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 ***Браун Вікторія Сергіївна***

академічної групи ***УБіт-15-1***

спеціальності ***6.170103 Управління інформаційною безпекою***

спеціалізації[1]

за освітньо-професійною програмою

на тему ***Розробка політики безпеки інформації інформаційно-телекомунікаційної системи приватного підприємства "Астра-Дніпро"***

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.ф.-м.н., проф. Кагадій Т.С.			
розділів:				
спеціальний	ас. Чебаненко О.В.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2019

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Браун Вікторії Сергіївни*** **академічної групи** ***УБіт-15-1***
(прізвище ім'я по-батькові) (шифр)

спеціальності *6.170103 Управління інформаційною безпекою*
(код і назва спеціальності)

на тему ***Розробка політики безпеки інформації інформаційно-телекомунікаційної системи приватного підприємства "Астра-Дніпро"***

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

Розділ	Зміст	Термін виконання
Розділ 1	Провести аналіз стану рішення проблеми та постановку задачі. Провести аналіз нормативно-правової бази у сфері захисту інформації	20.03.2019
Розділ 2	Виконати обстеження об'єкта інформаційної діяльності. Проаналізувати загрози ІБ ІТС підприємства. Розробити політику безпеки інформації ІТС підприємства	30.05.2019
Розділ 3	Провести розрахунок вартості політики безпеки інформації підприємства	15.06.2019

Завдання видано _____ Кагадій Т.С.
(підпис керівника) (прізвище, ініціали)

Дата видачі: 08.01.2019р.

Дата подання до екзаменаційної комісії: 17.06.2019р.

Прийнято до виконання _____ Браун В.С.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: ___ с., __рис., __ табл., __ додатків, __ джерел.

Об’єкт розробки: інформаційно-телекомунікаційна система ПП "Астра-Дніпро".

Предмет дослідження: політика безпеки інформації об’єкта інформаційної діяльності.

Мета дипломного проекту: розробка політики безпеки для підприємства ПП "Астра-Дніпро.

В роботі зібрані дані про підприємство, виконане обстеження ОІД, обстеження інформаційного середовища та обстеження обчислювальної системи.

На підставі зібраних даних була розроблена модель порушника і модель загроз, та зроблено аналіз ризиків.

Визначено загрози з найбільш високим рівнем ризику:

– розголошення інформації, модифікація, знищення співробітниками допущеними до її обробки;

– крадіжка інформації або носіїв інформації.

Після чого був обраний профіль захищеності і розроблена політика безпеки. Після впровадження політики безпеки був ще раз проаналізований рівень ризиків, і було визначено, що він зменшився.

ПОЛІТИКА БЕЗПЕКИ, МОДЕЛЬ ЗАГРОЗ, АНАЛІЗ РИЗИКУ, ПРОФІЛЬ ЗАХИЩЕНОСТІ, ISO 27001, ОБСТЕЖЕННЯ.

РЕФЕРАТ

Пояснительная записка: __ с., __ рис., __ табл., __ приложения, __ источников;

Объект разработки: информационно-телекоммуникационная система ЧП "Астра-Днепр".

Предмет исследования: политика безопасности информации объекта информационной деятельности.

Цель дипломного проекта: разработка политики безопасности для предприятия ЧП "Астра-Днепр.

В работе собраны данные о предприятии, выполнено обследование ОИД, обследование информационной среды и обследования вычислительной системы.

На основании собранных данных была разработана модель нарушителя и модель угроз, и сделан анализ рисков.

Определены угрозы с наиболее высоким уровнем риска:

- разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработки;

- кража информации или носителей информации.

После чего был избран профиль защищенности и разработана политика безопасности. После внедрения политики безопасности был еще раз проанализирован уровень рисков, и было определено, что он уменьшился.

ПОЛИТИКА БЕЗОПАСНОСТИ, МОДЕЛИ УГРОЗ, АНАЛИЗ РИСКОВ, ПРОФИЛЬ ЗАЩИЩЕННОСТИ, ISO 27001, ОБСЛЕДОВАНИЕ.

ABSTRACT

Executive: ___ pages., __ fig., __ table, __ annexes, __ sources.

Object of development: information and telecommunication system of PE "Astra-Dnepr".

Subject of research: security policy information object.

The purpose of the diploma project: development of a security policy for the enterprise of private enterprise "Astra-Dnepr.

In this work, data on the company is collected, an OIE survey is carried out, a survey of the information environment and a computer system examination.

Based on the collected data an offender model and a model of threats were developed, and a risk analysis was carried out.

The threats with the highest risk are identified:

- disclosure of information, modification, destruction by employees allowed for its processing;

- theft of information or information carriers.

After that, the security profile was selected, and a security policy was developed. After the implementation of the security policy, the level of risk was once again analyzed, and it has been determined that it has decreased.

SAFETY POLICY, DANGER MODEL, RISK ANALYSIS, PROFILE OF PROTECTION, ISO 27001, EXAMINATION.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ISO	–	International Organization for Standardization;
АС	–	автоматизована система;
ІТС	–	інформаційно-телекомунікаційна система;
ОС	–	операційна система;
ПБ	–	політика безпека;
ПЗ	–	програмне забезпечення;
ПП	–	приватне підприємство.

ЗМІСТ

с.

ВСТУП 9
РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ 11
1.1 Захист інформації комерційних підприємств 11
1.1.1 Основні загрози інформаційній безпеці комерційного підприємства 12
1.1.2 Інциденти інформаційної безпеки на підприємстві 14
1.1.3 Політика безпеки 19
1.2 Аналіз нормативно-правової бази у сфері захисту інформації 21
1.2.1 Законодавче регулювання інформаційної сфери в Україні 22
1.2.2 Нормативні документи в галузі технічного захисту інформації 24
1.2.3 Міжнародні стандарти забезпечення інформаційної безпеки підприємства 24
1.3 Постановка задачі 26
РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА 27
2.1 Загальні відомості про організацію 27
2.1.1 Організаційна структура підприємства 27
2.2 Обстеження об’єкта інформаційної діяльності 28
2.2.1 Обстеження обчислювальної системи ПП «Астра-Дніпро» 31
2.2.2 Обстеження інформаційного середовища ПП «Астра-Дніпро» 34
2.2.3 Аналіз загроз інформації 37
2.2.4 Модель порушника 42
2.3 Аналіз ризиків 45
2.4 Необхідність створення комплексної системи захисту інформації 51
2.5 Профіль захищеності 52
2.5.1 Реалізація критеріїв профілю 53
2.6 Розробка політики безпеки 58
2.7 Аналіз ризиків після впровадження політики безпеки 66
2.8 Висновки до другого розділу 72

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ 73
3.1. Розрахунок фіксованих (капітальних) витрат 73
3.2 Розрахунок поточних витрат 76
3.3 Оцінка можливого збитку 78
3.4 Загальний ефект від впровадження системи інформаційної безпеки 81
3.5 Визначення та аналіз показників економічної ефективності розробки політики інформаційної безпеки 82
3.6 Висновок 83
ВИСНОВКИ 84
СПИСОК ЛІТЕРАТУРИ 85
ДОДАТОК А 87
ДОДАТОК Б 88
ДОДАТОК В 89
ДОДАТОК Г 90
ДОДАТОК Д 91
ДОДАТОК Е 92

ВСТУП

В даний час, в Україні, у зв'язку з входженням у світовий інформаційний простір, швидкими темпами впроваджуються комп'ютерні і телекомунікаційні технології. Створюються локальні і регіональні обчислювальні мережі, великі території охоплюються мережами мобільного зв'язку. Системи телекомунікацій активно впроваджуються у фінансові, промислові, торгові і соціальні сфери.

Захист інформації – сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації.

Гострота проблем захисту інформації у сучасних умовах визначається наступними чинниками:

- високими темпами зростання кількості засобів обчислювальної техніки і зв'язку, розширенням областей використання ЕОМ, різноманіттям і широким розповсюдженням інформаційно-керуючих систем, що підлягають захисту;
- залученням в процес інформаційної взаємодії все більшого числа людей і організацій, різким зростанням їх інформаційних потреб;
- ставленням до інформації, як до товару, переходом до ринкових відносин, з властивою їм конкуренцією і промисловим шпигунством;
- концентрацією великих обсягів інформації різного призначення на електронних носіях;
- кількісним і якісним вдосконаленням способів доступу користувачів до інформаційних ресурсів.

Звичайно, в такій ситуації виникає потреба в захисті обчислювальних систем та інформації від несанкціонованого доступу, крадіжки, знищення і інших злочинних і небажаних дій.

Забезпечення захисту інформації необхідно здійснювати у таких напрямах:

1 Захист інформації, яку науковці використовують у процесі досліджень, а також захист результатів досліджень у вигляді інтелектуальної власності.

2 Захист інформації від руйнування і втрати у зв'язку з технологічними неполадками в комп'ютерних системах.

3 Захист інформації, яка стосується життєдіяльності особистості, груп людей або суспільства загалом і є конфіденційною, тобто такою, що може принести їм шкоду, коли стане легкодоступною для загалу.

4 Захист інформації, що висвітлює відкриття або є комерційною, технічною чи технологічною таємницею.

5 Захист інформації, яка є державною таємницею.

Тривалий час методи захисту інформації розроблялися тільки державними органами, а їхнє впровадження розглядалося як виключне право тієї або іншої держави. Проте в останні роки з розвитком комерційної і підприємницької діяльності збільшилась кількість спроб несанкціонованого доступу до конфіденційної інформації, а проблеми захисту інформації виявилися в центрі уваги багатьох спеціалістів із різноманітних країн. Внаслідок цього процесу значно зросла потреба у фахівцях із захисту інформації.

Об’єкт розробки: інформаційно – телекомунікаційна система ПП "Астра-Дніпро".

Предмет дослідження: політика безпеки інформації об’єкта інформаційної діяльності.

Мета роботи: розробка політики безпеки для підприємства ПП "Астра-Дніпро.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Захист інформації комерційних підприємств

Відмітною ознакою у сфері продажу є порівняння витрат і результатів роботи, прагнення до отримання максимального прибутку. Крім того, однією з особливостей у сфері продажу є те, що комерційна діяльність здійснюється в умовах жорсткої конкуренції, суперництва, боротьби підприємств за отримання вигод та переваг у порівнянні з підприємствами аналогічного профілю.

Конкурентна боротьба це супутник і рушій комерційної діяльності, а також умова виживання комерційних підприємств. Звідси їх прагнення зберегти в секреті від конкурента прийоми та особливості своєї діяльності, які забезпечують їм перевагу над конкурентом. Звідси і прагнення конкурентів виявити ці секрети, щоб використовувати їх у своїх інтересах для отримання переваги в конкурентній боротьбі. Несанкціоноване одержання, використання (розголошення) таких секретів без згоди їх власників віднесені до однієї з форм недобросовісної конкуренції, званої промисловим шпигунством.

Згідно зі статтею 505 Цивільного Кодексу України, комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію [1].

Під комерційною таємницею підприємства розуміються відомості, які не становлять державну таємницю, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою діяльністю підприємства, розголошення (передача, витік), яких може завдати шкоди його інтересам.

Збереження і захищеність інформації від стороннього втручання істотно впливає на роботу компанії. З кожним роком все більше зростає кількість вірусів, мережевих атак зловмисників, виникають загрози порушення

конфіденційності інформації всередині компанії, що призводить до фінансових втрат, і часто - вельми значних.

Порушення статусу будь-якої інформації полягає у порушенні її логічної структури та змісту, фізичного збереження її носія, доступності для правомочних користувачів. Порушення статусу конфіденційної інформації додатково включає порушення її конфіденційності або закритості для сторонніх осіб.

Згідно з Законом України «Про доступ до публічної інформації», конфіденційна інформація – інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов [2].

Отже, підсумовуючи вищесказане, необхідно підкреслити, що пріоритетним напрямком в процесі забезпечення інформаційної безпеки підприємства є забезпечення комерційної таємниці, що дозволяє успішно конкурувати на ринку товарів і послуг.

1.1.1 Основні загрози інформаційній безпеці комерційного підприємства

Загрози захисту інформації з обмеженим доступом можуть бути зовнішніми і внутрішніми. Значну небезпеку становлять дії інших господарюючих суб'єктів. В даному випадку ризик забезпечення безпеки інформації несе нездорова конкуренція, яка відноситься до зовнішніх .

Зовнішні дії можуть бути спрямовані на пасивні носії інформації і виражатися, наприклад, в наступному:

- спроби викрадення документів або зняття копій з документів, знімних носіїв (флеш-карти);
- зняття інформації, що виникає в процесі передачі;
- знищення інформації або пошкодження її носіїв;
- випадкове або навмисне доведення до відома конкурентів документів або матеріалів, що містять комерційну таємницю.

Зовнішні дії можуть бути також спрямовані на персонал компанії і виражатися в формі підкупу, погроз, шантажу, вивідування інформації, що становить комерційну таємницю, або припускати переманювання провідних спеціалістів на конкуруючу фірму та інше.

Внутрішні загрози становлять найбільшу небезпеку для знову сформованих колективів, де не встигли скластися традиції підтримки високої репутації підприємства. Не виключена ймовірність того, що окремі співробітники з високим рівнем самооцінки через незадоволення своїх амбіцій (невдоволення рівнем заробітної плати, відносинами з керівництвом, колегами та інше) можуть розголосити комерційну таємницю конкурентам, а також спробувати знищити важливу інформацію або пасивні носії (наприклад, внести комп'ютерний вірус).

Система безпеки потенційних і реальних загроз непостійна, оскільки ті можуть з'являтися, зникати, зменшуватися або наростати. На підставі цього система забезпечення інформаційної безпеки організації розглядається як цілий комплекс прийнятих управлінських рішень, спрямованих на виявлення і запобігання зовнішнім та внутрішнім загрозам.

Система інформаційної безпеки підприємства повинна включати:

- комп'ютерну безпеку, яка забезпечить якісну роботу всіх апаратних комп'ютерних систем і створить єдиний цілісний, конфіденційний і доступний ресурс;
- безпеку комунікацій;
- безпечне програмне забезпечення, яке включає комплекс програм, спрямованих як на безпечну обробку всіх даних так і на безпечну роботу всіх систем;
- безпеку даних, яка захистить інформацію від випадкових, недбалих, неавторизованих і умисних розголошень або злому системи.

Базою для забезпечення інформаційної безпеки організації служить вживання наступних заходів: аналіз реальних і потенційно можливих ситуацій, що становлять загрозу безпеці інформації, оцінка характеру загроз, прийняття

комплексу заходів для визначення загрози і реалізація прийнятих заходів щодо запобігання загрози.

Вельми важливим є також відображення питань захисту комерційної таємниці в контракті, що укладається з керівником підприємства при його призначенні на посаду.

1.1.2 Інциденти інформаційної безпеки на підприємстві

Кількість потенційних каналів витоку інформації достатньо велика. Найбільш поширені з них відносяться до категорії ненавмисного розкриття інформації співробітниками організації з причин непоінформованості або недисциплінованості. Відсутність уявлень щодо правил роботи з конфіденційними документами, невміння визначити, які документи є конфіденційними, та звичайна неуважність при роботі з інформацією – все це може призвести до виникнення події або інциденту інформаційної безпеки.

Розглянемо декілька визначень понять події та інциденту інформаційної безпеки:

1 Згідно з ISO/IEC TR 18044:2004 під подією інформаційної безпеки (ПІБ)

розуміється стан системи, сервісу або мережі, котрий свідчить про можливе порушення політики безпеки, або про невідому ситуацію, яка може мати відношення до безпеки, тоді як інцидент інформаційної безпеки (ІІБ) – це одна або серія подій інформаційної безпеки, які можуть призвести до збитків та втрат для організації. Втрати можуть бути, як матеріальними (вартість інформації, експлуатаційні витрати і т.д.) так і нематеріальними (репутація організації, зміна морально-психологічного клімату та інше [3].

2 Згідно з ISO/IEC 27001 подія інформаційної безпеки – це ідентифікований випадок стану системи або мережі, який вказує на можливе порушення політики інформаційної безпеки або відмову засобів захисту, або раніше невідому ситуацію, яка може бути суттєвою для політики безпеки. Інцидент інформаційної безпеки – це одинична подія або ряд небажаних та

непередбачених подій інформаційної безпеки, із-за яких велика ймовірність розкриття конфіденційної бізнес-інформації [4].

Управління інцидентами – це важливий процес, який забезпечує організації можливість спочатку виявити інцидент, а потім за допомогою коректно обраних засобів підтримки якомога швидше його вирішити.

Основна задача управління інцидентами – якомога швидше відновити нормальну роботу служб і звести до мінімуму негативний вплив інциденту на роботу організації для підтримки якості і доступності служб на максимально можливому рівні. Нормальною вважається робота служб, що не виходить за рамки угоди про рівень обслуговування.

Цілі управління інцидентами:

1 Відновлення нормальної роботи служб в найкоротші терміни.

2 Зведення до мінімуму впливу інцидентів на роботу організації.

3 Забезпечення злагодженої обробки всіх інцидентів і запитів обслуговування.

4 Зосередження ресурсів підтримки на найбільш важливіших напрямах.

5 Надання відомостей, які дозволяють оптимізувати процеси підтримки, зменшити кількість інцидентів і спланувати управління.

Для забезпечення управління інцидентами система повинна виконувати наступні функції:

1 Контроль зовнішніх пристроїв, що підключаються, зокрема можливість в режимі online контролювати клієнтські комп’ютери, контроль роботи агента, контроль політик агента, можливість налаштування реагування на події, захист агента від видалення або виключення, наявність засобів контролю цілісності.

2 Моніторинг агентів і їх захист, зокрема можливість в режимі online контролювати клієнтські комп’ютери, контроль роботи агента, контроль політик агента, можливість налаштування реагування на події, захист агента від видалення або виключення, контроль цілісності.

3 Управління системою та обробка інцидентів, зокрема наявність власної консолі, розподіл ролей адміністратора і спеціалістів з безпеки, налаштування

сповіщень, можливості реагування на інциденти, аналіз подій, зафіксованих системою, збереження історії інцидентів для наступного аналізу, заборона на пропуск затриманого повідомлення або дозвіл із записом про інцидент.

4 Формування системи звітності про роботу системи управління інцидентами, зокрема можливість побудови звітів про порушення, наявність варіантів отримання звітів про порушення, тимчасовий запис звіту в локальне сховище у разі недоступності сервера, експорт звітів, запис в журнал реєстрації дій адміністраторів системи.

Об’єкти системи моніторингу інцидентів:

- апаратні засоби (комутатори, маршрутизатори, сканери, UTM пристрої);
- програмні комплекси (операційні системи, антивірусні шлюзи, персональні антивірусні системи, підсистеми обробки даних, доступні служби та сервіси);
- інформаційні ресурси (бази даних, файли користувачів доступні в мережі тощо);
- дії користувачів корпоративної мережі.

Основні етапи функціонування системи управління інцидентами інформаційної безпеки.

1 Планування і підготовки. Здійснюється розробка схеми управління інцидентами, розробка і затвердження ряду організаційно-регламентуючих документів, виділення людських і матеріальних ресурсів, проведення необхідного навчання та апробація обраної схеми управління. Відповідно до ISO/IEC TR 18044 необхідно створити групу щодо розслідування інцидентів ІБ.

2 Експлуатації. Здійснюється виявлення інциденту ІБ, ідентифікація інциденту ІБ, реагування, розслідування й аналіз.

3 Аналізу. Група з реагування на інциденти проводить поглиблений аналіз інциденту, на основі результатів аналізу робляться висновки і складаються рекомендації щодо поліпшення процесу забезпечення ІБ та

реагування на інциденти. Формується звіт про інцидент. Основним процесом етапу є поглиблений аналіз інциденту.

4 Поліпшення. Здійснюється реалізація рекомендацій щодо поліпшення процесів забезпечення ІБ та реагування на інцидент. Затверджені уповноваженою особою організації рекомендації передаються на виконання відповідальним особам.

Як приклад, інцидентами інформаційної безпеки, що сталися з вини співробітників можуть бути:

- порушення конфіденційності та цілісності цінної інформації;
- незаконний моніторинг інформаційних систем;
- знищення інформації;
- компрометація інформаційної системи (наприклад, розголошення пароля користувача);
- відмова в обслуговувані сервісів, засобів обробки інформації, обладнання; пошкодження електричних мереж;
- неавторизоване використання системи для зберігання особистих даних;

та інші порушення вимог до інформаційної безпеки, прийнятих в компанії (порушення правил обробки інформації);

Для підвищення ефективності розслідування інцидентів інформаційної безпеки в організації повинен буди фахівець з інформаційної безпеки, що буде:

- розробляти політики безпеки (ПБ) з детально опрацьованими документами, які регламентують діяльність персоналу всіх рівнів з чітко вказаною відповідальністю в межах покладених обов’язків;
- розробляти посадові інструкції, правила, регламенти з чітко визначеними правами та обов’язками персоналу, пов’язані з текучими бізнес-процесами, що дозволяють добре прогнозувати наслідки та розробити надійні превентивні дії для запобігання повторення таких інцидентів.

В організації повинен бути розроблений відповідний дисциплінарний процес, що проводиться у відношенні до порушників безпеки і передбачає розслідування наслідків інцидентів та прийняття адекватних мір впливу на них.

При визначені міри запобігання виникненню інцидентів ІБ, фахівцю з інформаційної безпеки, необхідно орієнтуватися на положення дійсного законодавства України. Відносини між робітником та роботодавцем та відповідальність за порушення інформаційної безпеки організації регулюються Кримінальним Кодексом, Адміністративним Кодексом та Кодексом Законів про Працю:

1 Згідно з Кримінальним Кодексом України, ст. 231 за шкоду, заподіяну підприємству, установі, організації при виконанні трудових обов'язків, працівники, з вини яких заподіяно шкоду, несуть матеріальну відповідальність у розмірі прямої дійсної шкоди, але не більше свого середнього місячного заробітку [5].

2 Згідно з Кримінальним Кодексом України, ст. 232 умисні дії, спрямовані на отримання відомостей, що становлять комерційну таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб’єкту господарської діяльності, – караються штрафом від двохсот до тисячі неоподаткованих мінімумів доходів громадян або обмеженням волі на строк до п’яти років, або позбавленням волі на строк до трьох років [6].

3 Згідно з Кримінальним Кодексом України, ст. 232 умисне розголошення комерційної або банківської таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб'єкту господарської діяльності, - карається штрафом від двохсот до п'ятисот неоподатковуваних мінімумів доходів громадян з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років, або виправними роботами на строк до двох років, або позбавленням волі на той самий строк [6].

4 Згідно з Кримінальним Кодексом України, ст. 362 несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах(комп’ютерах), автоматизованих системах,

комп’ютерних мережах, або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, - караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк та з конфіскацією програмних чи технічних засобів, за допомогою яких було здійснено несанкціоновані перехоплення або копіювання інформації, які є власністю винної особи [7].

5 Згідно з Адміністративним Кодексом України, ст.212 здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в автоматизованих системах, - тягне за собою накладання штрафу від п’яти до десяти неоподатковуваних мінімумів доходів громадян з конфіскацією засобів, що використовувалися для незаконного доступу, або без такої [8].

1.1.3 Політика безпеки

Під політикою безпеки інформації слід розуміти набір законів, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін "політика безпеки" може бути застосовано щодо організації, АС, ОС, послуги, що реалізується системою (набору функцій), і т. ін. [9]

Під час розробки політики безпеки повинні бути враховані технологія обробки інформації, моделі порушників і загроз, особливості ОС, фізичного середовища та інші чинники. В ІТС може бути реалізовано декілька різних політик безпеки, які істотно відрізняються.

Як складові частини загальної політики безпеки в ІТС мають існувати політики забезпечення конфіденційності, цілісності, доступності оброблюваної інформації.

Політика безпеки повинна стосуватись: інформації (рівня критичності ресурсів ІТС), взаємодії об’єктів (правил, відповідальності за захист інформації,

гарантій захисту), області застосування (яких складових компонентів ІТС політика безпеки стосується, а яких – ні).

Політика безпеки має бути розроблена таким чином, що б вона не потребувала частої модифікації (потреба частої зміни вказує на надмірну конкретизацію, наприклад, не завжди доцільно вказувати конкретну назву чи версію програмного продукту).

Політика безпеки повинна базуватися на наступних основних принципах:

- системності;
- комплексності;
- неперервності захисту;
- достатності механізмів і заходів захисту та їхньої адекватності загрозам;
- гнучкості керування системою захисту, простоти і зручності її використання;
- відкритості алгоритмів і механізмів захисту, якщо інше не передбачено окремо.

Політика безпеки повинна доказово давати гарантії того, що:

- в ІТС (в кожній окремій складовій частині, в кожному функціональному завданні і т. ін.) забезпечується адекватність рівня захисту інформації рівню її критичності;
- реалізація заходів захисту інформації є рентабельною;
- в будь-якому середовищі функціонування ІТС забезпечується оцінюваність і перевіряємість захищеності інформації;
- забезпечується персоніфікація положень політики безпеки (стосовно суб’єктів ІТС), звітність (реєстрація, аудит) для всіх критичних з точки зору безпеки ресурсів, до яких здійснюється доступ в процесі функціонування ІТС;
- персонал і користувачі забезпечені достатньо повним комплектом документації стосовно порядку забезпечення захисту інформації;

- всі критичні з точки зору безпеки інформації технології (функції) ІТС мають відповідні плани забезпечення неперервної роботи та її поновлення у разі виникнення непередбачених ситуацій;
- враховані вимоги всіх документів, які регламентують порядок захисту інформації в ІТС, та забезпечується їхнє суворе дотримання.

Методологія розроблення політики безпеки включає в себе наступні роботи:

- розробка концепції безпеки інформації в ІТС;
- аналіз ризиків;
- визначення вимог до заходів, методів та засобів захисту;
- вибір основних рішень з забезпечення безпеки інформації;
- організація виконання відновлювальних робіт і забезпечення неперервного функціонування ІТС;
- документальне оформлення політики безпеки.

1.2 Аналіз нормативно-правової бази у сфері захисту інформації

Нормативно-правове забезпечення організації і проведення заходів щодо захисту інформації являє собою сукупність законів, нормативних актів і правил, що регламентують як загальну організацію робіт, так і створення і функціонування конкретних систем захисту інформації. В даний час в Україні, як і в інших країнах СНД, нормативно-правова база захисту інформації знаходиться в стадії формування.

При побудові правової бази системи безпеки інформації в Україна розв’язує такі задачі:

- розробка в якості правової основи системи забезпечення безпеки інформації базового закону, що регламентує відношення і розмежування сфери повноважень всіх учасників інформаційних відношень, а також визначальні державні органи, що забезпечують інформаційну безпеку і засоби контролю з боку держави за розмежуванням доступу до інформації;

- розробка законодавчих актів і правових норм, що усестороннє охоплюють всі проблеми захисту інформації і підходів, що визначають специфіку забезпечення безпеки інформації в різноманітних сферах діяльності держави і товариства;

- регламентація рівнів безпеки інформації й адекватних їм методів і засобів захисту. Однієї з найбільше важливих складових частин правового забезпечення системи безпеки інформації є стандартизація і сертифікація, що повинні вирішувати такі задачі;

- створення пакета основних стандартів організаційно-методичного і термінологічного забезпечення системи захисту інформації;

- стандартизація вимог по захисту інформації в засобах обчислювальної техніки, в автоматизованих системах, інформаційних мережах і засобах телекомунікації;

- нормативне і метрологічне забезпечення сертифікації й атестації технічних засобів захисту інформації і контролю їхньої ефективності.

1.2.1 Законодавче регулювання інформаційної сфери в Україні

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

Закон України "Про інформацію" установлює загальні правові основи одержання, використання, поширення і збереження інформації.

Закон закріплює право особистості на інформацію у всіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відношень, регулює доступ до інформації і забезпечує її охорону, захищає особистість і товариство від помилкової інформації. Чинність закону поширюється на інформаційні відношення, що виникають у всіх сферах життя і діяльності товариства і держави при одержанні, використанні, поширенні і збереженні інформації. Суб'єктами інформаційних відношень є громадяни України, юридичні особи, держава Україна, а також інші держави, їхні громадяни і юридичні особи, міжнародні організації й особи без громадянства. З метою задоволення потреби в інформаційній діяльності створюються інформаційні служби, системи, мережі, бази і банки даних. Закон передбачає створення загальної системи охорони інформації.

Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі - система) [10].

Метою цього закону є встановлення основ регулювання правових відношень по захисті інформації в автоматизованих системах за умови дотримання права власності громадян України і юридичних осіб на інформацію і права доступу до неї, права власника інформації на її захист, а також установленого чинним законодавством обмеження на доступ до інформації.

Закон України «Про державну таємницю» регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України [11].

Закон України «Про захист персональних даних» регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина,

зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних[12].

Значна кількість питань функціонування інформаційної сфери донині неврегульована на законодавчому рівні. Це стосується як проблем інфраструктури, так і діяльності ЗМІ, інформаційно-аналітичних установ тощо.

Значну проблему становить фактична відсутність правового регулювання функціонування в Україні міжнародних інформаційних систем, найяскравішим прикладом яких є Інтернет. Зокрема, відсутність відповідних нормативно-правових актів створює певні проблеми для Інтернет ЗМІ та сприяє їх використанню інформації у деструктивних цілях.

1.2.2 Нормативні документи в галузі технічного захисту інформації

На сьогодні в Україні чинними є ряд нормативних документів (НДТЗІ), що регулюють технічний захист інформації.

Перелік нормативних документів в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України (ДСТУ) стосовно створення і функціонування КСЗІ:

- НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
- Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96.
- НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.
- НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
- НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

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

1.2.3 Міжнародні стандарти забезпечення інформаційної безпеки підприємства

ISO/IEC 27001 – міжнародний стандарт по інформаційної безпеки розроблений спільно Міжнародною Організацією по Стандартизації (ISO) і Міжнародної електротехнічної комісією (IEC). Підготовлено до випуску підкомітетом SC27 Об’єднаного технічного комітету JTC 1.

Стандарт містить вимоги в області інформаційної безпеки для створення, розвитку і підтримки Системи менеджменту інформаційної безпеки.

Кращі світові практики в галузі управління інформаційною безпекою описані в міжнародному стандарті на системи менеджменту інформаційної безпеки ISO / IEC 27001 (ISO 27001). ISO 27001 встановлює вимоги до системи менеджменту інформаційної безпеки (СМІБ) для демонстрації здатності організації захищати свої інформаційні ресурси.

Поняття захисту інформації трактується міжнародним стандартом як забезпечення конфіденційності, цілісності та доступності інформації.

Основа стандарту ISO 27001 – система управління ризиками, пов’язаними з інформацією. Система управління ризиками дозволяє отримувати відповіді на наступні питання:

- напрямки інформаційної безпеки на яких потрібно зосередити увагу;
- часу і кошти, які можна витратити на дане технічне рішення для захисту інформації.

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

процес опису, розробки та перевірки продукту був проведений в строгому порядку. Прообразом даного документа послужили «Критерії оцінки безпеки інформаційних технологій» (англ. Evaluation Criteria for IT Security, ECITS), робота над якими почалася в 1990 році.

Стандарт містить два основних види вимог безпеки: функціональні, що висуваються до функцій безпеки і реалізує їх механізмів, і вимоги довіри, які пред’являються до технології та процесу розробки та експлуатації.

1.3 Постановка задачі

На підставі аналізу нормативно-правової бази, можна зробити висновок про необхідність захисту інформації на комерційних підприємствах. Отже, на ПП "Астра-Дніпро" необхідно виконати наступні завдання:

- зібрати дані про підприємство, виконати обстеження ОІД, обстеження інформаційного середовища та обстеження обчислювальної системи;
- на підставі зібраних даних про об’єкт розробити модель загроз та модель порушника;
- провести аналіз ризиків;
- вибрати профіль захищеності;
- розробити політику безпеки (інструкції, рекомендації);
- провести аналіз ризиків після впровадження політики безпеки.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про організацію

У роботі розглянуто приватне підприємство «Астра-Дніпро», яке займається оптовим та роздрібним продажем кави, чаю, та кавового обладнання через Інтернет – магазин, та через магазин у місті. Фірма здійснює доставку продукції по всій території України.

Повна назва підприємства: ПП «Астра-Дніпро».

Адреса: м. Дніпро, вул. Богдана Хмельницького 152.

Форма власності: приватна власність.

2.1.1 Організаційна структура підприємства

Підприємство працює кожен день з 9.00 – 19.00. Оформити замовлення на сайті, можливо в будь-який час.

Графік роботи співробітників:

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

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

Прибирання приміщення проводиться кожного буднього дня з 9.30 до 10.00.

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

Штатна чисельність співробітників:

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

- продавці – 2 людини;
- прибиральниця – 2 людини;

Всього – 17 чоловік;

2.2 Обстеження об’єкта інформаційної діяльності

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

На першому поверсі знаходяться офіси підприємств, що займаються діяльністю в сфері продажів та приватні приміщення. На другому поверсі знаходяться приватні приміщення.

Контрольована зона (КЗ) визначена наказом керівника підприємства №1 від 17.03.2009 р і обмежена

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

На ситуаційному плані підприємства (див. додаток Д) показано місце розташування ОІД та розташовані навколо нього об’єкти.

Комісія для проведена обстеження приміщення ОІД визначена наказом директора від 15 січня 2017 р (див. додаток Е)

На генеральному плані підприємства (рисунок 2.1) показане розміщення основних виробничих, допоміжних, складських об'єктів підприємства. Умовні позначення наведені в таблиці 2.1

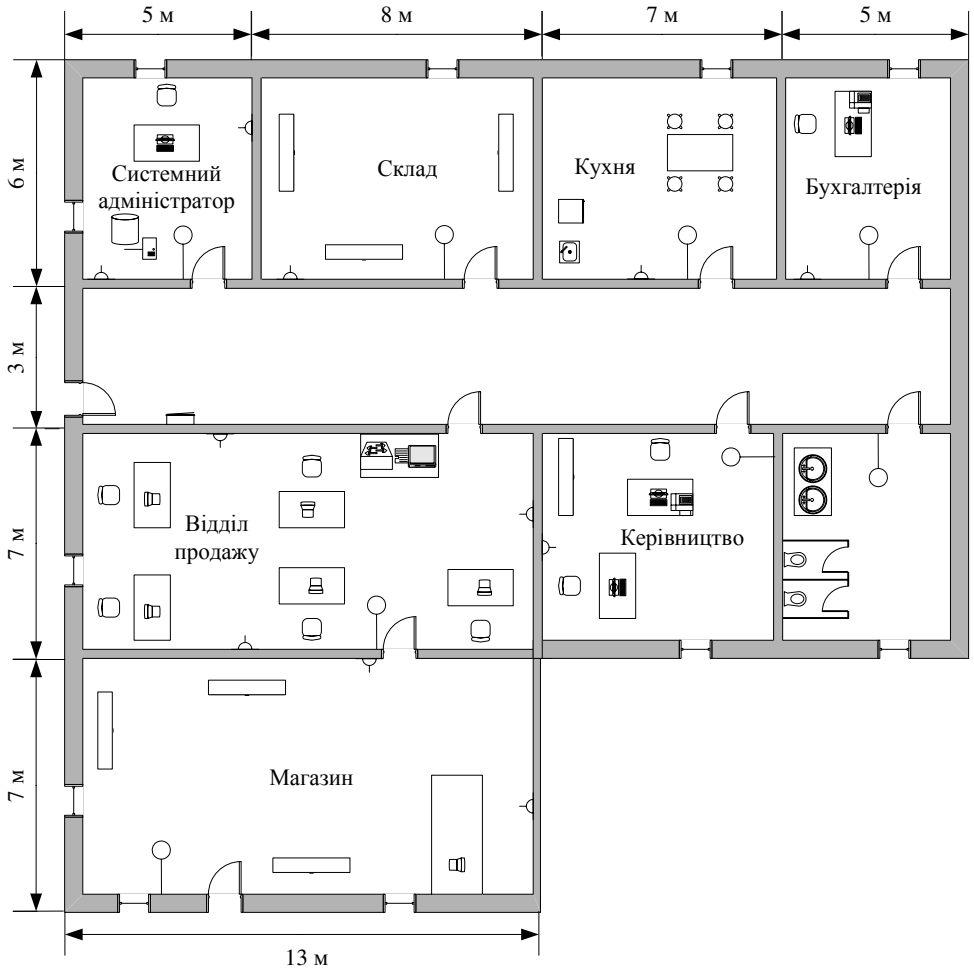
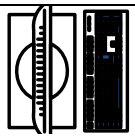
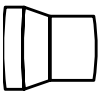
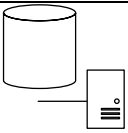
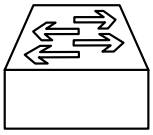
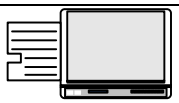
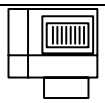
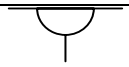
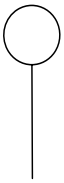


Рисунок 2.1- Генеральний план ПП «Астра-Дніпро»

Таблиця 2.1 – Умовні позначення

№	Позначка на плані	Значення
1	2	3
1		Ноутбук
2		Комп’ютер
3		Сервер
4		Комутатор

Продовження таблиці 2.1

1	2	3
5		МФУ мережевий
6		Принтер локальний
7		Розетка
8		Вимикач
9		Електричний щиток

Фізична характеристика об’єкта інформаційної діяльності:

- товщина несучих стін - 0,5 м;
- товщина перегородки - 0,25 м;
- склад стін - залізобетонні конструкції, висота перекриттів 2,6 м;
- склад перегородок - цегла, утеплений гіпсокартоном;
- стеля - залізобетонна монолітна заливна товщиною 150 мм;
- підлога - монолітна бетонна стяжка товщиною 100 мм;
- покриття підлоги – лінолеум 10 мм;
- вікна – 11 штук, зроблені з металопластику, розмірами 1400мм*1250мм, з 2-камерним склопакетом;
- внутрішні двері – 8 штук, зроблені з ламінованого МДФ, розміром 1200 мм * 2000мм;
- зовнішні двері – 2 штуки, зроблені зі звареної листової сталі, оздоблені замком, розміром 1200 мм * 2000мм;

- електропостачання здійснюється через підключення до трансформаторної підстанції, виходить за межі контрольованої зони, розетки і вимикачі - 220 В;

- система опалення підключена до міської мережі опалення, знаходиться за межами КЗ (пластикові труби, однотрубна вертикальна система опалення);

- на об’єкті є Інтернет і телефонний зв'язок;

- підприємство обладнано системою контролю доступу. Режим доступу здійснюється через контрольно-пропускний пункт (тобто вхід в будівлю здійснюється за пропусками та через охорону).

2.2.1 Обстеження обчислювальної системи ПП «Астра-Дніпро»

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

Мережу поділено на мережеві (робочі) групи – директор, заступник директора, системний адміністратор, бухгалтер, інші користувачі. Кожна з цих мережевих груп має доступ лише до певної інформації та програм. У кожного працівника підприємства є свій обліковий запис, доступ до якого має лише він. Забезпеченням роботи комп’ютерної техніки, комп’ютерної мережі і програмного забезпечення в організації займається системний адміністратор.

Використовувати зовнішні носії мають право лише директор, заступник директора та системний адміністратор. Усі співробітники мають доступ до Інтернету, але з обмеженням доступу до соціальних мереж. Усі співробітники мають доступ до факсу та принтеру.

Вихід комп’ютерів до мережі Інтернет забезпечується через кабель. На рисунку 2.2 зображена схема мережі інформаційно-телекомунікаційної системи ПП «Астра-Дніпро».

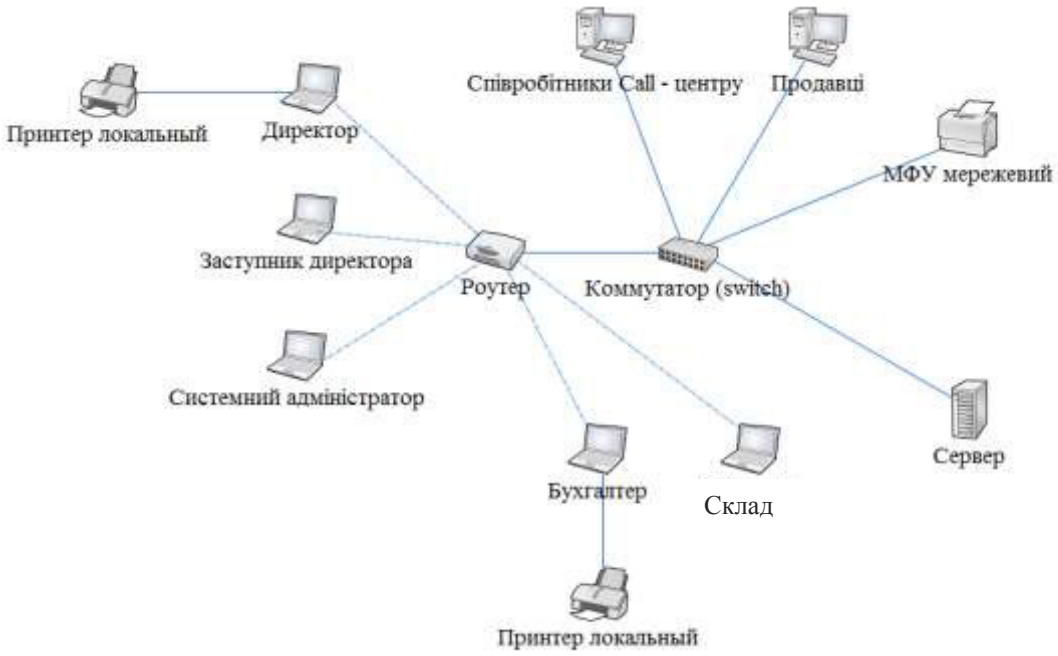


Рисунок 2.2 – Структурна схема мережі інформаційно-телекомунікаційної системи ПП «Астра-Дніпро»

Згідно з НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» у ПП «Астра-Дніпро» використовується АС третього класу, оскільки представляє собою розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності [13].

У таблицях 2.2 і 2.3 представлений перелік апаратного і програмного забезпечення мережі ПП «Астра-Дніпро».

Таблиця 2.2 – Апаратне забезпечення системи

№	Найменування	Характеристика	Кількість
1	2	3	4
1	Робоча станція	Модель: ASUS M52AD	5
2	Комутатор	Модель: D-Link DES-1016C	1
3	Принтер	Модель: HP LaserJet M127fw	2

		with Wi-Fi (CZ183A)	

Продовження табл. 2.2

1	2	3	4
4	Сервер	Patriot Tower E3-1220V3: Intel Xeon Quad-Core E3-1220 v3 (3.1 ГГц)/ 8 ГБ/ 2 x Seagate ST500NM0011 500 ГБ, 64 МБ, Constellation ES, Serial ATA 6 Гбіт/с	1
5	Wi-Fi роутер	Модель: TP-LINK TL-WR940N	1
6	Монітор	Модель: 23.8" LG 24MP58VQ-P	5
7	Ноутбук	Модель: Acer Aspire ES1-533-P2WF	5
8	Клавіатура	Модель: Roccat Isku USB (ROC-12-731)	5
9	Мишка	Модель: Asus Strix Claw (90YH00C1-BAUA00)	5
10	МФУ	Модель: Canon i-SENSYS MF4410	1

Таблиця 2.3 – Програмне забезпечення системи

№	Тип програмного забезпечення	Найменування

1	2	3
1	Операційна система	Windows 7

Продовження таблиці 2.3

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

2.2.2 Обстеження інформаційного середовища ПП «Астра-Дніпро»

Згідно з НД ТЗІ 1.6-005-2013: об’єкт інформаційної діяльності – інженерно-технічна споруда (приміщення), транспортний засіб, де здійснюється озвучення та/або обробка технічними засобами інформації з обмеженим доступом [14].

На підприємстві ПП «Астра-Дніпро» циркулює інформація з відкритим доступом та з обмеженим доступом (конфіденційна). Згідно закону України «Про інформацію»: конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних

осіб і поширюються за їх бажанням відповідно до передбачених ними умов [15].

Згідно з НД ТЗІ 1.1-003-99: конфіденційність інформації – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем [16].

На фірмі не має інформації, що становить державну таємницю.

Перелік інформації, яка циркулює на даному ОІД, наведений у таблиці 2.4

Таблиця 2.4 - Перелік інформації, що циркулює на ОІД.

№	Інформація	Режим доступу	Правовий режим	Вимоги
1	2	3	4	5
1	Організаційно - правові документи підприємства (статут, засновницький договір, структура і штатна чисельність, штатний розпис, посадові інструкції)	Інформація з обмеженим доступом	———	Цілісність і конфіденційність
2	Інформація про надання послуг, тарифи, контактна інформація	Інформація з відкритим доступом	Публічна інформація	Доступність, цілісність
3	Документи по особовому складу працівників підприємства, трудові контракти (договори), особисті справи, особисті картки ф. Т- 2, особові рахунки по зарплатні, трудові	Інформація з обмеженим доступом	Конфіденційна інформація	Цілісність і конфіденційність

	книжки)			

Продовження таблиці 2.4

1	2	3	4	5
4	Фінансово-бухгалтерські документи підприємства (головна книга, річні звіти, бухгалтерські баланси, рахунки прибутків і збитків, акти ревізій, інвентаризацій, плани, звіти, кошториси, рахунки, касові книги та ін.)	Інформація з обмеженим доступом	Конфіденційна інформація	Цілісність і конфіденційність
5	Інформація про постачальників та клієнтів	Інформація з обмеженим доступом	Конфіденційна інформація	Цілісність і конфіденційність
6	Відомості про плани підприємства (плани закупівель, поточні і перспективні плани роботи)	Інформація з обмеженим доступом	Конфіденційна інформація	Цілісність і конфіденційність
7	Інформація про кількість і наявність продукції на складі	Інформація з обмеженим доступом	_____	Доступність, цілісність

Згідно з НД ТЗІ 1.1-003-99: матриця доступу (access matrix) — n-мірна таблиця, вздовж кожного виміру якої відкладені ідентифікатори об’єктів КС

одного типу (об'єктів-користувачів, об'єктів-процесів чи пасивних об'єктів), і містить як елементи права доступу за кожним із типів доступу [16].

Матриця доступу співробітників підприємства до інформації з обмеженим доступом наведені у таблиці 2.5

Таблиця 2.5 – Матриця доступу до інформації.

№	Директор	Заступник директора	Бухгалтер	Системний адміністратор	Завідуючий складом	Співробітники Call – центру	Продавці
1	R,W,D	R,W	R,W	R,W	R	R	R
2	R,W,D	R,W	R,W	R,W	R	R	R
3	R,W,D	R,W	R,W	R,W	R	-	-
4	R,W,D	R,W	R,W,D	R,W	R	-	-
5	R,W,D	R,W	R	R,W	R	R,W	R,W
6	R,W,D	R,W	R	R,W	R	-	-
7	R,W,D	R,W,D	R	R,W	R,W,D	R,W	R,W

R – має право тільки читати, W – має право редагувати, D – має право видаляти.

2.2.3 Аналіз загроз інформації

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

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

Загроза інформації, що циркулює в інформаційній системі, залежить від її структури та конфігурації, технології оброблення інформації в ній, стану

навколишнього фізичного середовища, а також дій персоналу. Зазвичай загроза є наслідком наявності вразливих місць у захисті інформаційних систем. Носіями загроз безпеці інформації є джерела загроз. Всі джерела загроз безпеці інформації, що циркулює в корпоративній мережі можна розділити на три основні групи:

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

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

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

Внутрішні суб'єкти (джерела), як правило, представляють собою висококваліфікованих спеціалістів у галузі розробки та експлуатації програмного забезпечення та технічних засобів, які знайомі зі специфікою завдань, що вирішуються, структурою та основними функціями та принципами роботи програмно-апаратних засобів захисту інформації, та які мають можливість використання штатного обладнання та технічних засобів мереж. До них відносяться:

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

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

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

В якості критеріїв оцінки ступеню небезпеки виберемо:

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

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

Фатальність (К3) і - визначає ступінь непереборності наслідків реалізації загрози.

Кожний показник оцінюється від 1 до 5. Причому, 1 відповідає мінімальному обсязі впливу оцінюваного показника на небезпеку використання джерела, а 5 - максимальному.

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

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

Аналіз загроз наведена у таблиці 2.6

Таблиця 2.6 – Аналіз загроз

№	Джерело загрози	Вразливість	Загроза	Властивість інформації	К 1	К 2	К 3	К
1	2	3	4	5	6	7	8	9
Антропогенні								
1	Персонал підприємс	Вільний доступ співробітників	Перегляд інформації на	К	4	2	3	0.192

	тва	до чужих робочих місць	дисплеї співробітниками, які не допущені до обробки інформації з обмеженим доступом					

Продовження таблиці 2.6

1	2	3	4	5	6	7	8	9
2	Персонал підприємства	Відсутність зобов'язання про нерозголошення інформації	Розголошення інформації, модифікація, знищення співробітниками допущеними до її обробки	К,Ц, Д	4	3	3	0.288
3	Персонал підприємства (системний адміністратор)	Несвоєчасне оновлення системи антивірусного захисту	Модифікація інформації, знищення інформації	Ц	4	3	3	0.288
4	Внутрішні (персонал); Зовнішні (конкуренти, кримінальні структури, відвідувачі тощо)	Відсутність сигналізації	Крадіжка інформації, носіїв інформації	К,Ц, Д	3	3	3	0.216
5	Персонал підприємства	Необізнаність в питаннях безпеки	Помилки персоналу при роботі з інформацією	Ц	4	3	4	0.384
6	Персонал підприємства	Відсутність політики чистого столу	Втрата або пошкодження інформації	К,Ц, Д	4	3	4	0.384

Продовження таблиці 2.6

1	2	3	4	5	6	7	8	9
Техногенні (внутрішні)								
1	Зовнішні (засоби зв'язку, мережі інженерних комунікації). Внутрішні (неякісні технічні та програмні засоби обробки інформації)	Відсутність резервного копіювання	Втрата або модифікація інформації через вихід з ладу апаратно-програмних засобів	Ц	4	3	4	0.384
2		Неякісні апаратне та програмні засоби, кидки напруг.	Втрата або модифікація інформації через вихід з ладу апаратно-програмних засобів	Ц, Д	3	2	3	0.144
3		Нестабільне електропостачання.	Втрата або модифікація інформації через вихід з ладу апаратно-програмних засобів	Ц, Д	3	2	3	0.144
4		Дія на обладнання коливань напруги.	Втрата або модифікація інформації через вихід з ладу апаратно-програмних засобів	Ц, Д	2	3	2	0.096
Стихійні								
1	Пожежі			Ц, Д	2	2	2	0.064
2	Землетруси			Ц, Д	1	1	1	0.008
3	Підтоплення			Ц, Д	1	1	1	0.008

Згідно цієї таблиці можна зробити висновок, що найбільш значущими загрозами для підприємства ПП «Астра-Дніпро» є антропогенні загрози, а саме

втрата або пошкодження інформації через недостатню освіченість персоналу у сфері інформаційної безпеки та недотримання організаційних правил.

2.2.4 Модель порушника

Модель порушника – абстрактний формалізований або неформалізований опис порушника [9].

Порушники бувають внутрішні (ті, що працюють в організації) та зовнішні (наприклад, постачальники послуг).

Порушниками можуть бути:

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

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

За рівнем можливостей порушники поділяються на:

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

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

3 Можливість управління програмним забезпеченням АС.

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

За рівнем знань порушники поділяються на:

1 Не володіють інформацією про АС.

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

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

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

5 Володіють інформацією про функції та механізм дії засобів захисту.

За використовуваними методами і способами порушники поділяються на:

1 Використовують лише агентурні методи одержання інформації.

2 Використовують технічні засоби для перехоплення інформаційних сигналів.

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

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

За місцем дії порушники можуть класифікуватися як:

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

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

3 Мають доступ до робочих місць користувачів АС.

4 Мають доступ до місць накопичення і зберігання даних.

5 Мають доступ до засобів керування КСЗІ і до засобів адміністрування АС.

Після аналізу можливих порушників було складено модель порушника, яка наведена у таблиці 2.7

Таблиця 2.7 – Модель порушника

№	Порушник	За рівнем можливостей	За рівнем знань	За використовуваними методами і способами	За місцем дії
Внутрішні					
1	Директор	3	4	3	5
2	Заступник директора	2	4	3	4
3	Бухгалтер	2	4	3	4
4	Відділ продажу	1	2	3	3
5	Охоронці	1	1	2	2
6	Системний адміністратор	4	5	3	5
7	Завідуючий складом	1	3	3	3
8	Продавці	1	2	2	3
9	Прибиральниці	1	1	1	2
Зовнішні					
1	Відвідувачі	1	1	1	2
2	Конкуренти	1	1	1	2
3	Кримінальні структури	1	1	1	2
4	Персонал, що обслуговує комунікації	1	1	1	2
5	Постачальники товару	1	1	1	2

2.3 Аналіз ризиків

На основі аналізу загроз і моделі порушника було визначено можливі наслідки, які можуть виникнути внаслідок реалізації загроз, ймовірність реалізації загроз, величину збитків і ймовірні втрати.

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

Під час проведення аналізу ризику необхідно:

1 визначити види інформації, які можуть бути пошкоджені;

2 оцінити ймовірність реалізації загрози;

3 оцінити величину збитків;

4 визначити ймовірні наслідки:

- фінансові втрати
- зниження продуктивності праці
- неприємності для підприємства (які впливають на рівень суспільної довіри)

Таблиця 2.8 – Аналіз ризиків

№	Загроза	Інформація, яка може бути пошкоджена	Ймовірність реалізації загрози	Величина збитків	Ризик	Ймовірні наслідки
1	2	3	4	5	6	7
1	Перегляд інформації на дисплеї співробітниками, які не допущені до обробки	Організаційно - правові документи підприємства	Низька	Низька	Низький	Неприємності для підприємства

Продовження таблиці 2.8

1	2	3	4	5	6	7
1	Перегляд інформації на дисплеї співробітниками, які не допущені до обробки	Інформація про надання послуг, тарифи, контактна інформація	Низька	Відсутня	Низький	-
		Фінансово-бухгалтерські документи підприємства	Низька	Низька	Низький	Неприємності для підприємства
		Інформація про постачальників та клієнтів	Низька	Низька	Низький	Неприємності для підприємства
		Документи по особовому складу працівників підприємства	Низька	Середня	Низький	Зниження продуктивності праці, неприємності для підприємства
		Інформація про кількість і наявність продукції на складі	Низька	Відсутня	Низький	Неприємності для підприємства
		Відомості про плани підприємства	Низька	Низька	Низький	Неприємності для підприємства

Продовження табл. 2.8

1	2	3	4	5	6	7
2	Розголошення інформації, модифікація, знищення співробітниками допущеними до її обробки.	Організаційно - правові документи підприємства	Середня	Середня	Середній	Неприємності для підприємства
		Інформація про надання послуг, тарифи, контактна інформація	Середня	Висока	Середній	Фінансові втрати, неприємності для підприємства
		Фінансово-бухгалтерські документи підприємства	Середня	Висока	Середній	Фінансові втрати
		Інформація про постачальників та клієнтів	Висока	Висока	Високий	Фінансові втрати, неприємності для підприємства
		Документи по особовому складу працівників підприємства	Середня	Середня	Середній	Зниження продуктивності праці
		Інформація про кількість і наявність продукції на складі	Низька	Низька	Низький	Фінансові втрати, зниження продуктивності праці
		Відомості про плани підприємства	Середня	Середня	Середній	Зниження продуктивності праці

Продовження таблиці 2.8

1	2	3	4	5	6	7
3	Крадіжка інформації або носіїв інформації	Організаційно - правові документи підприємства	Низька	Низька	Низький	Неприємності для підприємства
		Інформація про надання послуг, тарифи, контактна інформація	Низька	Відсутня	Низький	-
		Фінансово-бухгалтерські документи підприємства	Середня	Висока	Середній	Фінансові втрати
		Інформація про постачальників та клієнтів	Середня	Середня	Середній	Фінансові втрати, неприємності для підприємства
		Інформація про кількість і наявність продукції на складі	Низька	Низька	Низький	Неприємності для підприємства
		Відомості про плани підприємства	Низька	Середня	Низький	Неприємності для організації

Продовження таблиці 2.8

1	2	3	4	5	6	7
4	Помилки персоналу при роботі з інформацією	Організаційно - правові документи підприємства	Низька	Низька	Низький	Зниження продуктивності праці
		Інформація про надання послуг, тарифи, контактна інформація	Низька	Середня	Низький	Фінансові втрати, неприємності для підприємства
		Фінансово-бухгалтерські документи підприємства	Середня	Висока	Середній	Фінансові втрати
		Інформація про постачальників та клієнтів	Середня	Середня	Середній	Фінансові втрати, зниження продуктивності праці, неприємності для підприємства
		Інформація про кількість і наявність продукції на складі	Низька	Низька	Низький	Зниження продуктивності праці
		Відомості про плани підприємства	Низька	Середня	Низький	Неприємності для підприємства

Продовження таблиці 2.8

1	2	3	4	5	6	7
5	Втрата або модифікація інформації через вихід з ладу апаратно-програмних засобів	Організаційно - правові документи підприємства	Низька	Середня	Низький	Зниження продуктивності праці
		Інформація про надання послуг, тарифи, контактна інформація	Низька	Висока	Середній	Фінансові втрати, неприємності для підприємства
		Фінансово-бухгалтерські документи підприємства	Низька	Висока	Середній	Фінансові втрати
		Інформація про постачальників та клієнтів	Низька	Середня	Низький	Фінансові втрати, зниження продуктивності праці, неприємності для підприємства
		Відомості про плани підприємства	Низька	Середня	Низький	Неприємності для підприємства
		Інформація про кількість і наявність продукції на складі	Низька	Середня	Низький	Зниження продуктивності праці
6	Стихійні лиха	Інформація з обмеженим доступом, інформація з відкритим доступом	Низька	Висока	Середній	Фінансові втрати, зниження продуктивності праці

У таблиці 2.8 проаналізовані ймовірність реалізації загроз і величини збитків, та вказані ймовірні наслідки, які можуть виникнути. Найбільш високий рівень ризику у таких загроз:

- розголошення інформації, модифікація, знищення співробітниками допущеними до її обробки;
- крадіжка інформації або носіїв інформації.

2.4 Необхідність створення комплексної системи захисту інформації

Згідно з НД ТЗІ 1.1-003-99: Комплексна система захисту інформації; КСЗІ — сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС [16].

Згідно з НД ТЗІ 1.1-005-07: Комплекс технічного захисту інформації (КТЗІ) – сукупність організаційних, інженерних і технічних заходів та засобів, призначених для захисту від витоку ІзОД технічними каналами на об’єктах інформаційної діяльності [17].

Згідно з НД ТЗІ 1.1-003-99: Політика безпеки (ПБ) – набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації [16].

Створення КСЗІ полягає у створенні комплексу організаційних та інженерно-технічних засобів захисту інформації. Створення КСЗІ в ІТС здійснюється відповідно до нормативного документа системи технічного захисту інформації НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі" на підставі технічного завдання (далі - ТЗ), розробленого згідно з вимогами нормативного документу системи технічного захисту інформації НД ТЗІ 3.7-001-99 "Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі".

На підприємстві ПП «Астра-Дніпро» обробляється і зберігається інформація з обмеженим доступом (конфіденційна інформація), а саме інформація про клієнтів та співробітників, відомості про плани підприємства, фінансово-бухгалтерські документи. Виток цієї інформації може призвести до погіршення становища

підприємства на ринку, погіршення фінансового положення, втрати клієнтської бази та інше. Для забезпечення захисту інформації від несанкціонованого доступу, втрати або пошкодження необхідна розробка КСЗІ.

На досліджуваному ОІД ПП «Астра-Дніпро» необхідно забезпечити:

- запобігання несанкціонованого доступу до конфіденційної інформації та ознайомлення з нею;
- запобігання втрати або пошкодження інформації через технічні відмови апаратури мережі, або помилок у програмному забезпеченні;
- запобігання втрати або пошкодження інформації через помилки персоналу;
- забезпечити контроль за виконання організаційних правил, вказаних у політиці безпеки;
- належне зберігання паперових носіїв інформації, для запобігання їх втрати або викрадання;
- запобігання застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів.

2.5 Профіль захищеності

Згідно з нормативними документами НД ТЗІ 2.5-004-99 і НД ТЗІ 2.5-005-99 потрібно визначити критерії захищеності даної АС. На ПП «Астра-Дніпро» АС належить до третього класу, та вимоги до захисту інформації - конфіденційність, цілісність та доступність. Отже обраний профіль має вигляд:

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 }

Результати попереднього обстеження ОІД наведені в таблиці 2.9

Таблиця 2.9 – Виконання критеріїв профілю

№	Позначення профілю	Значення	Виконання (+/-)
1	КД-2	Базова довірча конфіденційність	+
2	КО-1	Повторне використання об'єктів	-
3	КВ-1	Мінімальна конфіденційність при обміні	+
4	ЦД-1	Мінімальна довірча цілісність	+
5	ЦО-1	Обмежений відкат	-
6	ЦВ-1	Мінімальна цілісність при обміні	-
7	ДР-1	Квоти	+
8	ДВ-1	Ручне відновлення	+
9	НР-2	Захищений журнал	+
10	НИ-2	Одиночна ідентифікація і автентифікація	+
11	НК-1	Однонаправлений достовірний канал	+
12	НО-2	Розподіл обов'язків адміністраторів	-
13	НЦ-2	КЗЗ з гарантованою цілісністю	+
14	НТ-2	Самотестування при старті	+
15	НВ-1	Автентифікація вузла	-

2.5.1 Реалізація критеріїв профілю

1 КД-2. Базова довірча конфіденційність

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

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

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

Так як в системі всі користувачі мають свої права доступу до об’єктів та існує можливість встановлювати, які користувачі можуть активізувати конкретний процес можна зробити висновок, що ця послуга реалізується.

2 КО-1. Повторне використання об’єктів

Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

Тобто, після завершення роботи та виходу із облікового запису користувачі повинні закривати всі процеси. Ця умова не виконується, отже ця послуга не реалізована.

Задовольнити таку вимогу, функціонального профілю захищеності в ОС Microsoft Windows можна за допомогою спеціальних команд. Для того, щоб повністю впевнитися в недоступності процесів і результатів роботи іншим користувачам, можна скористатися командою taskkill, яка дозволяє завершити процес, який неможливо закрити за допомогою «Диспетчера задач».

3 КВ-1. Мінімальна конфіденційність при обміні

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище.

Ця послуга реалізується. В системі реалізується шифрування файлів перед їх передачею каналами зв'язку та шифрування файлів перед їх записуванням на диск.

4 ЦД-1. Мінімальна довірча цілісність

Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену.

В системі користувачі не мають доступ до облікових записів інших користувачів. Ця послуга реалізується завдяки авторизації користувачів в системі.

5 ЦО-1. Обмежений відкат

Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути захищений об'єкт до попереднього стану. Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

Реалізація цієї послуги дозволяє відновлюватися після збоїв програмного або апаратного забезпечення, а також після помилок користувачів. Тим самими забезпечує збереження цілісності інформації.

Ця послуга не реалізована в системі.

Для задоволення вимоги ЦО-1 функціонального профілю захищеності можна скористатися можливостями Windows або засобами резервного копіювання.

Наприклад, Пуск – Програми - Стандартні - Службові - Відновлення системи.

6 ЦВ-1. Мінімальна цілісність при обміні

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище.

Ця послуга не реалізована в системі.

Для задоволення вимоги ЦВ-1 функціонального профілю захищеності цінні документи при передачі через незахищене середовище повинні завірятися ЕЦП.

7 ДР-1. Квоти

Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Політика використання ресурсів повинна визначати обмеження, які

можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу.

В даній системі виділяється певний обсяг простору на жорсткому диску, тобто ця послуга реалізована.

8 ДВ-1. Ручне відновлення

Політика відновлення після збоїв, що реалізується КЗЗ, стосується: системного та функціонального програмного забезпечення; засобів захисту інформації та засобів управління КСЗІ; засобів адміністрування та управління обчислювальною системою АС – і гарантує повернення АС у відомий захищений стан після відмов або переривання обслуговування, спричинених помилковими діями користувачів.

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

Ця послуга реалізована.

9 НР-2. Захищений журнал

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

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

Адміністратори і користувачі, яким надані відповідні повноваження мають в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації. Ця послуга реалізована.

10 НИ-2. Одиночна ідентифікація і автентифікація

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача (фізичної особи), який намагається одержати доступ до КС. За результатами ідентифікації і автентифікації користувача система

(КЗЗ), по-перше, приймає рішення про те, чи дозволено даному користувачеві ввійти в систему.

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

11 НК-1. Однонаправлений достовірний канал

Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Дана послуга дозволяє гарантувати, що користувач взаємодіє безпосередньо з КЗЗ і ніякий інший користувач або процес не може втручатись у взаємодію (підслухати або модифікувати інформацію, що передається).

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

12 НО-2. Розподіл обов'язків адміністраторів

Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Умова не виконується, оскільки немає окремих адміністратора безпеки та системного адміністратора. Для задоволення вимоги НО-2 функціонального профілю захищеності було вирішено призначити заступника директора виконувати обов’язки менеджера з інформаційної безпеки.

13 НЦ-2. КЗЗ з гарантованою цілісністю

Дана послуга визначає міру спроможності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

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

Для рівня НЦ-2 необхідно, щоб КЗЗ підтримував власний домен виконання, відмінний від доменів виконання всіх інших процесів, захищаючи себе від зовнішніх впливів. Дана вимога є однією з вимог до реалізації

диспетчера доступу. Реалізація даної вимоги забезпечується можливостями апаратного забезпечення ОС.

14 НТ-2. Самотестування при старті

КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ.

Ця послуга реалізована.

15 НВ-1. Автентифікація вузла

КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму. Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

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

2.6 Розробка політики безпеки

1. Загальні положення

1.1 Метою політики безпеки є забезпечення захисту інформації на підприємстві ПП «Астра-Дніпро» від певних загроз на основі системи поглядів, основних принципів, практичних вимог і рекомендацій.

Політика розповсюджується на ПП «Астра-Дніпро» та всіх філіали. Політика обов'язкова для виконання усіма співробітниками, а також особами, що працюють з інформацією, що належить ПП «Астра-Дніпро», в рамках укладеного контракту.

Під забезпечення інформаційної безпеки або захисту інформації розуміється збереження її конфіденційності, цілісності та доступності. Конфіденційність інформації забезпечується в разі надання доступу до даного тільки авторизованим особам, цілісність - у разі введення в дані виключно

авторизованих змін, доступності - при забезпечення можливості отримання доступу до даних авторизованим особам у потрібне для них час.

1.2 При розробці політики безпеки враховані:

- види інформації, що обробляється, та технологія обробки інформації;
- особливості обчислювальної системи (технічних засобів та програмного забезпечення, що використовуються);
- фізичне середовище розташування ОІД;
- модель порушника;
- модель загроз інформації.

1.3 Предметом даного документа є:

- політика створення паролів;
- політика «чистого стола» та «чистого екрану»;
- політика використання електронної пошти;
- політика користування носіями інформації;
- політика доступу до місць зберігання носіїв з інформацією з обмеженим доступом;
- політика антивірусного захисту;
- обов'язки співробітників, допущених до конфіденційної інформації;
- обов'язки системного адміністратора;
- обов'язки користувачів;
- обов'язки менеджера з інформаційної безпеки.

2. Політика створення паролів

2.1 Огляд

Паролі є важливим компонентом інформаційної безпеки. Вони служать для захисту облікових записів користувачів. Погано сконструйований пароль може привести до компрометації окремих систем, даних або мережі.

2.2 Мета

Метою цих рекомендацій є забезпечення створення надійних паролів.

2.3 Сфера застування

Ця політика застосовується для всього підприємства і поширюється на всіх працівників.

2.4 Політика

- мінімально рекомендована довжина пароля - в межах від 12 до 14 символів;
- рекомендується генерувати випадкові паролі;
- рекомендується включати в пароль цифри і інші символи;
- рекомендується використовувати як прописні, так і малі літери;
- не використовувати у паролі персональну інформацію, пов'язану з власником пароля, наприклад, імена, номери телефону, дати народження, тощо;
- не використовувати службовий пароль на інших сайтах в особистих цілях.

3. Політика «чистого стола» та «чистого екрану»

3.1 Огляд

Політика чистого стола визначає, в якому вигляді співробітники повинні залишати свої робочі місця, коли вони залишають їх без нагляду або залишають офіс.

3.2 Мета

Метою даної політики є встановлення мінімальних вимог для підтримки «чистого столу» та «чистого екрану» - де знаходиться та обробляється інформація з обмеженим доступом.

3.3 Сфера застосування

Ця політика застосовується для всього підприємства і поширюється на всіх працівників.

3.4 Політика

- паперові та електронні носії інформації, коли вони не використовуються, зберігати в сейфах;
- персональні комп'ютери та принтери повинні бути вимкнені після закінчення роботи;

- надруковані документи з важливою або конфіденційною інформацією необхідно вилучати з принтерів негайно.

4. Політика використання електронної пошти

4.1 Огляд

Електронна пошта є основним засобом комунікації серед робітників підприємства. Політика збереження електронної пошти призначена для того, щоб визначити, яку інформацію слід надсилати чи отримувати.

4.2 Мета

Метою даної політики є визначення допустимого використання електронної
пошти на підприємстві.

4.3 Сфера застосування

Ця політика є частиною корпоративного управління компанії і поширюється
на всі корпоративні поштові системи.

4.4 Політика

Не використовувати електронну пошту:

- для відправлення конфіденційної інформації, якщо вона не зашифрована криптографічним ПО, яке дозволене для використання в компанії;
- для встановлення відносин із третіми сторонами, наприклад, для укладання контрактів на покупку або продаж, відправлення пропозицій про роботу або прайс-листів, якщо це не входить у ваші службові обов'язки;
- в особистих і благодійних цілях, не пов'язаних з бізнесом організації;
- для розсилки будь-яких підривних, неетичних, незаконних або інших неприпустимих матеріалів;
- для розсилки вірусів чи іншого зловмисного програмного забезпечення;

5. Політика користування носіями інформації

5.1 Огляд

Змінні носії використовується на підприємстві для збереження даних. Змінні

носії є додатковим шляхом розповсюдження шкідливого програмного забезпечення. Наслідки зараження вірусами змінних носіїв різні — починаючи від втрати інформації, її витоку і закінчуючи блокуванням роботи комп'ютера, інформаційної системи чи навіть втратою управління мережами спеціального зв'язку

5.2 Мета

Метою даної політики є визначення допустимого використання змінних носіїв на підприємстві.

5.3 Сфера застосування

Ця політика є частиною корпоративного управління компанії і поширюється

на всі змінні носії на яких є інформація з обмеженим доступом.

5.4 Політика

- завжди вчасно здійснювати оновлення баз антивірусної програми;
- після підключення носія інформації обов'язково перевірити його антивірусною програмою;
- відключити автозапуск змінних носіїв інформації;
- використовувати лише облікові носії інформації;
- не користуватися облікованими носіями в особистих цілях.

6. Політика доступу до місць зберігання носіїв з інформацією з обмеженим доступом.

6.1 Огляд

Політика призначена для забезпечення належного збереження носіїв інформації з обмеженим доступом.

6.2 Мета

Метою даної політики є встановлення вимог зберігання носіїв інформації з обмеженим доступом.

6.3 Сфера застосування

Ця політика застосовується для всього підприємства і поширюється на всіх працівників та місця зберігання носіїв інформації.

6.4 Політика

- сейфи повинні бути обліковані;
- документи або електронні носії, які містять інформацію з обмеженим доступом та документи, з відкритою інформацією повинні зберігатись окремо;
- не залишати без нагляду сейф або ключі від нього;
- необхідно завести журнал обліку ключів від сейфу;
- в разі втрати ключів необхідно написати пояснення щодо факту втрати, та змінити замок на сейфі.

7 Політика антивірусного захисту

7.1 Огляд

Ця політика визначає вимоги щодо захисту інформаційно-телекомунікаційної
інфраструктури ПП «Астра-Дніпро» від загроз інформаційної безпеки, причина виникнення яких пов'язана з розповсюдженням шкідливого програмного забезпечення.

7.2 Мета

Метою даної політики є встановлення вимог користування засобами антивірусного захисту.

7.3 Сфера застосування

Ця політика застосовується для всього підприємства і поширюється на керівників та співробітників ПП «Астра-Дніпро», що експлуатують та супроводжують ІС.

7.4 Політика

Системний адміністратор повинен:

- проводити моніторинг роботи антивірусних засобів захисту, та оперативно реагувати нам виникнення при цьому критичних ситуацій;
- контролювати своєчасне оновлювання антивірусного програмного забезпечення (оновлення баз проводити не рідше ніж один раз кожні 7 діб);

- оперативно взаємодіяти з користувачами АС у разі виникнення ситуацій, пов'язаних з антивірусним захистом;
- вести облік роботи антивірусних засобів захисту;

7 Обов’язки співробітників, допущених до конфіденційної інформації

Співробітникам, які допущені до конфіденційної інформації зобов’язані:

- не розголошувати конфіденційну інформацію ПП «Астра-Дніпро», і без згоди не використовувати її для власних потреб у період дії трудового договору, а також протягом трьох років після його закінчення;
- відшкодувати заподіяні збитки, якщо він винен у розголошенні конфіденційної інформації;
- передати ПП «Астра-Дніпро» при припиненні трудового договору матеріальні носії з конфіденційною інформацією;

Співробітникам, які допущені до конфіденційної інформації забороняється:

- вести переговори по конфіденційним питанням по незахищеним лініям зв'язку, запису та передачі даних (по мережам передачі даних загального користування, телефону, Інтернету та ін.);
- використовувати конфіденційну інформацію в службовій переписці, доповідях та виступах, в відкритих статтях та інших матеріалах, призначених для опублікування;
- робити без дозволу заступника директора відео зйомку, фото зйомку або звукозапис в приміщеннях, в яких оброблюється інформація з обмеженим доступом;

7. Обов’язки системного адміністратора

- встановлювати на сервери і робочі станції мережеве програмне забезпечення;
- консультувати співробітників з питань використання обчислювальної техніки й комп'ютерних інформаційних технологій;
- проводити комп'ютерні антивірусні заходи;

- усувати аварійні ситуації, пов'язані з ушкодженням програмного забезпечення й баз даних;
- організовувати тестування й навчання співробітників підприємства основам комп'ютерної грамотності й роботі із прикладними програмними засобами;
- проводити контроль за правильністю вибору, зберігання, своєчасній заміні паролів користувачів мережі;
- забезпечувати своєчасне копіювання і резервування даних;
- слідкувати за безпекою мережі в цілому;
- слідкувати за дотриманням правил політики безпеки;

8. Обов’язки користувачів

- знати правила роботи в системі і вжиті заходи щодо захисту ресурсів;
- при роботі на своїй робочій станції виконувати тільки службові завдання;
- перед початком роботи перевірити свої робочі папки на жорсткому магнітному диску, робочі дискети та CD-диски на відсутність вірусів за допомогою штатних засобів антивірусного захисту, переконатися в справності своєї робочої станції;
- при повідомленнях тестових програм про появу вірусів негайно припинити роботу, доповісти адміністратору мережі;
- при необхідності використання магнітних носіїв, що надійшли з інших підрозділів, установ, підприємств і організацій, перш за все, провести перевірку цих носіїв на відсутність вірусів;
- зберігати в таємниці свій індивідуальний пароль, періодично змінювати його і не повідомляти іншим особам;
- повідомляти системного адміністратора про збої роботи системи;

9. Обов’язки адміністратора безпеки (менеджера з інформаційної безпеки)

- організація експлуатації технічних і програмних засобів захисту інформації;

- поточний контроль роботи засобів і систем захисту інформації;
- контроль за роботою користувачів автоматизованих систем, виявлення та реєстрація спроб НСД до автоматизованим системам і об інформаційних ресурсів;
- підтримання системи в рамках обраної політики безпеки;
- забезпечення конфіденційності і цілісності даних;
- підготовка і збереження резервних копій даних, їх періодична перевірка і знищення;
- створення та підтримка в актуальному стані користувача облікових записів;
- відповідальність за інформаційну безпеку в компанії;
- відстеження інформації про уразливість системи та своєчасне вжиття заходів;
- періодичне практичне тестування захищеності системи;
- документування своєї роботи;
- усунення неполадок в системі.

2.7 Аналіз ризиків після впровадження політики безпеки

У таблиці 2.10 проаналізовані рівень ризику після впровадження політики безпеки. Отже, можна зробити висновок, що після впровадження інструкцій, які регламентують обов’язки співробітників, допущених до конфіденційної інформації зменшився рівень ризику у загрози: розголошення інформації, модифікація, знищення співробітниками допущеними до її обробки.

Після впровадження політики доступу до місць зберігання носіїв з інформацією з обмеженим доступом, політики «чистого стола» та «чистого екрану», політики користування носіями інформації зменшився рівень ризику у загрози – крадіжка інформації.

Таблиця 2.10 – Аналіз ризиків після впровадження політики безпеки

№	Загроза	Інформація, яка може бути пошкоджена	Ймовірність реалізації загрози	Величина збитків	Ризик	Ймовірні наслідки
1	Перегляд інформації на дисплеї співробітникам, які не допущені до обробки	Організаційно - правові документи підприємства	Низька	Низька	Низький	Неприємності для підприємства
		Інформація про надання послуг, тарифи, контактна інформація	Низька	-	Низький	-
		Фінансово-бухгалтерські документи підприємства	Низька	Низька	Низький	Неприємності для підприємства
		Інформація про постачальників та клієнтів	Низька	Низька	Низький	Неприємності для підприємства
		Документи по особовому складу працівників підприємства	Низька	Середня	Низький	Зниження продуктивності праці, неприємності для підприємства
		Інформація про кількість і наявність продукції на складі	Низька	Відсутня	Низький	Неприємності для підприємства

Продовження таблиці 2.10

1	2	3	4	5	6	7
		Відомості про плани підприємства	Низька	Низька	Низький	Неприємності для підприємства
2	Розголошення інформації, модифікація, знищення співробітниками допущеними до її обробки.	Організаційно - правові документи підприємства	Низька	Середня	Низький	Неприємності для підприємства
		Інформація про надання послуг, тарифи, контактна інформація	Низька	Висока	Середній	Фінансові втрати, неприємності для підприємства.
		Фінансово-бухгалтерські документи підприємства	Низька	Висока	Середній	Фінансові втрати
		Інформація про постачальників та клієнтів	Низька	Висока	Середній	Фінансові втрати, неприємності для підприємства.
		Документи по особовому складу працівників підприємства	Низька	Середня	Низький	Зниження продуктивності праці
		Інформація про кількість і наявність продукції на складі	Низька	Низька	Низький	Фінансові втрати, зниження продуктивності праці

Продовження таблиці 2.10

1	2	3	4	5	6	7
		Відомості про плани підприємства	Низький	Середня	Середній	Зниження продуктивності праці
3	Крадіжка інформації, носіїв інформації.	Організаційно - правові документи підприємства	Низька	Низька	Низький	Неприємності для підприємства
		Інформація про надання послуг, тарифи, контактна інформація	Низька	Відсутня	Низький	-
		Фінансово-бухгалтерські документи підприємства	Низький	Висока	Середній	Фінансові втрати
		Інформація про постачальників та клієнтів	Низький	Середня	Низький	Фінансові втрати, неприємності для підприємства
		Інформація про кількість і наявність продукції на складі	Низька	Низька	Низький	Неприємності для підприємства
		Відомості про плани підприємства	Низька	Середня	Низький	Неприємності для підприємства

Продовження таблиці 2.10

1	2	3	4	5	6	7
4	Помилки персоналу при роботі з інформацією.	Організаційно - правові документи підприємства	Низька	Низька	Низький	Зниження продуктивності праці
		Інформація про надання послуг, тарифи, контактна інформація	Низька	Середня	Низький	Фінансові втрати, неприємності для підприємства.
		Фінансово-бухгалтерські документи підприємства	Середня	Висока	Середній	Фінансові втрати
		Інформація про постачальників та клієнтів	Середня	Середня	Середній	Фінансові втрати, зниження продуктивності праці, неприємності для підприємства.
		Інформація про кількість і наявність продукції на складі	Низька	Низька	Низький	Зниження продуктивності праці
		Відомості про плани підприємства	Низька	Середня	Низький	Неприємності для підприємства

Продовження таблиці 2.10

1	2	3	4	5	6	7
5	Втрата або модифікація інформації через вихід з ладу апаратно-програмних засобів	Організаційно - правові документи підприємства	Низька	Середня	Низький	Зниження продуктивності праці
		Інформація про надання послуг, тарифи, контактна інформація	Низька	Висока	Середній	Фінансові втрати, неприємності для підприємства.
		Фінансово-бухгалтерські документи підприємства	Низька	Висока	Середній	Фінансові втрати
		Інформація про постачальників та клієнтів	Низька	Середня	Низький	Фінансові втрати, зниження продуктивності праці, неприємності для підприємства
		Відомості про плани підприємства	Низька	Середня	Низький	Неприємності для підприємства
		Інформація про кількість і наявність продукції на складі	Низька	Середня	Низький	Зниження продуктивності праці

Продовження таблиці 2.10

1	2	3	4	5	6	7
6	Стихійні лиха	Інформація з обмеженим доступом, інформація з відкритим доступом	Низька	Висока	Середній	Фінансові втрати, зниження продуктивності праці, неприємності для підприємства

2.8 Висновки до другого розділу

У даному розділі були зібрані дані про підприємство, виконане обстеження ОІД, обстеження інформаційного середовища та обстеження обчислювальної системи. На підставі зібраних даних була розроблена модель порушника і модель загроз, та зроблено аналіз ризиків. Визначено загрози з найбільш високим рівнем ризику:

- розголошення інформації, модифікація, знищення співробітниками допущеними до її обробки;
- крадіжка інформації або носіїв інформації.

Після чого був обраний профіль захищеності і розроблена політика безпеки. Після впровадження політики безпеки був ще раз проаналізований рівень ризиків, і було визначено, що він зменшився.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою виконання економічного розділу є техніко-економічне обґрунтування політики безпеки інформації приватного підприємства «Астра-Дніпро», яке займається оптовим та роздрібним продажем кави, чаю, та кавового обладнання через Інтернет-магазин та через магазин у місті, здійснюючи доставку продукції по всій території України.

Основою для визначення витрат на розробку політики безпеки інформації є концепція сукупної вартості володіння (Total Cost of Ownership), запропонована Gartner Group, де розраховуються фіксовані (капітальні) вкладення і поточні витрати, а також величини можливих збитків, які може отримати підприємство.

3.1 Розрахунок фіксованих (капітальних) витрат

Капітальні (фіксовані) витрати на проектування та впровадження політики безпеки інформації складають:

$$К = Кпр + Кзпз + Кпз + Каз + Кнавч + Кн , \quad (3.1)$$

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

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

Крп – вартість розробки політики безпеки інформації, тис. грн;

Каз – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

Кнавч – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн;

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

Розробку політики безпеки інформації для приватного підприємства «Астра-Дніпро» планується здійснювати без залучення для цього зовнішніх консультантів, тому Кпр=0 грн. Закупівлі апаратного забезпечення та допоміжних матеріалів не плануються, тому Каз=0.

Планується використання ліцензійного програмного забезпечення, вартість якого визначається на рік користування, тому ці витрати відображатимуться в експлуатаційних витратах.

Витрати на навчання технічних фахівців і обслуговуючого персоналу (Кнавч) складуть 4 тис. грн. Витрати на встановлення обладнання та налагодження системи інформаційної безпеки становлять (Кн) 3 тис. грн.

Витрати на розробку політики безпеки інформації Крп складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки Ззп і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації Змч.

Трудомісткість розробки політики безпеки інформації визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}, \text{ годин,} \qquad (3.2)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку політики безпеки інформації, $t_{тз}$=3 години;

$t_{в}$ – тривалість розробки концепції безпеки інформації у організації, $t_{в}$=5 годин;

$t_{а}$ – тривалість процесу аналізу ризиків, $t_{а}$=16 годин;

$t_{вз}$ – тривалість визначення вимог до заходів, методів та засобів захисту, $t_{вз}$=12 годин;

$t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації, $t_{озб}$=8 годин;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації, $t_{овр}$=8 годин

$t_д$ – тривалість документального оформлення політики безпеки, $t_д$=6 годин.

Отже,

$$t = 3 + 5 + 16 + 12 + 8 + 8 + 6 = 58 \text{ годин.}$$

Витрати на заробітну плату спеціаліста з інформаційної безпеки Ззп дорівнюватимуть Ззп = 58 * 93 = 5395 грн.

Середньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями складає 93 грн/годину, виходячи із заробітної плати 16000 грн/міс.

Вартість машинного часу для розробки політики безпеки інформації на ПК становить:

$$Змч = t * C_{мч} = 58 * 13,96 = 809,68 \text{ грн.}$$

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = 0,8 \cdot 10 \cdot 1,64 + \frac{2700 \cdot 0,5}{1920} + \frac{1300 \cdot 0,2}{1920} = 13,96 \text{ грн.}$$

Отже,

$$Крп = 5395 + 809,68 = 6204,68 \text{ грн.}$$

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

$$К = 4000 + 3000 + 6204,68 = 13204,68 \text{ грн.}$$

3.2 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \quad грн. \tag{3.3}$$

де $С_в$ - вартість відновлення й модернізації системи;

$С_к$ - витрати на керування системою в цілому;

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

Вартість ліцензійного програмного забезпечення на рік користування (табл. 3.1) визначає витрати на Upgrade-відновлення й модернізацію системи інформаційної безпеки ($С_в$).

Таблиця 3.1 - Вартість ліцензійного програмного забезпечення, грн/рік

№	Найменування	Ціна
1	ABC Backup Pro	безкоштовно
2	Avast Endpoint Security	1415 грн. для 1 ПК
3	AIDA64*	5800 грн.
Всього *Св*		7215 грн.

*AIDA64*Engineer - програмне забезпечення для діагностики і тестування, призначене для підприємств, ліцензія надається окремо для кожного фахівця

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

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.} \tag{3.4}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів становлять 4000 грн.

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

$$С_з = З_{осн} + З_{дод}, \text{ грн.} \quad (3.5)$$

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

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 16000 грн. Додаткова заробітна плата – 8% від основної заробітної плати. Отже,

$$С_з = 16000*12 + 16000*12*0,08= 207360 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2016 р. складає 22%.

$$С_{єв} = 207360*0,22 = 45619,2 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.}, \quad (3.6)$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=8,8 кВт);

Fр – річний фонд робочого часу системи інформаційної безпеки (Fр = 1920 год.);

Це – тариф на електроенергію, (Це = 1,64 грн./кВт за годину).

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

$$С_{ел} = 8,8*1920*1,64 = 27709,44 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 2% ($С_{тос}$ = 13204,68 *0,02= 264,09 грн).

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

$$С_к = 4000 + 207360 + 45619,2 + 27709,44 + 264,09 = 284952,73 \text{ грн.}$$

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

$$С = 7215 + 284952,73 = 292167,73 \text{ грн.}$$

3.3 Оцінка можливого збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

Необхідні вихідні дані для розрахунку:

tп – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 4 години;

tв – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

tви – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 10 годин;

Зо – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 7000 грн./міс.;

Зс – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 9000 грн./міс.;

Чо – чисельність обслуговуючого персоналу (адміністраторів та ін.), 5 осіб.;

Чс – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 60 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 1,5 млн. грн. у рік;

Пзч – вартість заміни встаткування або запасних частин, грн;

I – число атакованих сегментів корпоративної мережі, 5;

N – середнє число атак на рік, 30.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = Пп + Пв + V, \qquad (3.7)$$

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

Пв – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

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

$$П_П = \frac{\sum Зс}{F} \cdot t_n = \frac{7000 \cdot 60}{176} \cdot 4 = 9545{,}45 \text{ грн},$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

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

$$Пв = Пви + Ппв + Пзч,$$

де Пви – витрати на повторне уведення інформації, грн.;

Ппв – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

Пзч – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації Пви розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі Зс, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу тви:

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви} = \frac{7000 \cdot 60}{176} \cdot 10 = 23863{,}64 \text{ грн.}$$

Витрати на відновлення сегмента корпоративної мережі Ппв визначаються часом відновлення після атаки тв і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_{в} = \frac{9000 \cdot 5}{176} \cdot 2 = 511{,}36 \text{ грн.}$$

$$Пв = 23863{,}64 + 511{,}36 = 24375 \text{ грн.}$$

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{O}{Fг} \cdot (t_{п} + t_{в} + t_{ви})$$

$$V = \frac{1350000}{2080} \cdot (4 + 2 + 10) = 10384{,}62 \text{ грн.}$$

де Fг – річний фонд часу роботи філії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

$$U = 9545{,}45 + 24375 + 10384{,}62 = 44305{,}07 \text{ грн.}$$

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

$$B = \sum_i \sum_n U = \sum_5 \sum_{30} 44305{,}07 = 6645760{,}5 \text{ грн.}$$

3.4 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C \text{ грн.},$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (18,8%);

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

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

$$E = 6645760{,}5*0{,}188 - 292167{,}73 = 957235{,}24 \text{ грн.}$$

3.5 Визначення та аналіз показників економічної ефективності розробки політики інформаційної безпеки

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

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

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

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

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{957235{,}24}{13204{,}68} = 72{,}49, \quad \text{частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$\text{ROSI} > (\text{Nдеп} - \text{Nінф})/100),$$

де Nдеп – річна депозитна ставка, (19 %);

Nінф – річний рівень інфляції, (11%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$72,49 > (19 - 11)/100 = 72,49 > 0,08.$$

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{72,49} = 0,014, \text{ років.}$$

3.6 Висновок

Відповідно до проведених розрахунків можна зробити висновок, що для приватного підприємства «Астра-Дніпро» розробка політики безпеки інформації є економічно доцільною, оскільки коефіцієнт повернення інвестицій ROSI складає 72,49 грн. (тобто на кожну вкладену гривню в розробку політики інформаційної безпеки підприємство «Астра-Дніпро» матиме 72,49 грн. економічного ефекту). Термін окупності при цьому складе 0,014 років.

ВИСНОВКИ

У дипломній роботі була розроблена політика безпеки підприємства ПП «Астра-Дніпро».

Наведена актуальність захисту інформації на комерційних підприємствах. Також проведений аналіз нормативно-правової бази у сфері захисту інформації.

Були зібрані дані про підприємство, виконане обстеження ОІД, обстеження інформаційного середовища та обстеження обчислювальної системи.

На підставі зібраних даних була розроблена модель порушника і модель загроз, та зроблено аналіз ризиків. Визначено загрози з найбільш високим рівнем ризику:

- розголошення інформації, модифікація, знищення співробітниками допущеними до її обробки;
- крадіжка інформації або носіїв інформації.

Обраний профіль захищеності і розроблена політика безпеки. Після впровадження політики безпеки був ще раз проаналізований рівень ризиків, і було визначено, що він зменшився.

СПИСОК ЛІТЕРАТУРИ

1 Цивільний Кодекс України - Стаття 505.

2 Закон України «Про доступ до публічної інформації» - Стаття 7.

3 ISO/IEC TR 18044:2004 «Менеджмент інцидентів інформаційної безпеки».

4 ISO/IEC 27000. Менеджмент информационной безопасности.

5 Кримінальний Кодекс України - Стаття 231.

6 Кримінальний Кодекс України - Стаття 232.

7 Кримінальний Кодекс України, ст. 362.

8 Адміністративний Кодекс України, ст.212.

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

10 Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".

11 Закон України «Про державну таємницю».

12 Закон України «Про захист персональних даних».

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

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

15 Закон України «Про інформацію».

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

17 НД ТЗІ 1.1-005-07 «Захист інформації на об’єктах інформаційної діяльності. Створення комплексу ТЗІ. Основні положення».

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

ДОДАТОК А. Відомість матеріалів дипломної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	16	
6	А4	2 Розділ	46	
7	А4	3 Розділ	11	
8	А4	Висновки	1	
9	А4	Список літератури	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	1	
15	А4	Додаток Е	4	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

16 Додаток Д.doc

17 Додаток Е.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на дипломну роботу бакалавра на тему:

Розробка політики безпеки інформації інформаційно-телекомунікаційної системи приватного підприємства "Астра-Дніпро"

студента групи УБіт-15-1

Браун Вікторії Сергіївни

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

Об’єкт розробки: інформаційно-телекомунікаційна система ПП "Астра-Дніпро".

Предмет дослідження: політика безпеки інформації об’єкта інформаційної діяльності.

Мета дипломного проекту: розробка політики безпеки для підприємства ПП "Астра-Дніпро.

В роботі виконане обстеження ОІД, обстеження інформаційного середовища та обстеження обчислювальної системи.

На підставі зібраних даних була розроблена модель порушника і модель загроз, та зроблено аналіз ризиків.

Після чого був обраний профіль захищеності і розроблена політика безпеки. Після впровадження політики безпеки був ще раз проаналізований рівень ризиків, і було визначено, що він зменшився.

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

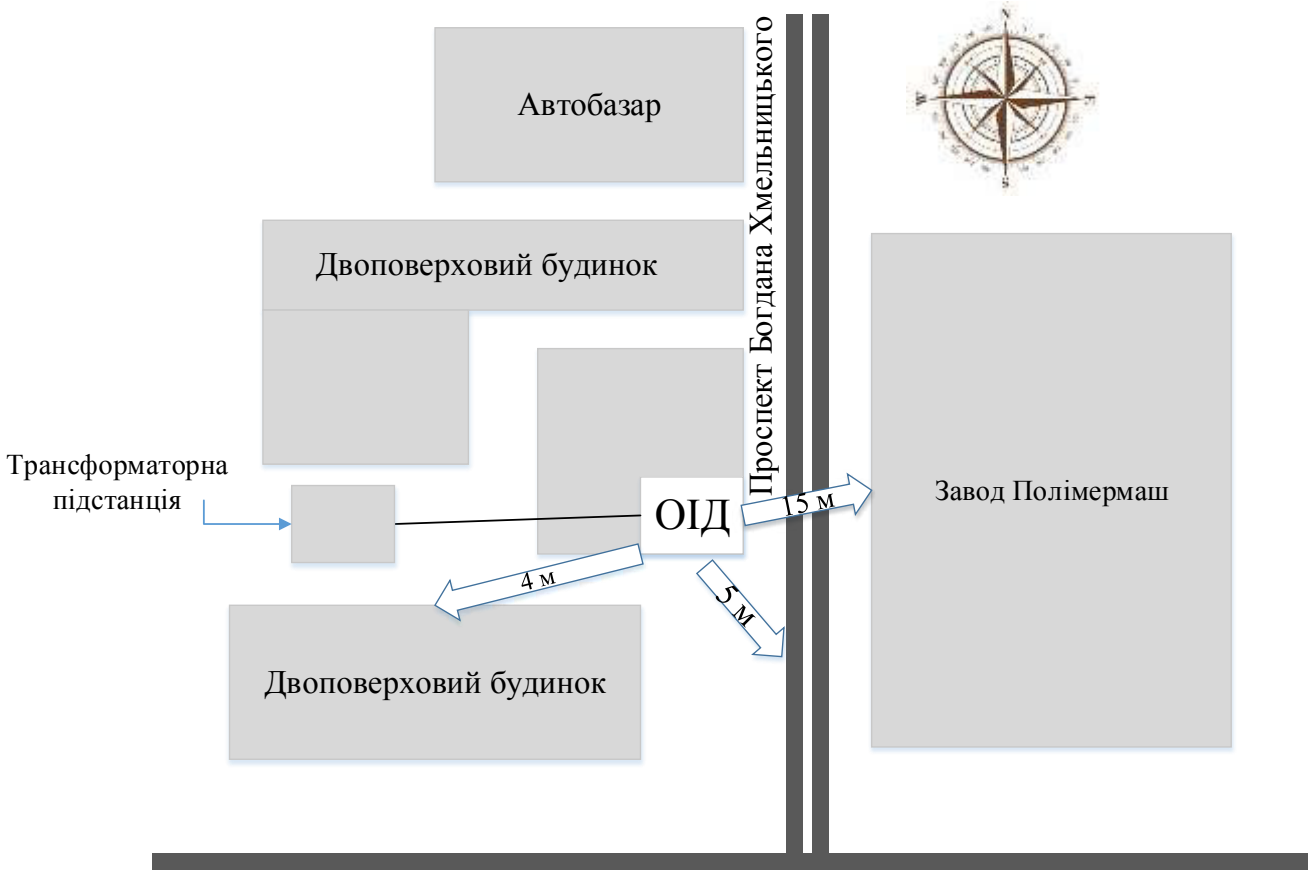
Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

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

Керівник дипломної роботи,
д.ф.-м.н., проф. Т.С. Кагадій

Керівник спец. розділу
ас. О.В. Чебаненко

ДОДАТОК Д. Ситуаційний план



ДОДАТОК Е

Наказ про створення комісії для проведення обстеження ОІД

ПП «Астра-Дніпро»

Місцезнаходження: м. Дніпро, вул. Богдана Хмельницького 152.

НАКАЗ

«15» січня 2019 р. м. Дніпро

Про створення комісії для
проведення обстеження
приміщення ОІД

НАКАЗУЮ:

1 Створити комісію для проведення обстеження приміщень ПП Астра-Дніпро, які знаходяться м. Дніпро, вул. Богдана Хмельницького 152., у складі:

Голова комісії: заступник директора організації;

Члени комісії: системний адміністратор.

2 Комісії, на чолі з головою, провести обстеження приміщень ПП Астра-Дніпро.

У ході обстеження необхідно:

- провести аналіз умов функціонування підприємства, його розташування на місцевості (ситуаційного плану) для визначення можливих джерел загроз;
- дослідити засоби забезпечення ІД, які мають вихід за межі контрольованої території;

- вивчити схеми засобів і систем життєзабезпечення підприємства (електроживлення, заземлення, автоматизації, пожежної та охоронної сигналізації), а також інженерних комунікацій та металоконструкцій;

- інформаційні потоки, технологічні процеси передачі, одержання, використання, розповсюдження і зберігання (далі - оброблення) інформації і провести необхідні вимірювання;

- визначити наявність та технічний стан засобів забезпечення ТЗІ;

- перевірити наявність на підприємстві нормативних документів, які забезпечують функціонування системи захисту інформації, організацію проектування будівельних робіт з урахуванням вимог ТЗІ, а також нормативної та експлуатаційної документації, яка забезпечує ІД;

- виявити наявність транзитних, незадіяних (повітряних, настінних, зовнішніх та закладених у каналізацію) кабелів, кіл і проводів;

- визначити технічні засоби і системи, застосування яких не обґрунтовано службовою чи виробничою необхідністю і які підлягають демонтуванню.

3 Термін виконання: «15» лютого 2019 р.

4 Результати діяльності комісії представити у вигляді актів.

5 Термін виконання: «13» лютого 2019 р.

6 Відповідальність за виконання акту обстеження покласти на голову робочої групи: заступника директора ПП «Астра-Дніпро»

7 Контроль за виконанням проведення обстеження покласти на системного адміністратора ПП «Астра-Дніпро»

8 Відповідальність за діяльність комісії залишаю за собою.

Директор

Наказ на створення служби захисту інформації (СЗІ)

ПП «Астра-Дніпро»

Місцезнаходження: м. Дніпро, вул. Богдана Хмельницького 152.

НАКАЗ

«20» січня 2019 р. м. Дніпро

На створення служби
захисту інформації СЗІ

НАКАЗУЮ:

1. Створити СЗІ згідно «НД ТЗІ 1.4-001-2000» та «НД ТЗІ 3.7-003-2005» для забезпечення завдань керування комплексною системою захисту інформації (КСЗІ) в АС та здійснення контролю за її функціонуванням та станом захищеності інформації в АС.

2. Призначити відповідальними системного адміністратора та заступника директора за створення служби захисту інформації (СЗІ) ПП «Астра-Дніпро» Відповідальні особи повинні узгоджувати всі прийняті рішенні щодо СЗІ з директором товариства з обмеженою відповідальністю ПП «Астра-Дніпро».

Директор

Наказ на створення комплексної системи захисту інформації (КСЗІ)

ПП «Астра-Дніпро»

Місцезнаходження: м. Дніпро, вул. Богдана Хмельницького 152.

НАКАЗ

«25» січня 2019 р. м. Дніпро

На створення комплексної
системи захисту інформації (КСЗІ)

НАКАЗУЮ:

1 Створити КСЗІ згідно «НД ТЗІ 3.7-003-05» та «НД ТЗІ 3.1-001-07» для забезпечення безпеки інформації під час її обробки в АС. Потрібно здійснити комплекс взаємоузгоджених заходів, спрямованих на розроблення і впровадження інформаційної технології, яка забезпечує обробку інформації в ІТС згідно з вимогами, встановленими нормативно-правовими актами та НД у сфері захисту інформації.

2 Призначити відповідальними системного адміністратора та заступника директора за створення служби захисту інформації (СЗІ) ПП «Астра-Дніпро». Відповідальні особи повинні узгоджувати кожну всі прийняті рішенні щодо СЗІ з директором ПП «Астра-Дніпро».

Директор