галузі, де потрібна технічна підтримка клієнтів або співробітників. Наприклад, на комп'ютерних підприємствах, де клієнти потребують допомоги в розв'язанні технічних проблем з програмним забезпеченням, або на підприємствах, де важливо швидко реагувати на запити клієнтів та забезпечити надання якісної технічної підтримки.

Helpdesk-система може бути інтегрована з іншими системами підприємства, наприклад з CRM-системою або з ERP-системою, для автоматизації процесу надання підтримки та покращення зв'язку з клієнтами. Така інтеграція дозволяє підприємствам підвищити ефективність та швидкість вирішення проблем клієнтів, а також отримувати додаткову інформацію про клієнтів та їх запити, що може бути використано для покращення продуктів та послуг компанії.

1.5.6 BI-система

BI-система (англ. Business Intelligence) – це програмне забезпечення, що дозволяє підприємствам отримувати, аналізувати та візуалізувати великі обсяги даних для прийняття рішень та управління бізнес-процесами. BI-система допомагає управлінцям та аналітикам отримати доступ до даних з різних

джерел, об'єднати їх в одну систему та виконувати аналіз, що допомагає зрозуміти стан підприємства та приймати рішення на основі даних.

BI-система складається з таких компонентів:

1. ETL-система (англ. Extract, Transform, Load) – це програмний компонент, який використовується для збору даних з різних джерел, їх обробки та зберігання в дата-складі.

2. Дата-склад (англ. Data Warehouse) – це централізована база даних, яка містить всі необхідні дані для аналізу. Дата-склад дозволяє зберігати дані в оптимізованому форматі для швидкого аналізу.

3. Аналітичний двір (англ. Analytical Cube) – це структуровані дані, які містяться в дата-складі та дозволяють виконувати швидкий аналіз даних за різними параметрами.

4. Інструменти візуалізації (англ. Visualization Tools) – це програмні засоби, які використовуються для візуалізації та відображення результатів аналізу даних у зручному для користувача форматі.

BI-системи дозволяють отримувати дані з різних джерел, включаючи бази даних, електронні таблиці, файлові системи та інші джерела, та об'єднувати їх у єдину систему. Для аналізу даних BI-системи використовують різні методи, включаючи статистичний аналіз, аналіз залежностей та інші методи. BI-системи дозволяють користувачам створювати звіти, графіки, дашборди та інші візуалізації, що допомагають зрозуміти динаміку даних та здійснювати прогнозування розвитку подій.

BI-системи використовуються в різних сферах бізнесу, включаючи фінанси, маркетинг, продажі, логістику та інші галузі. Наприклад, у фінансовій галузі BI-система може допомогти аналізувати доходи та витрати підприємства, прогнозувати прибутковість проектів та здійснювати моніторинг фінансового стану компанії. У маркетинговій галузі BI-система може допомогти аналізувати ринок та конкурентну ситуацію, визначати попит на продукцію та розробляти стратегії маркетингових кампаній.

Серед відомих BI-систем можна виділити такі програмні продукти, як Tableau, Power BI, QlikView, MicroStrategy та інші. Вони відрізняються за функціональністю, масштабом та іншими параметрами, але всі вони дозволяють користувачам отримувати, аналізувати та візуалізувати великі обсяги даних для прийняття рішень та управління бізнес-процесами.

1.6 Висновок

Зважаючи на описані модулі та користувачів інформаційної системи підприємства з продажу побутової техніки, можна зробити висновок, що така система включає в себе різні компоненти та програмні засоби, що спрямовані на автоматизацію різних бізнес-процесів, що відбуваються в підприємстві.

Особливості інформаційної системи підприємства з продажу побутової техніки включають:

1. Наявність різних модулів, що дозволяють автоматизувати різні бізнес-процеси, такі як закупівля товарів, логістика, продажі, обслуговування клієнтів тощо.
2. Наявність баз даних, що містять інформацію про товари, клієнтів, замовлення, операції з грошима та інші дані, необхідні для роботи підприємства.
3. Використання різних програмних засобів, що дозволяють виконувати аналіз даних, приймати рішення та управляти бізнес-процесами.

Види оброблювальної інформації в інформаційній системі підприємства з продажу побутової техніки включають інформацію про товари, клієнтів, замовлення, операції з грошима, аналітичні дані про ринок, конкурентів, фінансовий стан підприємства та інші дані, що дозволяють приймати рішення та управляти бізнес-процесами.

Однією з найважливіших проблем, що стикається інформаційна система підприємства з продажу побутової техніки, є несанкціонований доступ до системи. Це може призвести до витоку конфіденційної інформації, порушення безпеки даних, втрати даних або пошкодження програмного забезпечення. Для запобігання несанкціонованого доступу до системи можуть застосовуватися

різні заходи, такі як захист паролем, шифрування даних, контроль доступу, аудит та моніторинг системи, використання антивірусного програмного забезпечення та інші методи. Крім того, необхідно регулярно проводити навчання та свідомість користувачів про правила безпеки інформації та небезпеку несанкціонованого доступу до системи.

Інформаційна система підприємства з продажу побутової техніки є складною системою, що включає різні модулі та програмні засоби для автоматизації бізнес-процесів та забезпечення ефективного управління компанією. Вона містить велику кількість оброблювальної інформації про клієнтів, товари, замовлення та інші аспекти діяльності підприємства. Однією з ключових проблем, які стикається інформаційна система підприємства, є запобігання несанкціонованого доступу до системи, тому необхідно приділяти велику увагу заходам безпеки для забезпечення надійності та конфіденційності даних.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Модель загроз інформації

Модель загроз інформації – це систематичний підхід до виявлення, оцінки та управління загрозами для безпеки інформації в інформаційній системі. Основною метою цієї моделі є захист інформації від різних загроз, які можуть виникнути в процесі роботи системи. Розглянемо модель загроз для інформаційної системи підприємства з продажу побутової техніки.

– Перший етап – це ідентифікація загроз. Основними загрозами для інформаційної системи підприємства з продажу побутової техніки можуть бути:

– Несанкціонований доступ до системи: це може статися через використання неправильних паролів, шахрайства, підміни даних, атаки на мережу тощо.

– Віруси та інші види шкідливих програм: ці загрози можуть призвести до пошкодження або втрати даних, а також до втрати контролю над системою.

– Фізичні загрози: такі як пожежа, повінь, крадіжка або викрадення обладнання, можуть призвести до втрати даних або обладнання.

– Соціальна інженерія: це може включати спроби отримати доступ до системи через маніпулювання користувачами, що може призвести до витоку конфіденційної інформації.

Другий етап – оцінка загроз. В даному етапі визначається, наскільки серйозні загрози, що були ідентифіковані на попередньому етапі, можуть бути для інформаційної системи підприємства. Оцінка загроз зазвичай проводиться за допомогою методу ризик-аналізу, який дозволяє визначити ймовірність виникнення загрози та її вплив.

Третій етап – розробка стратегії управління загрозами. На основі оцінки загроз до інформаційної системи підприємства з продажу побутової техніки розробляється стратегія управління ризиками, що дозволяє зменшити можливість виникнення загроз та їх вплив на систему. Такі стратегії можуть включати в себе:

– Встановлення антивірусного програмного забезпечення, яке дозволяє захистити систему від шкідливих програм.

– Встановлення паролів та контроль доступу, що дозволяє забезпечити безпеку даних та запобігти несанкціонованому доступу до системи.

– Забезпечення фізичної безпеки обладнання, яке зберігає дані, наприклад, зберігаючи його в приміщенні з системою контролю доступу.

– Навчання користувачів про правила безпеки інформації, що дозволяє забезпечити свідомість користувачів про ризики, що пов'язані з роботою в системі.

Четвертий етап – впровадження стратегії. Розроблена стратегія управління загрозами в інформаційній системі підприємства з продажу побутової техніки виконується через впровадження заходів, які були розроблені в третьому етапі моделі. Впровадження може включати в себе інсталяцію програмного забезпечення, зміну конфігурації, проведення навчання та інші заходи.

П'ятий етап – моніторинг та оновлення стратегії. Після впровадження стратегії управління загрозами в інформаційну систему підприємства з продажу побутової техніки, потрібно постійно контролювати її дієвість та оновлювати за потребою. Моніторинг системи дозволяє вчасно виявляти нові загрози та проводити аналіз їх впливу на систему. При виявленні нових загроз або при зміні умов функціонування системи, стратегія управління загрозами повинна бути оновлена. Необхідно забезпечити постійне оновлення програмного забезпечення та апаратного забезпечення, забезпечити своєчасну підтримку, відповідати на запити користувачів і забезпечувати відповідну підтримку технічного персоналу.

Отже, модель загроз інформації ІКС підприємства з продажу побутової техніки – це система дій, спрямованих на виявлення загроз та зменшення їх впливу на інформаційну систему підприємства. Ця модель складається з п'яти етапів, які включають в себе аналіз загроз, визначення ризиків, розробку стратегії управління загрозами, впровадження стратегії, моніторинг та

оновлення стратегії. За допомогою цієї моделі можна забезпечити безпеку інформаційної системи підприємства з продажу побутової техніки та зменшити ризики несанкціонованого доступу до системи та витоку конфіденційної інформації.

Перелік загроз несанкціонованого доступу до модулів управління інформаційної системи підприємства з продажу побутової техніки може включати наступні елементи:

1. Перехоплення даних, включаючи конфіденційну інформацію, через використання несанкціонованих пристроїв або програмного забезпечення.

2. Використання слабкого пароля або недостатнього контролю доступу до модулів управління.

3. Злам системи безпеки ІТ, включаючи недостатні заходи забезпечення безпеки, такі як відсутність оновлень програмного забезпечення, слабкі паролі та недостатні заходи фізичної безпеки.

4. Фішингові атаки, що можуть призвести до втрати конфіденційної інформації.

5. Віруси та інші шкідливі програми, які можуть пошкодити або знищити дані на модулях управління.

6. Невірна настройка або конфігурація модулів управління, яка може призвести до порушення безпеки та доступу до даних.

7. Витік конфіденційної інформації через зловмисних або недбалих співробітників.

8. Неавторизоване використання програмного забезпечення, включаючи нелегальне копіювання або використання несанкціонованого ПЗ.

9. Атаки з використанням соціальної інженерії, таких як перехоплення даних з комп'ютерів, які заражені шкідливим ПЗ.

10. Атаки на службу аутентифікації та авторизації, які можуть призвести до незаконного доступу до конфіденційних даних в модулях управління.

11. Невірна конфігурація або застарілі настройки в інфраструктурі ІТ, які можуть дозволити зламувачам отримати доступ до системи.

12. Недостатня фізична безпека пристроїв, що містять конфіденційні дані, таких як сервери або резервні копії.

13. Компрометація системи з боку інших організацій або сторонніх партнерів, з якими підприємство здійснює взаємодію.

14. Атаки на веб-додатки, які можуть призвести до витоку конфіденційних даних, які зберігаються в інформаційній системі підприємства.

15. Атаки на різноманітні служби, які забезпечують роботу IT-інфраструктури, такі як DNS-сервери, DHCP-сервери, FTP-сервери та інші.

16. Відмова в обслуговуванні (DDoS) - це атака на сервери, яка полягає в перенавантаженні системи великою кількістю запитів, які заважають нормальній роботі серверів.

17. Витік конфіденційної інформації через інцидент з внутрішньою загрозою, наприклад, через недбалість або злочинні наміри співробітників підприємства.

18. Використання застарілих версій програмного забезпечення, які можуть містити вразливості, що можуть бути використані зловмисниками.

19. Використання слабких паролів, які можуть бути легко вгадані зловмисниками або скомпрометовані через недбалість користувачів.

Підприємство повинно бути готове до забезпечення захисту від цих загроз шляхом застосування заходів безпеки, таких як шифрування даних, регулярне оновлення програмного забезпечення, захист мережі від відмови в обслуговуванні, реалізація строго контролю доступу до системи та навчання персоналу з питань кібербезпеки.

Ось таблиця, яку можна використати для візуалізації загроз інформаційній системі підприємства з продажу побутової техніки:

Таблиця 2.1 – Аналіз загроз

Вид загрози	Модулі управління	Порушення	Ймовірність реалізації
Відмова в обслуговуванні	Всі модулі управління	Доступність	Середня до висока

Вид загрози	Модулі управління	Порушення	Ймовірність реалізації
(DDoS)			
Підробка даних	ERP-система, CRM-система, BI-система, Helpdesk система	Цілісність	Висока
Фішинг	Усі модулі управління	Конфіденційність	Висока
Злам паролів	Усі модулі управління	Конфіденційність	Середня
Віруси та інші віддалені загрози	Усі модулі управління	Цілісність, Доступність	Середня до висока
Невірний доступ	SCM-система, CMS система, Бухгалтерське ПЗ, TMS-система	Конфіденційність	Середня
Несанкціонований доступ	Усі модулі управління	Конфіденційність	Середня до висока
Атаки на служби	Всі модулі управління	Доступність	Середня до висока
Витік конфіденційної інформації	Усі модулі управління	Конфіденційність	Середня до висока
Використання застарілих версій програмного забезпечення	Усі модулі управління	Цілісність, Конфіденційність	Висока
Використання слабких паролів	Усі модулі управління	Конфіденційність	Середня

2.2 Модель порушника

Модель порушника (hacker model) – це опис потенційного злочинця, який може використовувати комп'ютерні засоби та різні техніки для здійснення злочинних дій в ІКС підприємства. Важливо розуміти, що така модель не передбачає жодної реальної особи, а складається з характеристик та прикладів

дійсної або можливої злочинної діяльності, яку можуть здійснювати зловмисники.

Модель порушника для ІКС підприємства може включати наступні складові:

1. Спеціалізація: зловмисник може мати певні спеціалізації, наприклад, в області комп'ютерної безпеки, соціальної інженерії, програмування, мережевих технологій і т.д.

2. Мотивація: зловмисники можуть мати різні мотивації для здійснення атак на ІКС підприємства, такі як фінансова вигода, намагання отримати конкурентну перевагу, розголос, політична мотивація тощо.

3. Методи атак: зловмисники можуть використовувати різні методи атак, включаючи соціальну інженерію, використання вразливостей в програмному забезпеченні, розповсюдження шкідливих програм, DDoS-атаки та інші.

4. Засоби: зловмисники можуть використовувати різні засоби, такі як комп'ютери, мобільні пристрої, програмне забезпечення, мережеві технології та інші для здійснення атак на ІКС підприємства.

5. Рівень навичок: залежно від рівня навичок, зловмисники можуть використовувати складні атаки, такі як експлойти.

6. Спосіб доступу: зловмисники можуть намагатися отримати доступ до ІКС підприємства зовнішнім шляхом, наприклад, шляхом використання мережевих технологій, або внутрішнім шляхом, зловживаючи своїм дозволеним доступом до системи.

7. Місце здійснення атаки: залежно від місця здійснення атаки, зловмисники можуть мати доступ до різних рівнів системи, від базових рівнів до важливих модулів управління.

8. Рівень злому: залежно від рівня злому, зловмисники можуть отримати доступ до різних рівнів системи, від базових рівнів до важливих модулів управління.

9. Вплив на систему: зловмисники можуть намагатися знищити, викрасти або пошкодити важливі дані, включаючи конфіденційну інформацію,

персональні дані клієнтів, фінансові дані, список клієнтів, замовлень, договорів, контрактів і т.д.

10. Визначення цілей: зловмисники можуть мати різні цілі, включаючи доступ до конфіденційної інформації, викрадення коштів, завдання шкоди репутації підприємства, завдання шкоди конкурентам і т.д.

За такими характеристиками можна визначити потенційних загроз до ІКС підприємства та прийняти заходи з їх запобігання.

На основі моделі порушника можна скласти таку таблицю:

Таблиця 2.2 – Модель порушника

Зловмисник	**Спеціалізація**	**Мотивація**	**Рівень навичок**	**Спосіб доступу**	**Місце здійснення атаки**	**Модулі системи**
Іноземний шпигун	Інформаційна розвідка	Здобуття технологій та конфіденційної інформації	Високий	Віддалений доступ	Зовнішній доступ	ERP, SCM, CRM
Безпечність держави	Інформаційна розвідка	Перешкоджання технологічному прогресу конкурентів	Високий	Віддалений доступ	Зовнішній доступ	ERP, SCM, CRM
Конкурент	Шпигунство	Здобуття комерційної інформації та підрив репутації підприємства	Високий	Віддалений доступ	Зовнішній доступ	ERP, SCM, CRM
ІТ-спеціаліст, що покинув підприємство	Невдоволеність роботою	Самовідновлення або крадіжка конфіденційної інформації	Високий	Локальний доступ	Внутрішній доступ	ERP, SCM, CRM, TMS, CMS
Користувач ІКС	Цікавість	Випробування можливостей ІКС	Середній	Локальний доступ	Внутрішній доступ	CMS, BI
Хакер	Вандалізм	Нанесення шкоди системі	Високий	Віддалений доступ	Зовнішній доступ	ERP, CRM, CMS
Користувач ІКС з власних мотивів	Зловживання привілеїв	Доступ до чутливої інформації	Середній	Локальний доступ	Внутрішній доступ	Бухгалтерське ПЗ
Фізичний зловмисник	Крадіжка	Викрадення комп'ютерів або	Низький	Фізичний доступ	Внутрішній доступ	Всі модулі системи

		носіїв інформації				

2.3 Визначення критеріїв захищеності та надання рекомендацій щодо реалізації системи захисту ІКС підприємства

Профіль захищеності 3.КЦД.1 відповідно до документа НД ТЗІ 2.5-005-99 визначає вимоги до забезпечення безпеки в автоматизованих системах, що містять конфіденційну інформацію.

3.КЦД.1 = { КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

КД-2. Базова довірча конфіденційність;

КО-1. Повторне використання об'єктів;

КВ-1. Мінімальна конфіденційність при обміні;

ЦД-1. Мінімальна довірча цілісність;

ЦО-1. Обмежений відкат;

ЦВ-1: Мінімальна цілісність при обміні;

ДР-1. Квоти;

ДВ-1. Ручне відновлення;

НР-2. Захищений журнал;

НИ-2. Одиночна ідентифікація і автентифікація;

НК-1. Однонаправлений достовірний канал;

НО-2. Розподіл обов'язків адміністраторів;

НЦ-2. КЗЗ з гарантованою цілісністю;

НТ-2. Самотестування при старті;

НВ-1: Автентифікація вузла.

Ці функціональні критерії захищеності визначають вимоги до автоматизованих систем класу 3, що містять конфіденційну інформацію, та дозволяють забезпечити високий рівень захищеності інформації в цих системах.

Система захисту має відповідати наступним вимогам:

- Захист від несанкціонованого доступу;
- Захист від вторгнень;

- Захист від витоку інформації;
- Захист від вірусів та шкідливих програм;
- Захист фізичної інфраструктури;
- Забезпечення цілісності та конфіденційності даних;
- Захист мережі;
- Забезпечення доступності;
- Захист від соціального інжинірингу.

2.3.1 Захист від несанкціонованого доступу

Захист від несанкціонованого доступу: система повинна мати механізми захисту від несанкціонованого доступу до ресурсів, що включають автентифікацію та авторизацію користувачів.

Рекомендації, щодо реалізації вимог пункту:

Для забезпечення захисту від несанкціонованого доступу можна використовувати різні програмні засоби, такі як системи управління доступом, механізми автентифікації та авторизації, файрволи тощо. Один з найбільш поширених програмних засобів для автентифікації та авторизації користувачів є Active Directory від Microsoft.

Для налаштування Active Directory необхідно встановити й налаштувати сервер домену, додати користувачів та групи, налаштувати політики безпеки та доступу до ресурсів. Для забезпечення високого рівня захищеності рекомендується використовувати складні паролі, вимагати регулярну зміну паролів, використовувати механізми двофакторної автентифікації, обмежувати доступ до ресурсів залежно від прав користувачів та груп. Також варто регулярно аудитувати доступ до ресурсів та вчасно виявляти та ліквідовувати можливі порушення безпеки.

При налаштуванні Active Directory необхідно враховувати конкретні потреби та вимоги підприємства з продажу побутової техніки та дотримуватись рекомендацій та стандартів безпеки інформації. Також важливо забезпечити резервне копіювання та відновлення Active Directory у разі необхідності.

2.3.2 Захист від вторгнень

Захист від вторгнень: система повинна мати механізми захисту від вторгнень, що включають виявлення та запобігання вторгнень, а також реагування на інциденти.

Рекомендації, щодо реалізації вимог пункту:

Щодо програмного забезпечення IDS/IPS, можна рекомендувати такі відомі рішення, як Snort, Suricata, Cisco IDS/IPS, PaloAlto IDS/IPS, Symantec IDS/IPS.

Налаштування IDS/IPS:

– встановіть та налаштуйте IDS/IPS на всіх комп'ютерах та серверах в мережі.

– налаштуйте IDS/IPS на збір трафіку, що проходить через мережу та на аналіз його на наявність шкідливих програм та інших загроз.

– встановіть правила блокування на IDS/IPS та налаштуйте їх на автоматичне виконання.

– налаштуйте IDS/IPS на сповіщення про виявлені загрози та на дії, які повинні бути виконані в разі виявлення атаки.

– періодично оновлюйте базу даних IDS/IPS та перевіряйте налаштування на наявність помилок та можливих проблем.

2.3.3 Захист від витоку інформації

Захист від витоку інформації: система повинна мати механізми захисту від витоку інформації, що включають криптографічний захист, засоби захисту від перехоплювання пакетів даних, контроль доступу та інші заходи.

Рекомендації, щодо реалізації вимог пункту:

– використовуйте криптографічний захист для захисту конфіденційної інформації. виберіть надійні алгоритми шифрування та ключі, а також встановіть правильні параметри захисту.

– встановіть засоби захисту від перехоплювання пакетів даних, наприклад, фільтри пакетів, інтегровані засоби захисту та мережеві екрани. це дозволить виявляти та блокувати спроби перехопити дані.

– встановіть правильні налаштування контролю доступу, які обмежують доступ до конфіденційної інформації лише авторизованим користувачам.

– використовуйте засоби моніторингу трафіку, які дозволяють виявляти та реагувати на атаки на мережу та систему.

– навчайте користувачів зберігати конфіденційну інформацію у безпечному місці, не надсилати її по електронній пошті та не ділитися паролями з невідомими особами.

Щодо програмного забезпечення, можна використовувати криптографічні засоби захисту, такі як PGP (Pretty Good Privacy), GPG (GNU Privacy Guard) або TrueCrypt/VeraCrypt для шифрування файлів і директорій. Також можна використовувати засоби моніторингу трафіку, наприклад, Snort, Bro або Suricata, які дозволяють виявляти та реагувати на атаки на мережу та систему.

2.3.4 Захист від вірусів та шкідливих програм

Захист від вірусів та шкідливих програм: система повинна мати механізми захисту від вірусів та шкідливих програм, що включають виявлення та вилучення шкідливих програм та вірусів.

Рекомендації, щодо реалізації вимог пункту:

Для захисту від вірусів та шкідливих програм рекомендується використовувати антивірусне програмне забезпечення, яке має наступні можливості:

– регулярне оновлення бази даних вірусів та шкідливих програм.

– автоматичне сканування системи на наявність вірусів та шкідливих програм.

– виявлення та блокування потенційно небезпечних файлів та програм.

– встановлення налаштувань захисту, які відповідають потребам організації.

– захист від атак на вразливості в операційній системі та програмах.

Додатково, рекомендується використовувати такі заходи захисту:

– регулярно оновлювати програмне забезпечення на комп'ютерах та серверах.

– використовувати файрвол для контролю доступу до мережі та Інтернету.

– визначити права доступу до файлів та папок згідно з принципом найменших привілеїв.

– навчати співробітників про заходи захисту та попереджати про потенційні небезпеки в Інтернеті.

– робити резервні копії даних та зберігати їх у безпечному місці.

2.3.5 Захист фізичної інфраструктури

Захист фізичної інфраструктури: система повинна мати механізми захисту фізичної інфраструктури, що включають фізичну захисну інфраструктуру, контроль доступу та інші заходи.

Рекомендації, щодо реалізації вимог пункту:

Для захисту фізичної інфраструктури інформаційної системи підприємства можна рекомендувати такі заходи:

– забезпечити фізичну безпеку приміщення, де розміщено обладнання системи. Застосувати такі заходи, як встановлення системи відеоспостереження, встановлення системи контролю доступу, блокування доступу до приміщення поза робочими годинами.

– застосувати заходи контролю доступу до серверів і обладнання системи. Встановити паролі на доступ до серверів, використовувати мережеві комутатори з можливістю контролю доступу, заборонити підключення зовнішніх пристроїв без дозволу адміністратора.

– регулярно проводити аудит безпеки фізичної інфраструктури та оцінювати ризики безпеки. Проводити регулярну перевірку системи

відеоспостереження та контролю доступу, а також перевірку роботи системи аварійного відключення обладнання.

2.3.6 Забезпечення цілісності та конфіденційності даних

Забезпечення цілісності та конфіденційності даних: система повинна забезпечувати цілісність та конфіденційність даних шляхом застосування криптографічних засобів, механізмів контролю цілісності та перевірки цифрових підписів, а також використання доступу до даних на основі ролей та обмеженням прав доступу користувачів.

Рекомендації, щодо реалізації вимог пункту:

Основні рекомендації для забезпечення цілісності та конфіденційності даних:

– використовуйте криптографічні алгоритми для захисту даних від несанкціонованого доступу, вибирайте алгоритми з надійними ключами та правильними параметрами захисту.

– застосовуйте механізми контролю цілісності даних, такі як цифрові підписи та хеш-функції.

– використовуйте систему контролю доступу на основі ролей та обмеженням прав доступу користувачів, що зменшує ризик несанкціонованого доступу до конфіденційних даних.

– захищайте систему від шкідливих програм та вірусів, забезпечуючи щоденне оновлення антивірусного програмного забезпечення та контрольовану ізоляцію файлів від невідомих джерел.

– використовуйте механізми резервного копіювання та відновлення даних для забезпечення їх відновлення у разі втрати або пошкодження.

2.3.7 Захист мережі

Захист мережі: система повинна мати механізми захисту мережі, що включають контроль доступу до мережі, захист від DoS-атак, контроль доступу до мережевих ресурсів та інші заходи.

Рекомендації, щодо реалізації вимог пункту:

– встановити мережеві брандмауери для контролю доступу до мережі та виявлення та блокування шкідливих пакетів даних.

– використовувати VPN для безпечного доступу до мережевих ресурсів зовнішніх користувачів.

– використовувати IDS/IPS для виявлення та блокування DoS-атак та інших мережевих загроз.

– використовувати механізми контролю доступу до мережевих ресурсів, такі як ACLs та RBAC.

– використовувати мережеві протоколи з криптографічним захистом, такі як SSL/TLS для захисту мережевої комунікації.

2.3.8 Забезпечення доступності

Забезпечення доступності: система повинна забезпечувати доступність своїх ресурсів, що включають резервування системних компонентів, кластеризацію та інші заходи.

Рекомендації, щодо реалізації вимог пункту:

– резервування системних компонентів: рекомендується налаштувати резервування жорстких дисків, пам'яті, мережевих контролерів та інших критичних системних компонентів.

– кластеризація: рекомендується використовувати кластеризацію для забезпечення доступності системи в разі відмови одного з компонентів. Кластеризація може бути реалізована як за допомогою програмного забезпечення, так і за допомогою апаратних засобів.

– моніторинг системи: рекомендується використовувати програмні засоби для моніторингу системи та виявлення проблем з доступністю ресурсів.

– резервне копіювання даних: рекомендується регулярно виконувати резервне копіювання даних для запобігання їх втраті в разі відмови системи.

2.3.9 Захист від соціального інжинірингу

Захист від соціального інжинірингу: система повинна мати механізми захисту від соціального інжинірингу, що включають навчання персоналу та використання механізмів контролю доступу.

Рекомендації, щодо реалізації вимог пункту:

– навчання персоналу: Навчайте свій персонал виявляти та запобігати соціальному інжинірингу. Організуйте регулярні тренінги та інформаційні кампанії з питань кібербезпеки, де надаватимете корисні поради та вказівки щодо запобігання соціальному інжинірингу.

– використання механізмів контролю доступу: Застосовуйте механізми контролю доступу, такі як двофакторна аутентифікація, щоб зменшити ризик несанкціонованого доступу до систем та даних.

– контроль доступу до інформації: Обмежуйте доступ до конфіденційної інформації лише тим працівникам, які мають необхідний рівень допуску. Застосовуйте принцип найменших привілеїв та регулярно перевіряйте права доступу до інформації.

– використання захисту від фішингу: Встановіть захист від фішингу на всіх пристроях, що використовуються в організації. Це може бути програмне забезпечення з захистом від шкідливих програм та електронних листів, яке фільтрує небезпечний контент та блокує спроби фішингу.

– створення політики безпеки: Розробіть та впровадьте політику безпеки, яка включає правила поведінки та процедури для персоналу в разі виявлення спроб соціального інжинірингу. Оновлюйте політику регулярно, щоб вона відповідала найсучаснішим загрозам.

2.4 Політика безпеки захисту від несанкціонованого доступу ІКС підприємства з продажу побутової техніки

1. Вступ

Ця політика безпеки захисту від несанкціонованого доступу до ІКС підприємства з продажу побутової техніки має на меті забезпечення

конфіденційності, цілісності та доступності інформаційних ресурсів підприємства, а також захисту від зловживання, зламу або втрати інформації. Ця політика визначає вимоги, процедури та рекомендації щодо захисту від несанкціонованого доступу до системи, включаючи заходи з фізичної та мережевої безпеки, ідентифікації користувачів, рольового управління доступом, контролю доступу та процедур дії в разі виникнення інцидентів з безпекою. Ця політика повинна бути дотримана всіма працівниками підприємства, а також третіми сторонами, що мають доступ до системи.

2. Загальні положення

2.1. Мета політики безпеки захисту від несанкціонованого доступу полягає у забезпеченні безпеки інформації в ІКС підприємства з продажу побутової техніки шляхом запобігання несанкціонованого доступу до ресурсів та забезпечення конфіденційності, цілісності та доступності даних. Політика безпеки захисту від несанкціонованого доступу є ключовим документом у системі управління інформаційною безпекою підприємства та визначає загальний підхід до захисту інформації. Всі користувачі, які мають доступ до ІКС, повинні дотримуватись цієї політики, щоб забезпечити безпеку та захист інформації в системі.

2.2. Забезпечення надійного та безперебійного функціонування ІКС підприємства з продажу побутової техніки, забезпечення конфіденційності, цілісності та доступності інформації в системі.

2.3. Мінімізація ризику несанкціонованого доступу до ресурсів ІКС підприємства з продажу побутової техніки.

2.4. Захист інформації від витоку та втрати, а також забезпечення можливості відновлення інформації в разі непередбачених ситуацій.

2.5. Виконання вимог законодавства та стандартів у галузі інформаційної безпеки.

3. Організаційна структура управління безпекою

3.1. Організаційна структура управління безпекою в ІКС підприємства з продажу побутової техніки повинна включати наступні посади та відповідальності:

3.1.1. Директор підприємства забезпечує загальне керівництво безпекою інформації та приймає рішення щодо призначення відповідальних осіб з питань безпеки.

3.1.2. Відповідальна особа з питань безпеки ІКС забезпечує розробку та впровадження політики безпеки, визначає методи і процедури контролювання безпеки, проводить навчання та свідомості користувачів щодо питань безпеки.

3.1.3. Адміністратор системи забезпечує належну роботу комп'ютерної системи та мережі, встановлює та контролює правила доступу, а також забезпечує контроль рівня доступу користувачів.

3.1.4. Користувачі ІКС повинні знати про політику безпеки, дотримуватися правил, встановлених адміністратором системи, та повідомляти про будь-які виявлені загрози безпеки.

3.1.5. Спеціаліст з безпеки даних відповідає за забезпечення безпеки даних в ІКС підприємства з продажу побутової техніки, включаючи захист від несанкціонованого доступу, захист від зміни даних та відновлення даних після аварій.

3.1.6. Комісія з безпеки даних відповідає за розгляд і вирішення питань, що стосуються безпеки даних в ІКС підприємства з продажу побутової техніки, включаючи розгляд і аналіз виявлених загроз, розробку стратегії безпеки та прийняття рішень.

4. Відповідальність за безпеку

4.1 Відповідальність за безпеку ІКС підприємства з продажу побутової техніки повинна бути розподілена між різними посадовими особами та відповідними підрозділами. Кожен з них повинен бути відповідальним за дотримання відповідних процедур та захисних заходів. Зокрема, до відповідальності за безпеку відносяться наступні аспекти:

Директор підприємства забезпечує виконання політики безпеки та приймає рішення щодо придбання і використання захисних засобів та технологій.

Керівник відділу ІТ (заступник директора) забезпечує безпеку інформації, що зберігається в комп'ютерних системах та мережах, та відповідає за безпеку доступу до цієї інформації.

Спеціаліст з безпеки мереж (системний адміністратор) забезпечує безпеку мережевих засобів та технологій, що використовуються в ІКС підприємства.

Спеціаліст з фізичної безпеки (охоронець) забезпечує безпеку фізичного доступу до комп'ютерних систем та інших ресурсів ІКС.

Кожен користувач системи зобов'язаний дотримуватись правил безпеки, встановлених в компанії, та вчасно повідомляти про будь-які підозрілі дії, які можуть загрожувати безпеці комп'ютерних систем або інформації.

5. Процедури захисту від несанкціонованого доступу

5.1. Визначення загроз та ризиків безпеки інформації

5.1.1. Аналіз потенційних загроз безпеці інформації, які можуть бути здійснені ззовні та всередині ІКС підприємства з продажу побутової техніки.

5.1.2. Оцінка потенційного впливу цих загроз на безпеку інформації, включаючи визначення імовірності та наслідків реалізації загроз.

5.1.3. Визначення рівня ризику безпеки інформації відповідно до результатів оцінки загроз та їх впливу.

5.1.4. Визначення пріоритетних напрямків заходів з попередження та зменшення ризику безпеки інформації.

5.2. Встановлення правил користування ІКС підприємства та інструкцій з доступу до ресурсів.

5.2.1. Всі користувачі ІКС підприємства повинні бути ознайомлені з політикою безпеки та правилами користування системою.

5.2.2. Користувачам повинні бути надані інструкції з доступу до ресурсів ІКС підприємства, включаючи рівень доступу, права користувача та відповідальність за порушення політики безпеки.

5.2.3. Усім користувачам ІКС підприємства повинні бути надані унікальні ідентифікатори та паролі для доступу до системи.

5.2.4. Паролі повинні бути складними та не повинні бути збережені на пристроях або у відкритому вигляді на документах.

5.2.5. Політика безпеки повинна включати процедуру зміни паролів, яка повинна вимагати від користувачів зміни паролів на регулярній основі, а також після будь-якого підозрілого використання пароля.

5.2.6. Права користувача повинні бути встановлені відповідно до їхніх обов'язків та відповідальності.

5.2.7. Усім користувачам ІКС підприємства повинна бути забезпечена доступність та зрозумілість інструкцій щодо безпеки та доступу до ресурсів системи.

5.2.8. Права доступу користувачів повинні бути оновлювані відповідно до змін у їхніх обов'язках та відповідальності, а також при звільненні або переведенні на іншу посаду.

5.2.9. У разі виявлення порушень правил користування ІКС підприємства та політики безпеки, користувачі несуть особисту відповідальність.

5.3. Політики щодо паролів, управління доступом та аудиту доступу

5.3.1. Всі користувачі мають бути привернені до уваги до важливості зберігання паролів і забезпечення конфіденційності доступу до інформаційних ресурсів.

5.3.2. Всі користувачі мають мати унікальні ідентифікаційні дані, які забезпечують конфіденційність доступу до ресурсів ІКС підприємства з продажу побутової техніки.

5.3.3. Кожен користувач має мати унікальний пароль, який повинен бути складним і складатися з комбінації букв, цифр та символів.

5.3.4. Користувачам повинно заборонятися використовувати паролі, що повторюються, а також легко вгадувані паролі, наприклад, дати народження, імена членів родини тощо.

5.3.5. Паролі мають бути змінювані щонайменше раз на три місяці або після кожного випадку порушення безпеки.

5.3.6. Досягнення рівня доступу до ресурсів ІКС підприємства з продажу побутової техніки повинно бути обмеженим і контрольованим з метою запобігання несанкціонованого доступу.

5.3.7. Управління доступом повинно включати регулярне оновлення списків користувачів та їх рівнів доступу.

5.3.8. При роботі з ІКС підприємства з продажу побутової техніки повинен бути забезпечений аудит доступу, що дозволяє виявляти спроби несанкціонованого доступу та неправомірної діяльності.

5.3.9. Аудит доступу повинен включати контроль доступу до файлів, баз даних, системного ПЗ та мережевих ресурсів.

5.4. Управління аккаунтами користувачів

5.4.1. Кожен користувач ІКС повинен мати окремий обліковий запис з ідентифікатором та паролем.

5.4.2. Аккаунти користувачів повинні бути створені на підставі заявок відповідальних осіб та документів, що підтверджують їхню працевлаштування.

5.4.3. Кожен користувач повинен мати встановлені права доступу відповідно до своїх обов'язків та потреб в роботі.

5.4.4. При прийнятті на роботу нового співробітника, його аккаунт повинен бути створений до початку роботи та відключений у разі звільнення з роботи або зміни посади.

5.4.5. Паролі користувачів повинні бути достатньо складними та змінюватись не рідше одного разу на кожні 90 днів.

5.4.6. Адміністратор повинен мати доступ до управління аккаунтами користувачів та вести журнал змін аккаунтів.

5.4.7. Користувачі повинні бути повідомлені про правила використання аккаунтів та несуть відповідальність за їхнє надійне збереження та використання.

5.5. Захист системи від шкідливих програм та вірусів

5.5.1. Придбання та встановлення оновлень антивірусного програмного забезпечення на всіх комп'ютерах в мережі.

5.5.2. Забезпечення частого оновлення баз даних антивірусного програмного забезпечення.

5.5.3. Проведення сканування всіх файлів, які завантажуються на комп'ютери в мережі, на наявність шкідливих програм та вірусів.

5.5.4. Забезпечення копіювання важливих даних на зовнішні носії для збереження цілісності та доступності даних у разі атаки шкідливої програми або віруса.

5.5.5. Заборона завантаження файлів з невідомих джерел та від ненадійних джерел.

5.5.6. Забезпечення проведення регулярних навчань для співробітників щодо захисту від шкідливих програм та вірусів, в тому числі щодо усвідомлення ризиків відкривання невідомих файлів та посилань в електронних листах.

5.6. Процедури випадкових аудитів доступу

5.6.1. Ціль процедури

Ціль процедури випадкових аудитів доступу полягає у перевірці правильності застосування процедур автентифікації та авторизації користувачів, виявленні можливих порушень та встановленні їх причин.

5.6.2. Відповідальність за процедуру

Відповідальність за проведення випадкових аудитів доступу несе відділ з безпеки інформації.

5.6.3. Частота проведення

Випадкові аудити доступу повинні проводитись не рідше одного разу на квартал.

5.6.4. Обсяг проведення

Обсяг проведення випадкових аудитів доступу повинен охоплювати не менше 10% користувачів, які мають доступ до критичних ресурсів.

5.6.5. Порядок проведення

Процедура випадкових аудитів доступу включає в себе наступні етапи:

- вибір користувачів, які підлягають аудиту.
- перевірка правильності процедури автентифікації та авторизації.
- виявлення можливих порушень та встановлення їх причин.
- розробка рекомендацій щодо покращення процедур автентифікації та авторизації.
- формування звіту про результати аудиту.

5.6.6. Контроль за виконанням

Відділ з безпеки інформації повинен забезпечувати контроль за виконанням процедури випадкових аудитів доступу та реалізацією рекомендацій щодо покращення процедур автентифікації та авторизації.

5.7. Процедури відключення доступу для звільнених або змінивших підрозділ

Для забезпечення безпеки ІКС підприємства з продажу побутової техніки, кожен відділ повинен мати механізми, які дозволяють швидко та ефективно відключати доступ користувачам, що покинули підрозділ або були переміщені на іншу посаду.

5.7.1. Процедури відключення доступу повинні включати такі етапи:

5.7.1.1. Повідомлення про відключення доступу до всіх відповідних додатків та ресурсів, включаючи електронну пошту, файли та бази даних.

5.7.1.2. Забезпечення збереження важливих даних або документів, які можуть бути потрібні після відключення доступу.

5.7.1.3. Вилучення дозволів на доступ та видалення ідентифікаційних даних користувача з усіх систем.

5.7.1.4. Перевірка наявності будь-яких пристроїв, що можуть бути володінням звільненого користувача, таких як комп'ютери, мобільні телефони тощо, і їх вилучення.

Крім того, процедури повинні бути узгоджені зі спеціалістами з безпеки та з підрозділом управління персоналом, щоб забезпечити їх ефективність та відповідність діючим правилам та законодавству.

5.8. Заходи у разі порушення безпеки

5.8.1. При виявленні порушення безпеки користувач повинен негайно повідомити про це відповідальну особу з питань безпеки інформації або системного адміністратора.

5.8.2. При порушенні безпеки, пов'язаному з втратою, крадіжкою або пошкодженням обладнання, користувач повинен повідомити про це відповідальну особу з питань безпеки інформації і правоохоронні органи.

5.8.3. При порушенні безпеки, пов'язаному з незаконним доступом до системи, користувач повинен негайно змінити свій пароль та повідомити про це відповідальну особу з питань безпеки інформації або системного адміністратора.

5.8.4. При порушенні безпеки, пов'язаному з пошкодженням, втратою або розголошенням конфіденційної інформації, користувач повинен негайно повідомити про це відповідальну особу з питань безпеки інформації і провести відповідні заходи з її відновлення та захисту.

5.8.5. В разі виявлення порушень безпеки, відповідальна особа з питань безпеки інформації повинна негайно прийняти заходи з їх усунення та запобігання подібних інцидентів у майбутньому.

5.8.6. В разі виявлення серйозних порушень безпеки, які загрожують нормальному функціонуванню ІКС, необхідно повідомити про це вищестоящий орган або органи державного управління, а також правоохоронні органи.

5.9. Організаційні заходи для забезпечення безпеки фізичного доступу до приміщення інформаційної системи

5.9.1. Доступ до приміщення, що містить інформаційну систему, має бути обмеженим та контрольованим.

5.9.2. Для забезпечення безпеки фізичного доступу до приміщення, що містить інформаційну систему, необхідно використовувати принаймні один із наступних заходів:

- електронний доступ;
- фізичний ключ або картка з доступом на замку;

– біометричний доступ.

5.9.3. Для забезпечення безпеки фізичного доступу до приміщення, що містить інформаційну систему, необхідно використовувати систему відеоспостереження та реєстрації вхідних та вихідних дій.

5.9.4. Для забезпечення безпеки фізичного доступу до приміщення, що містить інформаційну систему, необхідно забезпечити контроль доступу до серверної кімнати та інших приміщень з обладнанням.

5.9.5. Передбачити механізми автоматичного зберігання резервних копій інформаційних ресурсів інформаційної системи в інших приміщеннях, забезпечення захисту резервних копій від несанкціонованого доступу.

5.10. Організаційні та технічні заходи щодо захисту мережі інформаційної системи та обмеження доступу до неї.

5.10.1. Забезпечити використання захищеного зв'язку при передачі даних.

5.10.2. Встановити ефективні засоби захисту мережі та забезпечення безпеки передачі даних (наприклад, захищений тунельний протокол, VPN, SSL, TLS тощо).

5.10.3. Обмежити фізичний доступ до приміщень, де знаходиться обладнання інформаційної системи.

5.10.4. Забезпечити відповідну фізичну захищеність серверних приміщень, де знаходиться обладнання інформаційної системи, включаючи системи контролю доступу та відеоспостереження.

5.10.5. Забезпечити безпеку мережі шляхом використання ефективних засобів захисту мережі, таких як персональні брандмауери, IDS/IPS, антивірусне програмне забезпечення, системи виявлення вторгнень та інші.

5.10.6. Забезпечити використання ефективних методів аутентифікації та авторизації користувачів, зокрема, використання складних паролів, двофакторної аутентифікації, ідентифікації по IP-адресі, рівням доступу та інші.

5.10.7. Забезпечити захист від відомих вразливостей в програмному забезпеченні, оновлювати програмне забезпечення інформаційної системи вчасно та регулярно.

5.10.8. Забезпечити регулярне виконання резервного копіювання інформації та тестування процедур відновлення.

6. Ідентифікація користувачів та рольове управління доступом

6.1. Процедури ідентифікації користувачів

6.1.1. Усі користувачі, які мають доступ до ІКС підприємства з продажу побутової техніки, повинні бути ідентифіковані за допомогою унікальних облікових записів та паролів.

6.1.2. Комплексні паролі повинні мати достатню складність, включати мінімум вісім символів та містити різні типи символів, такі як великі та малі літери, цифри та спеціальні символи.

6.1.3. Користувачі повинні забезпечувати конфіденційність своїх облікових даних та не передавати їх іншим особам.

6.1.4. Періодичність зміни паролів повинна бути визначена відповідно до ризиків і встановлених правил безпеки.

6.2. Управління доступом

6.2.1. Керування доступом до ресурсів системи повинно здійснюватись на основі політики рольового доступу.

6.2.2. Кожен користувач системи має бути ідентифікований унікальним ідентифікатором та мати обмежений доступ до ресурсів системи відповідно до своїх обов'язків та потреб.

6.2.3. Доступ користувачів до конфіденційної інформації та ресурсів, що містять важливу інформацію, має бути здійснений тільки за наявності обґрунтованої потреби та після отримання відповідних дозволів.

6.2.4. Для кожного користувача має бути визначено його роль в системі та набір прав доступу, які відповідають його обов'язкам та функціональній ролі в організації.

6.2.5. Управління ролями та правами доступу до ресурсів системи повинно здійснюватись централізовано з метою забезпечення контролю доступу до різних ресурсів та зменшення ризиків несанкціонованого доступу до них.

6.2.6. Права доступу до ресурсів системи повинні бути визначені на основі необхідності доступу користувача до відповідних ресурсів для виконання його обов'язків, а також на основі принципу найменшого привілеювання, що дозволяє обмежити доступ користувача лише до необхідного мінімуму ресурсів.

6.2.7. Доступ до ресурсів системи повинен бути забезпечений за допомогою механізмів автентифікації та авторизації користувачів, які мають обмежену відповідність до ролі та набору прав доступу, визначеного для кожного користувача.

6.3. Управління рольовою моделлю

6.3.1. Опис

Управління рольовою моделлю полягає в забезпеченні доступу користувачів до ресурсів системи на основі їхньої ролі в організації та принципу найменшого доступу. Це дозволяє зменшити можливість несанкціонованого доступу до ресурсів та збільшити ефективність управління доступом.

6.3.2. Вимоги

6.3.2.1. Управління рольовою моделлю повинно забезпечувати можливість створення, редагування та видалення ролей, а також призначення користувачів до ролей.

6.3.2.2. Призначення ролей повинно здійснюватися на основі принципу найменшого доступу, тобто користувачеві повинні призначатися лише ті ролі, які необхідні для виконання його робочих обов'язків.

6.3.2.3. Управління рольовою моделлю повинно забезпечувати можливість налаштування прав доступу до конкретних ресурсів для кожної ролі, в тому числі прав на перегляд, редагування та видалення даних.

6.3.2.4. При зміні ролі користувача, управління рольовою моделлю повинно автоматично переназначати права доступу відповідно до нової ролі.

6.3.2.5. Управління рольовою моделлю повинно забезпечувати моніторинг доступу користувачів до ресурсів системи на основі їхньої ролі, а також забезпечувати можливість аудиту прав доступу користувачів.

6.3.2.6. Управління рольовою моделлю повинно забезпечувати можливість налаштування терміну дії ролі та автоматичне її відключення після закінчення терміну.

6.4. Захист інформації про користувачів

6.4.1. Інформація про користувачів повинна бути захищена від несанкціонованого доступу, модифікації та видалення.

6.4.2. Користувацькі дані повинні зберігатися в захищеному від інтернет-загроз місці, що має обмежений доступ для некваліфікованих осіб.

6.4.3. Доступ до інформації про користувачів має бути обмежений та контрольований.

6.4.4. Користувацькі дані повинні зберігатися в захищеному від крадіжки місці з обов'язковим шифруванням даних.

6.4.5. Доступ до інформації про користувачів має бути надано лише у разі необхідності та з урахуванням принципу необхідного обсягу доступу.

6.4.6. При видаленні акаунту користувача, його дані повинні бути повністю видалені з системи та забезпечена недоступність цих даних для інших користувачів системи.

6.4.7. Під час передачі користувацьких даних, необхідно забезпечувати їх захищеність від несанкціонованого доступу, використовуючи шифрування та інші заходи захисту.

6.5.1. Визначення прав доступу

6.5.1.1. Кожен користувач повинен мати окремий обліковий запис, який містить інформацію про його права доступу.

6.5.1.2. Права доступу до різних ресурсів системи повинні бути визначені з урахуванням ролі користувача і не повинні допускати несанкціонований доступ до інформації.

6.5.1.3. Рольове управління доступом повинно бути реалізовано з використанням ролей, які повинні бути пов'язані з конкретними задачами та відповідальностями користувача.

6.5.2. Аутентифікація

6.5.2.1. Для аутентифікації користувача повинен використовуватися ідентифікатор та пароль.

6.5.2.2. Користувачі повинні використовувати складні паролі, які містять букви, цифри та символи, та регулярно змінювати їх.

6.5.2.3. Для підвищення безпеки можна використовувати двофакторну аутентифікацію.

6.5.3. Аудит доступу

6.5.3.1. Повинен бути забезпечений аудит доступу до системи та її ресурсів.

6.5.3.2. Інформація про доступ до ресурсів повинна бути збережена в логах, що дозволяє встановлювати факти несанкціонованого доступу та інших порушень.

6.5.3.3. Логи повинні зберігатися на протязі певного періоду часу, залежно від вимог законодавства.

6.5.4. Керування сесією

6.5.4.1. Повинен бути забезпечений контроль сесії користувача для запобігання несанкціонованого доступу до системи під час відсутності користувача за робочим місцем.

6.5.4.2. Механізми автоматичного відключення користувача

Механізми автоматичного відключення користувача в системі повинні бути налаштовані для забезпечення безпеки і захисту від несанкціонованого доступу. Такі механізми повинні активуватися при виявленні підозрілих дій, спроб несанкціонованого доступу або порушень правил використання системи.

6.5.5. Моніторинг доступу та ідентифікація небезпечних дій

6.5.5.1. Моніторинг доступу

6.5.5.1.1. Система повинна мати засоби моніторингу доступу, що дозволяють стежити за діяльністю користувачів в системі.

6.5.5.1.2. Засоби моніторингу повинні збирати та зберігати інформацію про:

- ідентифікацію користувачів, які входять до системи;
- ролі користувачів в системі;
- ресурси, які використовуються користувачами;
- час та тривалість сеансів користувачів;
- об'єм даних, які передаються користувачами;
- випадки невдалих спроб входу до системи;
- випадки спроб доступу до ресурсів, на які користувач не має прав доступу.

6.5.5.2. Ідентифікація небезпечних дій

6.5.5.2.1. Система повинна мати засоби ідентифікації небезпечних дій, що дозволяють вчасно виявляти та запобігати атакам на інформаційну систему.

6.5.5.2.2. Засоби ідентифікації небезпечних дій повинні забезпечувати виявлення:

- спроб входу до системи з неправильними обліковими даними;
- спроб доступу до ресурсів, на які користувач не має прав доступу;
- спроби зміни конфіденційної інформації;
- спроби виконання небезпечних команд або програм;
- спроби виконання інших дій, що загрожують безпеці системи.

6.5.5.2.3. Засоби ідентифікації небезпечних дій повинні мати механізми автоматичної реакції на виявлені загрози, що дозволяють негайно вжити заходів для запобігання або обмеження шкоди внаслідок атаки.

7. Автоматизовані засоби контролю доступу

7.1. Для контролю доступу до ресурсів інформаційної системи підприємства з продажу побутової техніки використовуються автоматизовані засоби, що дозволяють забезпечити необхідний рівень безпеки.

7.2. Всі користувачі повинні пройти процедуру аутентифікації та авторизації з використанням сучасних криптографічних методів, що дозволяють забезпечити надійний захист від несанкціонованого доступу.

7.3. Для керування правами доступу використовується рольова модель, що забезпечує можливість забезпечити доступ до ресурсів тільки тим користувачам, які мають необхідні повноваження.

7.4. Для моніторингу активності користувачів та виявлення можливих загроз використовуються системи відслідковування подій (Event Log), що дозволяють в режимі реального часу контролювати дії користувачів та вчасно реагувати на можливі інциденти з безпекою.

7.5. При наявності можливості використовуються додаткові засоби контролю доступу, такі як біометричні системи, карткові системи доступу, системи відеоспостереження та інші, що дозволяють забезпечити найвищий рівень безпеки.

8. Мережева безпека

8.1. Контроль доступу до мережі зовнішніх користувачів: для забезпечення безпеки мережі зовнішніх користувачів, необхідно контролювати доступ до мережевих ресурсів та встановлювати обмеження для зовнішніх з'єднань.

8.2. Контроль доступу до мережі внутрішніх користувачів: контроль доступу до мережі внутрішніх користувачів передбачає обмеження доступу до мережевих ресурсів та розподіл прав доступу між користувачами відповідно до їхніх ролей в організації.

8.3. Захист від мережевих атак включає в себе використання захисних засобів, таких як брандмауери, IDS та IPS системи, та регулярне оновлення програмного забезпечення.

8.4. Конфігурація мережевих пристроїв та мережевих послуг передбачає налаштування мережевих пристроїв, включаючи маршрутизатори, комутатори та точки доступу до мережі, та забезпечення безпеки мережевих послуг.

8.5. Захист від комп'ютерних вірусів та інших шкідливих програм включає в себе встановлення антивірусного програмного забезпечення та регулярне оновлення баз даних вірусних сигнатур.

8.6. Контроль використання мережевого трафіку передбачає моніторинг та обмеження використання мережевих ресурсів, включаючи використання протоколів мережевої адресації та управління трафіком.

8.7. Резервне копіювання даних, збережених на серверах мережі, забезпечує збереження важливої інформації та можливість відновлення даних в разі їх втрати або пошкодження.

8.8. Захист від DDoS-атак: Розробка та використання механізмів захисту від DDoS-атак на рівні мережі, таких як IPS, IDS та Firewall.

8.9. Віддалене управління мережею: Забезпечення захищеного віддаленого доступу до мережі за допомогою VPN-з'єднань та інших механізмів шифрування.

9. Фізична безпека

9.1. Обмеження фізичного доступу до приміщень, де знаходяться серверні кімнати, мережеві елементи та інші пристрої інфраструктури.

9.2. Захист серверних кімнат від потенційно небезпечних факторів, таких як вогонь, вода, перенапруга, електромагнітні поля, вібрації тощо.

9.3. Контроль доступу до серверної кімнати, включаючи фізичний контроль входу, перевірку ідентифікації та авторизації користувачів, моніторинг за участю відеокамер, сканування біометричних даних тощо.

9.4. Захист обладнання від крадіжки та шахрайства, включаючи фізичні заходи захисту, які обмежують можливість винесення обладнання з приміщення, наприклад, кріплення до підлоги, корпусів з замками та інших заходів.

9.5. Контроль за фізичними носіями інформації, такими як диски, флешки, знімні жорсткі диски, CD та DVD диски, що відображається у відповідній політиці безпеки, яка визначає правила використання, зберігання та утилізації цих пристроїв.

9.6. Правильне зберігання запасних копій даних в безпечному місці захисту від пожежі, води та інших потенційно небезпечних факторів.

10. Заходи у разі виникнення інцидентів з безпекою

10.1. Класифікація інцидентів з безпекою: Установлюється система класифікації інцидентів з безпекою відповідно до рівня серйозності та впливу на функціонування системи.

10.2. Звітність та процедури повідомлення: Визначаються процедури повідомлення про інциденти з безпекою та встановлюється відповідальність за надання звітності щодо заходів, прийнятих для врегулювання інциденту.

10.3. Комунікація з користувачами та співробітниками щодо інцидентів з безпекою: Визначається процедура комунікації з користувачами та співробітниками щодо інцидентів з безпекою, у тому числі повідомлення про інциденти та надання рекомендацій щодо їх уникнення.

10.4. Аналіз інцидентів з безпекою та підвищення рівня захищеності системи: Визначається процедура аналізу інцидентів з безпекою та розробки заходів щодо підвищення рівня захищеності системи від подібних інцидентів у майбутньому.

10.5. Зберігання інформації про інциденти з безпекою – установлення процедур зберігання документації про інциденти з безпекою.

10.6. Відновлення роботи системи після інциденту з безпекою – визначення процедур відновлення роботи системи після виникнення інциденту з безпекою.

10.7. Процедури виконання резервного копіювання та відновлення даних – розроблення процедур зберігання резервних копій і відновлення даних після інцидентів з безпекою.

10.8. Розслідування та встановлення причин виникнення інцидентів з безпекою – визначення процедур розслідування інцидентів з безпекою та встановлення їх причин.

10.9. Коригування політики безпеки з урахуванням результатів аналізу інцидентів з безпекою – визначення процедур коригування політики безпеки з урахуванням результатів аналізу інцидентів з безпекою.

11. Оцінка ефективності політики безпеки

11.1. З метою визначення ефективності політики безпеки, підприємство проводить системний аналіз стану безпеки інформаційних ресурсів та інформаційних технологій на підприємстві.

11.2. Результати аналізу служать підставою для складання звіту з оцінки ефективності політики безпеки. Звіт повинен містити такі показники:

- кількість зареєстрованих випадків порушення безпеки;
- кількість зроблених помилок при введенні даних;
- кількість несанкціонованого доступу до інформаційних ресурсів;
- кількість виявлених інцидентів з вірусами та іншими загрозами;
- кількість виявлених помилок в роботі програмного забезпечення;
- кількість успішних атак на інформаційні ресурси підприємства.

11.3. Звіт з оцінки ефективності політики безпеки повинен бути представлений на затвердження вищому керівництву підприємства. При необхідності, на основі результатів звіту, можуть бути внесені зміни до політики безпеки.

12. Заключні положення

12.1. Дана політика безпеки є обов'язковою для всіх працівників підприємства з продажу побутової техніки та користувачів ІКС.

12.2. Зміни та доповнення до даної політики безпеки можуть бути внесені згідно з процедурою затвердження документів.

12.3. Політика безпеки повинна періодично переглядатись та оновлюватись з урахуванням нових загроз та ризиків.

12.4. Кожен працівник та користувач ІКС зобов'язаний дотримуватись встановлених процедур та заходів безпеки.

12.5. Порушення політики безпеки може бути підставою для застосування дисциплінарних заходів.

12.6. Дана політика безпеки є відкритою для перевірки та ознайомлення всіх працівників та користувачів ІКС підприємства з продажу побутової техніки.

2.5 Висновок

Застосування описаної моделі загроз та моделі порушника в дослідженні показало, що система ІКС підприємства з продажу побутової техніки піддається різним типам загроз з боку ворогів, що може призвести до компрометації конфіденційної інформації, втрати цілісності даних, а також перерв у роботі системи.

Для забезпечення захисту ІКС підприємства було визначено критерії захищеності та розроблено рекомендації щодо захисту від різних видів загроз, таких як несанкціонований доступ, вторгнення, виток інформації, віруси та шкідливі програми, фізичні загрози, захист мережі, доступність та соціальний інжиніринг.

Підсумовуючи, розробка політики безпеки та виконання визначених рекомендацій допоможуть у забезпеченні захищеності ІКС підприємства від можливих загроз та порушників, а також дозволять забезпечити високу конфіденційність, цілісність та доступність даних. Окрім цього, важливо забезпечувати навчання персоналу та постійний моніторинг стану безпеки системи, щоб захистити систему від нових загроз та вразливостей.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Постановка задачі

Метою економічного розділу є обґрунтування доцільності розробки політики безпеки інформаційно-комунікаційної системи підприємства з продажу побутової техніки.

Завданням був розрахунок капітальних та експлуатаційних витрат на розробку політики безпеки. А також визначення та аналіз показників економічної ефективності створеної політики.

3.2 Визначення капітальних витрат на створення політики безпеки

3.2.1 Визначення трудомісткості розробки та опрацювання ПБ

При проведенні нормування праці робітників, що займаються створенням політики безпеки, виникає проблема, пов'язана з тим, що ця праця є творчою.

Трудомісткість створення політики безпеки визначається тривалістю кожної робочої операції. При умові, що весь об'єм робіт буде виконано одним робітником, розраховується за формулою 3.1:

$$t = tmз + tв + tа + tпр + tопр, \text{ годин,} \qquad (3.1)$$

де $tmз$ – тривалість складання політики безпеки;

$tв$ – тривалість вивчення технічного завдання (ТЗ), літературних джерел за темою тощо;

$tа$ – тривалість розробки алгоритму створення політики безпеки;

$tпр$ – тривалість розробки політики безпеки інформаційно-комунікаційної системи підприємства з продажу побутової техніки;

$tопр$ – тривалість опрацювання.

Отже трудомісткість створеної ПБ складає:

$$t = 8 + 25 + 15 + 80 + 30 = 158, \text{ годин.}$$

3.2.2 Розрахунок витрат на створення політики безпеки

При підрахунку витрати на створення політики безпеки Км за формулою 3.2 треба знайти загальні витрати на оплату заробітної плати розробнику політики безпеки Ззп та вартість машинного часу, що необхідний для розробки та опрацювання політики безпеки на ПК Змч:

$$К_м = З_{зп} + З_{мч} . \quad (3.2)$$

Заробітна плата розробника політики безпеки враховує основну і додаткову заробітну плату, відрахування на соціальні потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою 3.3:

$$З_{зп} = t \cdot З_{пр}, \text{ грн,} \quad (3.3)$$

де t – загальна тривалість створення ПБ, годин;

Зпр – средньогодинна заробітна плата розробника з нарахуваннями, грн/годину.

Таким чином, заробітна плата розробника за весь період праці складатиме:

$$З_{зп} = 158 \cdot 90 = 14220, \text{ грн.}$$

До загальної суми потрібно включити вартість машинного часу для розробки політики безпеки на ПК, що визначається за формулою 3.4:

$$З_{мч} = t_{опр} \cdot С_{мч}, \text{ грн,} \quad (3.4)$$

де $t_{опр}$ – трудомісткість розробки політики безпеки на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою 3.5:

$$Смч = P \cdot Ce + \frac{Фзал \cdot Ha}{Fp} + \frac{Клпз \cdot Hапз}{Fp}, \text{ грн./година,} \qquad (3.5)$$

де Р – встановлена потужність ПК (0,6 кВт);

$С_е$ – тариф на електричну енергію (1,44 грн/кВт·година);

$Ф_{зал}$ – залишкова вартість ПК на поточний рік (15000 грн.);

$Н_а$ – річна норма амортизації на ПК, частки одиниці (0,3);

$К_{лпз}$ – вартість ліцензійного програмного забезпечення (ОС Microsoft Windows 11 – 5800 грн., Microsoft Office 365 – 8300 грн.);

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці (0,3);

$F_р$ – річний фонд робочого часу (2080 годин).

Отже, 1 година машинного часу ПК вартує:

$$С_{мч} = 0{,}6 \cdot 1{,}44 + \frac{15000 \cdot 0{,}3}{2080} + \frac{(5800+8300) \cdot 0{,}3}{2080} = 5.06 \text{ , грн./година.}$$

$$З_{мч} = 120 \cdot 5.06 = 607.20 \text{ , грн.}$$

$$К_м = 14220 + 607.20 = 14827{,}20 \text{ , грн.}$$

Таким чином, після всіх проведених розрахунків, загальні витрати на розробку політики безпеки, складають 14827,20 грн.

3.3 Розрахунок експлуатаційних витрат

До експлуатаційних витрат віднесено:

– річну заробітну плату співробітника, що проводить оцінку загроз інформаційній безпеці;

– відрахування на соціальні заходи від річної заробітної плати співробітника;

– витрати машинного часу.

3.3.1 Річна заробітна плата співробітника, що проводить оцінку загроз інформаційній безпеці

Годинна заробітна плата становить:

$$Зпрс = 135 \text{ грн./год.}$$

Для підрахунку заробітної плати працівника, що проводить оцінку загроз інформаційній безпеці, використовується формула 3.6:

$$Ззпс = t * Зпрс, \text{ грн.}, \quad (3.6)$$

де t – загальна тривалість роботи працівника за рік, годин.

Середня тривалість одного сеансу роботи щодо перевірки дотримання вимог політики безпеки становить 4 години, з періодичністю 2 раз на місяць. Тобто за рік $t = 12 * 4 * 2 = 96$ години.

Витрати на оплату заробітної плати за рік:

$$Ззпс = 96 * 135 = 12960, \text{ грн.}$$

3.3.2 Відрахування на соціальні заходи від річної заробітної плати співробітника, що проводить оцінку загроз інформаційній безпеці

Відрахування на соціальні заходи від річної заробітної плати співробітника, що проводить оцінку загроз інформаційній безпеці, розраховують за формулою 3.7:

$$Зєсв= 22\% * Ззпс \text{ , грн.} \quad (3.7)$$

Що, з урахуванням 96 годин робочого часу в рік, складуть:

$$Зєсв= 0,22 * 12960 = 2851,20 \text{ грн.}$$

3.3.3 Витрати машинного часу

Година машинного часу була розрахована раніше та становить:

$$С_{мч} = 0,6 \cdot 1,44 + \frac{15000 \cdot 0,3}{2080} + \frac{(5800+8300) \cdot 0,3}{2080} = 5.06 \text{ грн./година.}$$

Тобто, за рік роботи потрібно витратити, розрахувавши за формулою 3.8:

$$Вмч = t * Смч \text{ , грн.} \quad (3.8)$$

Що становитиме:

$$Вмч = 96 * 5.06 = 485,76 \text{ , грн.}$$

3.3.4 Загальні витрати на експлуатацію

Загальні витрати на експлуатацію розраховуються за формулою 3.9:

$$Векп = Ззпс + Зєсв + Вмч \text{ , грн.} \quad (3.9)$$

$$Векп = 12960 + 2851,20 + 485,76 = 16296,96 \text{ грн.}$$

3.4 Визначення збитку від поломок обладнання

Запобігти поломкам обладнання практично не можливо. Природно, первинна передумова наступна: витрати на ремонт або заміну деяких деталей обладнання не повинні перевищувати вартість самого обладнання.

Вихідні дані для підрахунку збитку:

- час простою внаслідок поломки, $t_п$ (в годинах), $t_п = 4$ год;
- час відновлення після поломки, $t_в$ (в годинах), $t_в = 2$ год;
- час повторного введення втраченої інформації, $t_{ви}$ (в годинах), $t_{ви} = 2$ год;
- заробітна плата обслуговуючого персоналу, Z_0 (грн. в місяць з податками), $Z_0 = 15500$ грн.;
- заробітна плата співробітників, Z_c (грн. в місяць з податками), $Z_c = 16000$ грн.;
- кількість обслуговуючого персоналу, N_0, $N_0 = 1$;
- число співробітників, N_c, $N_c = 13$;
- прибуток , О (грн. на рік), О = 18000000 грн.;
- вартість заміни обладнання та запасних частин, виправлення помилок в роботі системи, $П_{зч}$ (грн.), $П_{зч} = 0$ грн;
- число зламаного обладнання, I, I = 1;
- число поломок на рік, n, n = 12.

Вартість втрат від зниження продуктивності співробітників несправного обладнання розраховується за формулою 3.10:

$$П_п = \frac{\sum Z_c}{\frac{N_c}{160}} \cdot t_п, \text{ грн.}, \qquad (3.10)$$

де місячний фонд робочого часу при 40-а годинний робочий тиждень 176 годин.

Підставивши вихідні дані отримаємо:

$$П_П = (13*16000/160)*4 = 5200 \text{ , грн.}$$

Вартість відновлення зламаного обладнання розраховується за формулою 3.11:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \text{ грн.} \quad (3.11)$$

де $П_{ВИ}$ – вартість повторного введення інформації(формула 3.12),

$П_{ПВ}$ – вартість відновлення обладнання(формула 3.13).

$$П_{ви} = \frac{\sum Z_c}{\frac{N_c}{160}} \cdot t_{ви}, \text{ грн.} \quad (3.12)$$

$$П_{пв} = \frac{\sum Z_o}{\frac{N_o}{160}} \cdot t_в, \text{ грн.} \quad (3.13)$$

Отримаємо:

$П_{ВИ}$ = (13*16000/160)*2 = 2600 грн.

$П_{ПВ}$ = (1*15500/160)*2 = 193,75 грн.

Вартість заміни обладнання та запасних частин, виправлення помилок в системі, $П_{зч}$ (грн.) $П_{зч}$ = 0 грн.

Підставивши отримані результати в загальну формулу отримаємо:

$П_В$ = 2600 + 193,75 + 0 = 2793,75 грн.

Втрачена вигода від простою зламаного обладнання становить та розраховується за формулою 3.14 й 3.15 відповідно:

$$U = П_п + П_в + V, \text{ грн.} \quad (3.14)$$

$$V = \frac{O}{Fг} \cdot (t_п + t_в + t_{ви}), \text{ грн,} \quad (3.15)$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить 2080 годин.

$$V = (18000000/2080)*(4+2+2) = 69230,80 \text{ грн.}$$

$$U = 5200 + 2793,75 + 69230,80 = 77224,55 \text{ грн.}$$

Таким чином, загальний збиток від поломки обладнання, повторного введення інформації в системі, виявлення та усунення помилок в системі складе (формула 3.16):

$$ОУ = \sum_{n}\sum_{I} U \text{ , грн.} \qquad (3.16)$$

$$ОУ = 12 * 1 * 77224,55 = 926684,60, \text{ грн.}$$

3.5 Загальний ефект від впровадження ПБ

Загальний ефект від впровадження політики безпеки, визначається за формулою 3.17 з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = ОУ \cdot R - C, \text{ грн,} \qquad (3.17)$$

де ОУ – загальний збиток від атаки на вузол або сегмент корпоративної мережі, грн;

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

C – щорічні витрати на експлуатацію, грн.

Таким чином, загальний ефект від впровадження становить:

$$E = 926684,60 * 0,4 - 16296,96 = 354380,88 \text{ грн.}$$

3.6 Визначення та аналіз показників економічної ефективності

Оцінка економічної ефективності, розглянутої у спеціальній частині роботи, здійснюється на основі визначення та аналізу коефіцієнта повернення інвестицій ROSI (Return on Investment for Security) за формулою 3.18 та терміну окупності капітальних інвестицій T_o за формулою 3.20.

$$ROSI = \frac{E}{K}, \text{ частки одиниці,} \quad (3.18)$$

де Е – загальний ефект від впровадження системи захисту, грн.;

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

Підставивши відповідні значення, маємо:

$$ROSI = 354380,88 / 14827,20 = 23,9$$

Організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів (частини прибутку та амортизаційних відрахувань).

Проєкт визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта формула 3.19:

$$ROSI > (N_{деп} - N_{інф})/100) \quad (3.19)$$

де $N_{деп}$ – річна депозитна ставка, (18% - Юнекс Банк, Укрбудінвестбанк, Банк Кредит Дніпро);

$N_{інф}$ – річний рівень інфляції, (3% - період січень-березень 2023).

Підставивши відповідні значення, маємо:

$$ROSI > (18 - 3)/100),$$

$$23,9 > 0,15.$$

Отже, проєкт є економічно доцільним.

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI}, \text{ років.} \quad (3.19)$$

Підставимо значення:

$$T_o = 1 / 23,9 = 0,04 \text{ року.}$$

3.7 Висновок

Розрахувавши збитки від реалізації можливих несправностей, які склали 926684,60 грн., і порівнявши їх з витратами на забезпечення підтримки працездатності системи 16296,96 грн., та витратами на розробку 14827,20 грн., можна зробити висновок, що витрати на забезпечення інформаційної безпеки є не значними у співвідношенні до збитків, впровадження системи є економічно доцільним заходом (ROSI = 23,9), термін окупності системи безпеки становить 0,04 року. Для подальшого розвитку діяльності підприємства впровадження даних заходів є необхідною умовою для виконання.

ВИСНОВКИ

Використання описаних у цій роботі моделей загроз та порушників, а також визначення функціональних критеріїв захищеності та надання рекомендацій з захисту дозволяє підвищити рівень безпеки інформаційної системи підприємства з продажу побутової техніки.

Для захисту від несанкціонованого доступу, рекомендується використовувати механізми автентифікації та авторизації, такі як Active Directory. Для захисту від вторгнень рекомендується використовувати IDS/IPS програмне забезпечення та виконати налаштування.

Захист від витоку інформації може бути забезпечений за допомогою криптографічного захисту, захисту від перехоплювання пакетів даних, контролю доступу та інших заходів. Захист від вірусів та шкідливих програм забезпечується виявленням та вилученням шкідливих програм та вірусів.

Захист фізичної інфраструктури передбачає використання фізичної захисної інфраструктури, контроль доступу та інших заходів. Захист мережі може бути забезпечений за допомогою контролю доступу до мережі, захисту від DoS-атак, контролю доступу до мережевих ресурсів та інших заходів.

Для забезпечення доступності системи рекомендується резервування системних компонентів, кластеризацію та інші заходи. Захист від соціального інжинірингу може бути забезпечений навчанням персоналу та використанням механізмів контролю доступу.

Розроблена політика безпеки дозволить регламентувати всі аспекти захисту інформаційної системи підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

1. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу».

2. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

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

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

5. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу».

6. 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».

7. НД ТЗІ 3.7-003-05. «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».

8. Закон України "Про захист інформації в інформаційно-комунікаційних системах";

9. Закон України №2938-17 від 13.01.2011р."Про інформацію"//Відомості Верховної Ради України. – 2011. -№ 32, с.313.

10. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB – сторінки від несанкціонованого доступу.

11. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.

12. НД ТЗІ 3.6-005-21 Порядок категоріювання безпеки інформаційної системи та інформації.

13. НД ТЗІ 3.6 -004-21. Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці.

14. НД ТЗІ 3.6-006-21. Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем.

15. НД ТЗІ 3.6-007-21. Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	32	
6	А4	2 Розділ	33	
7	А4	3 Розділ	10	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

Пояснювальна записка.docx

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:
Розробка політики безпеки інформаційно-комунікаційної системи підприємства з продажу побутової техніки
студента групи 125-19-2
Храмов Микола Олегович

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 91 сторінках та містить 2 рисунка, 4 таблиці, 15 джерел та 4 додатка.

Мета роботи – розробити стратегію захисту інформаційної системи підприємства з продажу побутової техніки від можливих загроз та створення політики безпеки, що дозволить запобігти несанкціонованому доступу до даних та мінімізувати можливі наслідки випадкових чи зловісних дій.

Об’єкт дослідження – інформаційна система підприємства з продажу побутової техніки.

Предмет дослідження – заходи захисту інформаційної системи підприємства з продажу побутової техніки.

У роботі визначена актуальність розробки засобів захисту інформаційних ресурсів з обмеженим доступом, виконано опис виду діяльності підприємства, визначені посадові обов'язки персоналу підприємства з продажу побутової техніки та розглянута типова інформаційна система підприємства з продажу побутової техніки.

Розроблена модель загроз та модель порушника, визначено критерії захищеності та надані рекомендацій щодо реалізації системи захисту ІКС підприємства. Розроблено детальну політику безпеки захисту від несанкціонованого доступу ІКС підприємства з продажу побутової техніки.

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

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

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

Керівник