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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Сидоренка Даніїла Олександровича*

академічної групи *125-20-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка політики безпеки інформації інформаційно-комунікаційної системи відділу статистики Дніпровської районної державної адміністрації*

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

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2024

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту ***Сидоренку Д.О.*** **академічної групи** ***125-20-2***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Розробка політики безпеки інформації інформаційно-комунікаційної системи відділу статистики Дніпровської районної державної адміністрації***

Затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № _____

Розділ	Зміст	Термін виконання
1	Аналіз законодавства в сфері захисту інформації.	26.05.2024
2	Обстеження ОІД підприємства, розробка моделі загроз, порушника та аналіз ризиків. Розробка політики безпеки інформації, вибір профілю захищеності.	19.06.2024
3	Розрахунок річних витрат на розробку політики безпеки, оцінка величини збитку. Розрахунок ефективності запропонованої політики безпеки інформації.	26.06.2024

Завдання видано _____ Корнієнко В.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 06.05.2024

Дата подання до екзаменаційної комісії: 01.07.2024

Прийнято до виконання _____ Сидоренко Д.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка містить 87 сторінок, 4 рисунки, 14 таблиць, 4 додатки, 10 джерел.

Об'єкт розробки: політика безпеки інформації інформаційно-комунікаційної системи відділу статистики Дніпровської районної державної адміністрації.

Мета роботи: на підставі чинних законодавчих і нормативних документів України розробити політику безпеки інформації інформаційно-комунікаційної системи відділу статистики Дніпровської районної державної адміністрації.

В даній кваліфікаційній роботі дана характеристика об'єкта захисту та існуючої системи безпеки. детально проаналізовано нормативно-правову базу України у сфері захисту інформації. Було обрано основні нормативні документи щодо захисту статистичної інформації. Було визначено основні задачі щодо забезпечення конфіденційності статистичних даних.

У спеціальній частині було проведено детальне обстеження об’єкта інформаційної діяльності, наведено детальну класифікацію щодо циркулюючої інформації та визначені основні загрози, а також розроблено інструкції щодо захисту статистичної інформації.

В економічному розділі визначені витрати на розробку і впровадження системи захисту інформації, та аналіз її економічної ефективності.

Практичне значення роботи полягає в підвищенні рівня захищеності статистичної інформації, що циркулює у відділі статистики Дніпровської районної державної адміністрації.

КАТЕГОРІЮВАННЯ, АНАЛІЗ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, АНАЛІЗ РИЗИКІВ, НЕСАНКЦІОНОВАНИЙ ДОСТУП, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ФУНКЦІОНАЛЬНІЙ ПРОФІЛЬ ЗАХИЩЕНОСТІ.

ABSTRACT

The explanatory note consists of 87 pages, 4 images, 14 tables, 4 appendices, 10 sources.

Object of development: information security policy of the information and communication system of the statistics department of the Dnipro regional state administration.

The purpose of work: to develop the information security policy of the information and communication system of the statistics department of the Dnipro regional state administration on the base of existing standard documents of Ukraine.

This qualification work describes the protection object and the existing security system. the normative and legal framework of Ukraine in the field of information protection is analyzed in detail. The main normative documents on the protection of statistical information were selected. The main tasks for ensuring the confidentiality of statistical data were defined.

In the special part, a detailed survey of the object of information activity was carried out, a detailed classification of circulating information was given and the main threats were identified, as well as instructions for the protection of statistical information were developed.

Economic part includes determination of expenses for development and implementation of information security system and analysis for its economic efficiency.

Practical significance of the work consists in the increasing of the level of defense of statistical information circulating at the statistics department of the Dnipro regional state administration.

CATEGORIZATION, THREAT ANALYSIS, INTRUDER MODEL, RISK ANALYSIS, UNAUTHORIZED ACCESS, OBJECT OF INFORMATION ACTIVITY, INFORMATION SECURITY POLICY, FUNCTIONAL PROFILE OF SECURITY.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

Д – доступність;

ДТЗС – допоміжні технічні засоби і системи;

ІзОД – інформація з обмеженим доступом;

ІКС – інформаційно–комунікаційна система;

К – конфіденційність;

КЗ – контрольована зона;

КЗЗ – комплекс засобів захисту;

КМ – комп'ютерні мережі;

КС – комп'ютерна система;

КСЗІ – комплексна система захисту інформації;

МНІ – машинні носії інформації;

НСД – несанкціонований доступ;

ОІД – об'єкт інформаційної діяльності;

ОС – операційна система;

ПЗ – програмне забезпечення;

ПК – персональний комп'ютер;

СУБД – система управління базами даних;

ТЗПІ – технічні засоби обробки і передачі інформації;

Ц – цілісність.

ЗМІСТ

ВСТУП

Актуальність проблеми захисту інформації сьогодні не викликає сумнівів. Адже у світі технологічних та технічних інновацій інформація грає неабияку роль. Успіх та досягнення сучасних компаній і їх розвиток в умовах гострої конкуренції в значній мірі залежать від застосування інформаційних технологій, а отже, від ступеня забезпечення інформаційної безпеки.

У сучасному бізнесі найціннішим товаром є інформація. Для того, щоб мати успішний бізнес, забезпечити економічну безпеку, уникнути банкрутства, захистити себе і свою компанію від недобросовісної конкуренції і комерційного шпигунства, попередити рейдерські атаки, необхідно, передусім, захистити інформацію, якою ми володіємо. Будь-яке підприємство має в своєму розпорядженні різними видами інформації, котрі представляють інтерес для зловмисників. Інформація та інформаційні системи підприємств, мережеве оточення, у яких вони функціонують, є невід'ємними складовими сучасного бізнес середовища. Їх доступність, цілісність і конфіденційність можуть мати вирішальне значення для забезпечення конкурентоспроможності підприємства, руху коштів, рентабельності, відповідності правовим нормам і стандартам. Водночас, унаслідок посилення залежності підприємств від інформаційних, комунікаційних систем і сервісів вони стають вразливішими до порушень режиму безпеки. Порушення режиму безпеки інформаційних систем може істотно ускладнити реалізацію виробничих завдань, тому захист інформації від неправомірного оволодіння нею відводиться дуже значне місце. При цьому цілями захисту інформації є: запобігання розголошення, витоку і несанкціонованого доступу до охоронюваним відомостями; запобігання протиправних дій по знищенню, модифікації, спотворення, копіювання, блокування інформації; запобігання інших форм незаконного втручання в інформаційні ресурси та інформаційні системи; забезпечення правового режиму документованої інформації як об'єкта власності; захист конституційних прав громадян на збереження особистої таємниці та конфіденційності персональних даних, наявних в інформаційних системах; збереження державної таємниці,

конфіденційності документованої інформації у відповідність із законодавством; забезпечення прав суб'єктів в інформаційних процесах при розробці, виробництві та застосуванні інформаційних систем, технології та засобів їх забезпечення.

Відтак, захист інформації є складником загальної соціально-економічної безпеки підприємства, а інформаційна безпека - досить багатогранна проблема, яка охоплює не тільки визначення необхідності захисту інформації, але і те, як її захищати, від чого захищати, коли захищати, ніж захищати і якою має бути цей захист.

Кожне підприємство повинне усвідомити необхідність підтримання відповідного режиму безпеки та виділення на ці цілі значних ресурсів.

Політика інформаційної безпеки - звід документів, в яких розглядаються питання організації, стратегії, методів і процедур щодо конфіденційності, цілісності та доступності інформаційних ресурсів підприємства. Політика безпеки будується на основі аналізу ризиків - процесу визначення загроз безпеки системи і окремих її компонентів, визначення їх характеристик і потенційного збитку. Кінцева мета розробки політики інформаційної безпеки - забезпечити цілісність, доступність і конфіденційність для кожного інформаційного ресурсу.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Інформаційні технології охоплюють методи збору, обробки, перетворення, зберігання і розподілу інформації. У цей час інформаційно-ділова активність людства зміщається в область кібернетичного простору. Інформаційні процеси, що проходять повсюдно у світі, висувають на перший план, поряд із задачами ефективного опрацювання і передача інформації, найважливішу задачу забезпечення безпеки інформації. Це пояснюється особливою значимістю для розвитку держави його інформаційних ресурсів, зростанням вартості інформації в умовах ринку, її високою уразливістю і нерідко значним збитком у результаті її несанкціонованого використання.

У багатьох країнах порушення безпеки в системах опрацювання і передачі інформації приносять великі втрати. Вони найбільше значні в системах телекомунікацій, що обслуговують банківські і торгові заснування. У США, наприклад, збитки від несанкціонованого проникнення в ці системи оцінюються в десятки мільйонів доларів.

Про ступінь небезпеки електронних злочинів можна судити по тим витратам на засоби захисту, що рахуються припустимими і доцільними. Наслідки від несанкціонованого одержання інформації мають самий різноманітний масштаб: від необразливої прокази до фінансових утрат великих розмірів.

Найбільше вразливими об’єктами, що страждають від несанкціонованого доступу до даного, є системи автоматизованого перерахування коштів. Останнім часом також різко почастішали випадки розкрадання програм у комп’ютерних мережах. Ці розкрадання прийняли характер епідемії: на кожну законну копію програми, що має скільки-небудь широке поширення, існує декілька копій, отриманих незаконним шляхом. Оскільки основний інформаційний обмін оснований на інформаційній технології, то важливою умовою безпеки стає безпека в комп’ютерних мережах (КМ). Порушення цієї безпеки називають комп’ютерним злочином.

Перерахуємо основні загрози для КМ:

- читання інформації (порушення конфіденційності);
- порушення цілісності (інтегральності) інформації;
- блокування доступу до об'єктів і ресурсів КМ.

Загрози діляться на пасивні і активні. До пасивних загроз відноситься підслуховування (зчитування) інформації та аналіз трафіка (ідентифікація користувачів і визначення інтенсивності інформаційного обміну). До активних загроз відноситься модифікація даних, створення фальшивих даних під чужим ім'ям, введення вірусів і програмних закладок, блокування доступу до ресурсів КМ.

Основні можливі місця вторгнення в комп'ютерну мережу це:

- термінали (монітори, принтери, клавіатура, пульти, телефонні апарати);
- комутатори у вузлах КМ;
- лінії зв'язку (модеми, підсилювачі, ретранслятори);
- комп'ютерні процесори;
- файли на різноманітних носіях;
- додаткові плати, карти;
- пластикові карти;
- бази даних.

Зауважимо, що протяжність комп'ютерної мережі призводить до її значної вразливості і до трудності відслідковування комп'ютерних злочинів. Комп'ютерні злочини можуть відбуватися в органах державного і регіонального керування, на оборонних і інших державних підприємствах, у комерційних і промислових структурах. Основними групами правопорушників є: хакери (hackers), крейкери (creakers), терористи й екстремісти, а також комерційні підприємства, що ведуть промислове шпигунство. Ціллю захисту інформації є запобігання приведення до виконання перерахованих вище загроз.

В обчислювальних машинах є велике число можливостей для несанкціонованого доступу до інформації. Ніякий окремо взятий спосіб захисту не може забезпечити адекватну безпеку. Надійний захист може бути гарантований

лише при створенні механізму комплексного забезпечення безпеки як засобів опрацювання інформації, так і каналів зв'язку .

Технічні засоби являють собою електричні, механічні, електромеханічні або електронні пристрої. Вся сукупність технічних засобів ділиться на фізичні й апаратні. Фізичні засоби реалізуються у виді автономних пристроїв і систем і виконують функції загального захисту об'єктів, на яких опрацьовується інформація. До них ставляться, наприклад, устрої захисту територій і будинків, замки на дверях, де розміщені апаратура, грати на вікнах, електронно-механічне устаткування охоронної сигналізації. Під апаратними технічними засобами прийнято розуміти пристрої, що вбудовуються безпосередньо в обчислювальну техніку, у телекомунікаційну апаратуру, або пристрої, що працюють з подібною апаратурою по стандартному інтерфейсу. З найбільше відомих апаратних засобів можна відзначити схеми контролю інформації з парності, схеми захисту масивів пам'яті по ключу та ін.

Програмні засоби являють собою програмне забезпечення, спеціально призначене для виконання функцій захисту інформації.

Організаційні засоби захисту подають собою організаційно-технічні й організаційно-правові заходи, здійснювані в процесі створення й експлуатації апаратури телекомунікацій для забезпечення захисту інформації. Організаційні заходи охоплюють усі структурні елементи апаратури на всіх етапах їхнього життєвого циклу (будівництво помешкань, проектування системи, монтаж і наладка устаткування, іспити й експлуатація).

Морально-етичні засоби захисту реалізуються у вигляді всіляких норм, що склалися традиційно в даній країні або товаристві. Ці норми здебільшого не є обов'язковими, як законодавчі міри, проте їхнє недотримання веде звичайно до втрати авторитету і престижу співробітника.

Законодавчі засоби захисту визначаються законодавчими актами країни, які регламентують правила використання, опрацювання і передачі інформації обмеженого доступу і встановлюють міри відповідальності за порушення цих правил.

Політика Держстату у сфері захисту конфіденційної статистичної інформації визначається відповідно до Основних принципів офіційної статистики, схвалених Європейською економічною комісією ООН у 1992 році, Регламенту (ЄС) N 223/2009 Європейського парламенту та Ради Європи від 11 березня 2009 року щодо Європейської статистики, Декларації професійної етики, прийнятої Міжнародним статистичним інститутом у 2010 році, Законів України «Про державну статистику», «Про інформацію», «Про доступ до публічної інформації» і «Про захист персональних даних» та Принципів діяльності органів державної статистики, гармонізованих з Кодексом діяльності європейської статистики.

Політика Держстату у сфері захисту конфіденційної статистичної інформації полягає в забезпеченні встановлених законодавством гарантій захисту первинних даних, отриманих органами державної статистики від респондентів (як від юридичних, так і від фізичних осіб) у ході проведення державних статистичних спостережень, статистичної інформації, на підставі якої можна визначити інформацію щодо конкретного респондента, і адміністративних даних щодо респондентів, які використовуються для статистичних цілей. Ці дані є конфіденційною інформацією, яка охороняється законом.

Політика Держстату у сфері захисту конфіденційної статистичної інформації ґрунтується на системно узгоджених принципах, які визначають засади державної статистичної діяльності у зазначеній сфері:

- законність і верховенство права;
- відкритість і прозорість діяльності;
- партнерство у відносинах з респондентами та користувачами статистичної інформації;
- відповідальність працівників органів державної статистики у сфері захисту конфіденційної статистичної інформації.

Держстат реалізує політику захисту конфіденційної статистичної інформації шляхом:

- розроблення відповідних нормативно-правових актів і сприяння їхньому прийняттю, а також безумовного дотримання норм законодавства, що регулюють відносини у цій сфері;
- розроблення й оприлюднення методологічної та методичної документації щодо захисту конфіденційної статистичної інформації;
- використання сучасних інформаційних технологій, технічних і програмних засобів для комплексної системи захисту інформації;
- формування корпоративної етики та культури працівників органів державної статистики, вжиття необхідних організаційних заходів, які забезпечують захист конфіденційної статистичної інформації;
- навчання працівників органів державної статистики методам і процедурам захисту конфіденційної статистичної інформації;
- установлення правових зобов'язань працівників органів державної статистики щодо захисту конфіденційної статистичної інформації та контролю дотримання ними процедур доступу до такої інформації;
- проведення роз'яснювальної роботи з респондентами державних статистичних спостережень та користувачами даних щодо захисту конфіденційної статистичної інформації;
- упровадження міжнародних стандартів та використання найкращого досвіду статистичних служб інших країн у сфері захисту конфіденційної статистичної інформації.

Органи державної статистики гарантують конфіденційність первинних статистичних даних, отриманих від респондентів, а також статистичної інформації, на підставі якої можна визначити інформацію щодо конкретного респондента, і адміністративних даних, що використовуються для статистичних цілей. У Головному управлінні статистики в Дніпропетровській області циркулює велика кількість інформації конфіденційного характеру, доступ до якої необхідно обмежити. Тому, метою даної роботи буде розробка такої системи захисту інформації, при якій загрози витоку конфіденційної інформації будуть мінімальні.

1.2 Аналіз нормативно-правової бази у сфері ЗІ

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 Україні треба буде розв'язати 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 всебічно охоплюють усі проблеми захисту інформації і підходів, що відбивають специфіку, до забезпечення безпеки інформації в різноманітних сферах діяльності держави і товариства;
- регламентація рівнів безпеки інформації й адекватних їм методів і засобів захисту. Однією з найбільш 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.

До складу законодавчої бази України з питань інформаційної діяльності входять близько 240 законодавчих актів. Безпосередньо законодавчу базу з питань технічного захисту інформації складають:

- Закон України «Про державну таємницю»;
- Закон України «Про інформацію»;
- Закон України «Про державну статистику»;
- Закон України «Про захист інформації в автоматизованих системах».

Закон України «Про державну таємницю» введений в дію постановою Верховної Ради України № 3856-12 від 21.01.1994 року.

Цей Закон регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту життєвоважливих інтересів України у сфері оборони, економіки, зовнішніх відносин, державної безпеки і охорони правопорядку.

Державна таємниця – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони право порядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою.

Спеціально уповноваженим органом державної влади у сфері забезпечення охорони державної таємниці є Служба безпеки України.

Забезпечення охорони державної таємниці відповідно до вимог режиму секретності в органах Державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях, діяльність яких пов'язана з державною таємницею, покладається на керівників зазначених органів, підприємств, установ і організацій.

До державної таємниці у порядку, встановленому цим Законом, відноситься інформація про організацію, зміст, стан і плани розвитку технічного захисту секретної інформації.

З метою охорони державної таємниці впроваджується цілий перелік заходів,

у тому числі технічний та криптографічний захисти секретної інформації. Технічний та криптографічний захист секретної інформації здійснюється в порядку, встановленому Президентом України.

В Законі визначено, що технічний захист секретної інформації – вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації.

Закон України «Про інформацію» установлює загальні правові основи одержання, використання, поширення і збереження інформації. Відповідно до цього закону:

Інформація – це документовані або привселюдно оголошені відомості про події і явища, що відбуваються в товаристві, державі або навколишньому природному середовищі.

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.

Відповідно до закону основними видами інформації є:

- статистична інформація;
- масова інформація;
- інформація про діяльність державних органів влади й органів місцевого і регіонального самоврядування;
- правова інформація;

- інформація про особистість;
- інформація довідково-енциклопедичного характеру;
- соціологічна інформація.

Категорії інформації і режим доступу до неї визначаються такими статтями Закону.

Стаття 28. Режим доступу до інформації

Режим доступу до інформації це передбачений правовими нормами порядок одержання, використання, поширення і збереження інформації.

По режиму доступу інформація ділиться на відкриту та інформацію з обмеженим доступом.

Держава здійснює контроль за режимом доступу до інформації.

Задача контролю за режимом доступу до інформації складається в забезпеченні дотримання вимог законодавства про інформацію всіма державними органами, підприємствами, заснуваннями й організаціями, недопущенні необґрунтованого віднесення зведень до категорії інформації з обмеженим доступом. Державний контроль за дотриманням установленого режиму здійснюється спеціальними органами, що визначаються Верховною Радою України і Кабінетом Міністрів України.

У порядку контролю Верховних Рада України може жадати від урядових заснувань, міністерств, відомств звіти, що містять зведення про їхню діяльність по забезпеченню інформацією зацікавлених осіб (кількість випадків відмови в наданні доступу до інформації з указівкою мотивів таких відмов; кількість і обґрунтування застосування режиму обмеженого доступу до окремих видів інформації; кількість скарг на неправомірні дії посадових осіб, що відмовили в доступі до інформації, прийняті до них міри тощо).

Стаття 30. Інформація з обмеженим доступом

Інформація з обмеженим доступом по своєму правовому режимі ділиться на конфіденційну і секретну.

Конфіденційна інформація це зведення, що знаходяться у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб і що поширюються по їхньому бажанню відповідно до передбачених ними умов.
Громадяни, юридичні особи, що володіють інформацією фахового, ділового, виробничого, банківського, комерційного й іншого характеру, отриманої на власні засоби, або яка є предметом їх фахового, ділового, виробничого, банківського, комерційного й іншого інтересу і порушуючи не передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи приналежність її до категорії конфіденційної, і встановлюють для неї систему (засоби) захисту.

Виняток складає інформація комерційного і банківського характеру, а також інформація, правовий режим якої установлений Верховною Радою України по уявленню Кабінету Міністрів України (із питань статистики, екології, банківських операцій, податків тощо), і інформація, утаювання якої являє загрозу життя і здоров'ю людей.

До секретної інформації відноситься інформація, що містить зведення, що складають державну й іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, товариству і державі. Віднесення інформації до категорії секретних зведень, що складають державну таємницю, і доступ до неї громадян здійснюється відповідно до закону про цю інформацію.

Порядок обертання секретної інформації і її захист визначається відповідними державними органами за умови дотримання вимог, установлених дійсним Законом.

Порядок і терміни обнародування секретної інформації визначаються відповідним законом.

Стаття 53. Інформаційний суверенітет

Основою інформаційного суверенітету України є національні інформаційні ресурси.

До інформаційних ресурсів України відноситься вся приналежна їй інформація, незалежно від утримання, форм, часу і місця створення.

Україна самостійно формує інформаційні ресурси на своїй території і вільно розпоряджається ними, за винятком випадків, передбачених законами і міжнародними договорами.

Стаття 54. Гарантії інформаційного суверенітету України

Інформаційний суверенітет України забезпечується:

- виключним правом власності України на інформаційні ресурси, що формуються за рахунок засобів державного бюджету; створенням національних систем інформації;
- установленням режиму доступу інших держав до інформаційних ресурсів України;
- використанням інформаційних ресурсів на основі рівноправного співробітництва з іншими державами.

Закон України «Про державну статистику»

Цей Закон регулює правові відносини в галузі державної статистики, визначає права і функції органів державної статистики, організаційні засади здійснення державної статистичної діяльності з метою отримання всебічної та об'єктивної статистичної інформації щодо економічної, соціальної, демографічної та екологічної ситуації в Україні та її регіонах і забезпечення нею держави та суспільства.

Стаття 21. Гарантії органів державної статистики щодо забезпечення конфіденційності статистичної інформації

Первинні дані, отримані органами державної статистики від респондентів під час проведення статистичних спостережень, а також адміністративні дані щодо респондентів, отримані органами державної статистики від органів, що займаються діяльністю, пов'язаною із збиранням та використанням адміністративних даних, є конфіденційною інформацією, яка охороняється Законом і використовується виключно для статистичних цілей у зведеному знеособленому вигляді. Поширення статистичної інформації, на підставі якої можна визначити конфіденційну статистичну інформацію щодо конкретного

респондента, забороняється. Статистична інформація, отримана органами державної статистики у процесі статистичних спостережень, не може вимагатися державними органами, органами місцевого самоврядування, іншими юридичними особами, об'єднаннями громадян, посадовими та іншими особами з метою використання для прийняття рішень до конкретного респондента.

Ціллю Закону України «Про захист інформації в автоматизованих системах» 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.

Приведемо зведення найбільше важливих статей Закону, що стосуються умов опрацювання і заходів для забезпечення захисту інформації.

Стаття 10. Забезпечення захисту інформації в АС

Захист інформації в АС забезпечується шляхом: дотримання суб'єктами правових відношень норм, вимог і правил організаційного і технічного характеру по захисту оброблюваної інформації; використання засобів обчислювальної техніки, програмного забезпечення, засобів зв'язку й АС у цілому, засобів захисту інформації, що відповідають установленим вимогам по захисту інформації (маючих відповідний сертифікат); перевірки відповідності засобів обчислювальної техніки, програмного забезпечення, засобів зв'язку й АС в цілому установленим вимогам по захисту інформації (сертифікація засобів обчислювальної техніки, засобів зв'язку й АС);
здійснення контролю по захисту інформації.

Стаття 11. Встановлення вимог і правил по захисту інформації

Вимоги і правила по захисту інформації, що є власністю держави, або інформації, захист якої гарантується державою, установлюються державним органом, уповноваженим Кабінетом Міністрів України. Ці вимоги і правила є обов'язковими для власників АС, де така інформація опрацьовується, і носить рекомендаційний характер для інших суб'єктів права власності на інформацію.

Стаття 12. Умови опрацювання інформації

Інформація, що є власністю держави або інформація, захист якої гарантується державою, повинна опрацьовуватися в АС, що має відповідний сертифікат (атестат) захищеності, у порядку, обумовленому уповноваженим Кабінетом Міністрів України органом. У процесі сертифікації (атестації) цих АС здійснюються також перевірка, сертифікація (атестація) розроблених засобів захисту інформації. Інформація, що є власністю інших суб'єктів, може опрацьовуватися в зазначених АС по розсуду власника інформації. Власник інформації може звернутися в органи сертифікації з клопотанням про проведення аналізу можливостей АС по належному захисту його інформації й одержанні відповідних консультацій.

Стаття 13. Політика в області захисту інформації

Вимоги і правила щодо захисту інформації, яка є власністю держави, або інформації, захист якої гарантується державою, встановлюються державним органом, уповноваженим Кабінетом Міністрів України. Ці вимоги і правила є обов'язковими для власників АС, де така інформація обробляється, і мають рекомендаційний характер для інших суб'єктів права власності на інформацію.

Стаття 14. Державне керування захистом інформації в АС

Уповноважений Кабінетом Міністрів України орган здійснює керування захистом інформації шляхом: проведення єдиного технічної політики по захисту інформації; розробки концепції, вимог, нормативно-технічних документів і науково-методичних рекомендацій по захисті інформації в АС;

ствердження порядку організації, функціонування і контролю за виконанням мір, спрямованих на захист оброблюваної в АС інформації, що є власністю держави, а також рекомендацій по захисті інформації власності юридичних і фізичних осіб; організації іспитів і сертифікації засобів захисту інформації в АС, у якій здійснюється опрацювання інформації, що є власністю держави; створення відповідних структур для захисту інформації в АС; проведення атестації сертифікаційних (іспитових) органів, центрів і лабораторій, видача ліцензії на право проведення сервісних робіт в області захисту інформації в АС; здійснення

контролю захищеності оброблюваної в АС інформації, що є власністю держави; визначення порядку доступу осіб і організацій закордонних держав до інформації в АС, що є власністю держави, або до інформації власності фізичних і юридичних осіб, щодо поширення і використання якої державою встановлені обмеження. Міністерства, відомства й інші центральні органи державної влади забезпечують рішення питань захисту інформації в АС у межах своїх повноважень.

Стаття 15. Служби захисту інформації в АС

У державних заснуваннях і організаціях можуть створюватися підрозділи, служби, що організують роботу, пов'язану з захистом інформації, підтримкою рівня захисту інформації в автоматизованих системах, і відповідають за ефективність захисту інформації відповідно до вимог дійсного Закону.

Стаття 20. Забезпечення інформаційних прав України

Фізичні і юридичні особи в Україні на підставі Закону України "Про інформацію" можуть встановлювати взаємозв'язок з АС інших держав із метою опрацювання, обміну, продажі, покупки відкритої інформації. Такі взаємозв'язки повинні виключати можливість несанкціонованого доступу з боку інших держав або їхніх представників резидентів України або осіб без громадянства до інформації, наявної в АС України, незалежно від форм власності і підпорядкування, у відношенні якої установлені вимоги нерозповсюдження її за межі України без спеціального дозволу.

Іноземні держави, іноземні фізичні і юридичні особи можуть виступати власниками АС в Україні, власниками інформації, що поширюється й опрацьовується в АС України, або заснувати спільні з українськими юридичними і фізичними особами підприємства з метою створення АС України, обміну інформацією між АС України й АС інших держав. Окремі види такої діяльності здійснюються на підставі спеціального дозволу (ліцензії), що видається уповноваженим на це органом.

1.3 Постановка задачі

У спектрі інтересів підприємств державної статистики, пов'язаних з використанням локальних обчислювальних мереж, можна виділити необхідність забезпечення наступних функціональних властивостей захищеності інформаційних об'єктів і які забезпечуються відповідними рівнями послуг ІБ:

1. Конфіденційність (захист від несанкціонованого ознайомлення);

2. Цілісність (актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованої зміни);

3. Доступність (можливість за прийнятний час одержати необхідну інформацію).

На сьогоднішній день вимоги щодо конфіденційності, цілісності та доступності викладені в досить розвиненій нормативно – правовій базі.

Конфіденційність. Цей рівень послуг ІБ відповідає за загрози, що відносяться до несанкціонованого ознайомлення з інформацією за рахунок реалізації загроз на кшталт несанкціонованого доступу до неї, чи використання витоків інформації технічними каналами. Ці загрози і є загрозами конфіденційності. Вітчизняні та закордонні апаратно-програмні продукти дають змогу закрити практично всі потенційні канали відтоку інформації.

Цілісність. Загрози, що відносяться до несанкціонованої модифікації інформації, складають загрози цілісності. Відповідними послугами є довірча цілісність, адміністративна цілісність, відкіт і цілісність при обміні. Останню можна поділити на статичну (зрозумілу як незмінність інформаційних об'єктів) і динамічну (що стосується конкретного виконання складних дій (транзакцій)). Приклад динамічної цілісності – контроль потоку повідомлень (виявлення крадіжки, упорядкування або дублювання окремих повідомлень).

Доступність. Загрози, що відносяться до порушення можливості використання комп'ютерних чи систем оброблюваної інформації, складають загрози доступності. Відповідними послугами є використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв.

Основні напрямки збереження конфіденційності статистичних даних:

- органи державної статистики гарантують конфіденційність первинних статистичних даних, отриманих від респондентів, а також статистичної інформації, на підставі якої можна визначити інформацію щодо конкретного респондента, і адміністративних даних, що використовуються для статистичних цілей:
- конфіденційність статистичної інформації гарантується законодавством;
- фахівці органів державної статистики при призначенні на посаду підписують документ про зобов'язання не розголошувати конфіденційну статистичну інформацію;
- законодавством передбачені санкції за порушення порядку використання конфіденційної статистичної інформації;
- підготовлена методологічна/методична документація щодо захисту конфіденційної статистичної інформації у процесі її збирання, опрацювання, аналізу, поширення, збереження і використання, яка оприлюднена та доступна для широкого загалу;
- застосовуються організаційні та технічні заходи захисту статистичної інформації;

Тому як мету цієї дипломної роботи можна розглядати визначення та оцінку ризиків при застосуванні тих чи інших засобів забезпечення конфіденційності, цілісності та доступності інформаційних об'єктів в інформаційно – телекомунікаційних системах та їх специфічному класу – локальних обчислювальних мережах.

1.4 Висновки до першого розділу

В даному розділі було детально проаналізовано стан питання інформаційної безпеки державних підприємств, які оброблюють статистичну інформацію, та нормативно-правову базу України у сфері захисту інформації. Було визначено основні нормативні документи щодо захисту статистичної інформації та основні задачі щодо забезпечення конфіденційності статистичних даних.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про підприємство

Повна назва: Відділ статистики Дніпровської районної державної адміністрації.

Місцезнаходження: 49000, м. Дніпро, вул. Столярова, 3.

Напрям діяльності підприємства: здійснює реалізацію державної політики у сфері регіональної статистики, статистики діяльності підприємств та тенденцій ділової активності в регіоні. Забезпечує відповідність статистичної інформації критеріям якості, бере участь у розробленні, вдосконаленні, впровадженні та поширенні науково обґрунтованої статистичної методології, проводить аналіз повноти охоплення респондентів державних статистичних спостережень. Забезпечує формування інформаційної бази для прогнозування й аналізу тенденцій і закономірностей соціально-економічного розвитку регіону.

Принципи діяльності органів державної статистики України – це зведення стандартів у галузі статистики, дотримання яких гарантує державі та суспільству, що офіційна статистична інформація розробляється і поширюється на основі професійної незалежності, неупередженості, об'єктивності, надійності, економічності та статистичної конфіденційності.

Штат співробітників:

- Начальник відділу аналізу даних статистики фінансів підприємств;
- Провідний економіст-спеціаліст аналізу даних статистики фінансів підприємств (1 співробітник);
- Головний економіст-спеціаліст аналізу даних статистики фінансів підприємств (5 співробітників).

Всього 7 співробітників. Форма власності: державна власність.

Режим роботи підприємства : 08.00 – 17.00

Робочі дні: понеділок – п'ятниця.

Обов'язки співробітників

Начальник відділу:

- здійснює керівництво діяльністю відділу у межах делегованих йому начальником управління повноважень;
- вживає заходів щодо вдосконалення організації роботи відділу;
- організовує та контролює проведення працівниками відділу статспостережень зі структурної статистики та статистики фінансів підприємств, передачу відповідних даних (квартальних і річних) на державний рівень в зазначені терміни;
- забезпечує дотримання працівниками відділу правил внутрішнього трудового розпорядку і етики поведінки;
- у межах своєї компетенції забезпечує здійснення заходів щодо запобігання корупції та контроль за їх виконанням у відділі;
- готує проєкт технологічної програми державних статистичних спостережень та комплексного плану роботи;
- надає методологічну допомогу працівникам відділу аналізу даних статистики фінансів підприємств, респондентам та відокремленим підрозділам;
- контролює діяльність відокремлених підрозділів;
- аналізує роботу відділу щодо узгодження кола респондентів державних статистичних спостережень зі структурними та відокремленими підрозділами, контролює повноту охоплення респондентів згідно з сукупностями звітних одиниць для проведення державних статистичних спостережень зі статистики фінансів підприємств, актуалізацію сукупностей;
- організовує та контролює підготовку відповідей на запити респондентів та користувачів працівниками відділу;
- контролює ведення діловодства та роботу з укомплектування, зберігання, обліку та використання архівних документів у порядку, встановленому чинним законодавством;
- забезпечує у межах своїх повноважень виконання завдань з мобілізаційної підготовки та цивільного захисту;

- організовує та контролює підготовку місцевим державним органам та органам місцевого самоврядування статистичну інформацію в обсягах, за формами і в строки, визначені планом державних статистичних спостережень;
- бере участь у конференціях, семінарах, нарадах з питань, що належать до його компетенції;
- використовує вміло комп'ютерну техніку та програмне забезпечення;
- бере участь у забезпечені функціонування інтегрованої інформаційно-аналітичної системи органів державної статистики на регіональному рівні;
- забезпечує відповідно до чинного законодавства збереження та захист статистичної інформації;
- бере участь у підготовці відповідей на запити щодо публічної інформації у встановленому законодавством порядку;
- організовує та контролює надання звітів на паперових носіях для проведення виїмки (вилучення на виконання відповідних ухвал);
- взаємодіє з підрозділами збирання та обробки інформації;
- взаємодіє з Держстатом з питань статистики фінансів підприємств; забезпечує надання послуг та підготовку статистичної інформації користувачам на платній основі працівниками управління;
- використовує дані Єдиного державного реєстру підприємств та організацій України і реєстрів респондентів статистичних спостережень у регіоні;
- забезпечує відповідність статистичної інформації критеріям якості;
- здійснює аналіз інформації щодо витрат робочого часу у відділі.

Провідний економіст-спеціаліст:

- здійснює супровід на обласному рівні та відправку на державний рівень моніторингу подання фінансової звітності (річної, піврічної) (бере участь у проведенні семінарів, нарад стосовно обробки моніторингу подання фінансової звітності; відповідає за розробку форми, за якість отриманих даних, порівняльний аналіз та узгодження показників форми з даними інших форм державних статистичних спостережень) (як дублер);

- здійснює та відповідає за підготовку та здачу до архіву справ постійного зберігання та відповідає за діловодство (як дублер);
- відповідає за ведення обліку робочого часу працівників відділу;
- бере участь у зборі, здійснює контроль, узагальнення та аналіз даних первинних звітів зі статистики фінансів підприємств, структурної статистики та статистики ділової активності підприємств по підприємствах;
- працює над поліпшенням якості звітів, вдосконаленням розробки та випуску всіх форм державних статистичних спостережень на закріпленій ділянці;
- проводить консультаційну роботи для забезпечення партнерських взаємовідносин з респондентами, готує оглядові листи за результатами державних статистичних спостережень;
- здійснює перевірну роботу з достовірності первинних та статистичних даних, вивчає стан первинного обліку та статистичної звітності, складає протоколи про адміністративні правопорушення;
- бере участь у інформаційно-публікаційній діяльності та підготовці аналітичних матеріалів для користувачів статистичної інформації;
- консультує спеціалістів відокремлених підрозділів статистики з питань статистики фінансів підприємств, структурної статистики та статистики ділової активності підприємств, готує методичні вказівки, оглядові листи на матеріали перевірок відокремлених підрозділів статистики та за результатами розробок державних статистичних спостережень;
- бере участь у наданні тимчасового доступу до первинних фінансових та статистичних звітів;
- здійснює підготовку та здачу до архіву справ постійного зберігання;
- забезпечує відповідно до законодавства збереження отриманих первинних звітів тощо;
- виконує інші роботи, що відносяться до компетенції відділу, за дорученням начальника відділу, начальника управління.

Головний економіст-спеціаліст:

- здійснює супровід на обласному рівні та відправку на державний рівень державного статистичного спостереження за формою № 2-Б "Звіт про випуск, розміщення та обіг цінних паперів" (річна) (приймає участь у проведенні семінарів, нарад стосовно обробки державного статистичного спостереження за формою № 2-Б; відповідає за розробку форми, за якість отриманих даних, порівняльний аналіз та узгодження показників форми з даними інших форм державних статистичних спостережень);
- здійснює супровід на обласному рівні та відправку на державний рівень моніторингу подання фінансової звітності (річної, піврічної) (приймає участь у проведенні семінарів, нарад стосовно обробки моніторингу подання фінансової звітності; відповідає за розробку форми, за якість отриманих даних, порівняльний аналіз та узгодження показників форми з даними інших форм державних статистичних спостережень) (як дублер);
- проводить опрацювання електронної звітності зі статистики фінансів;
- бере участь у зборі, здійснює контроль, узагальнення та аналіз даних первинних звітів по підприємствах зі статистики фінансів підприємств, структурної статистики та статистики ділової активності підприємств;
- працює над поліпшенням якості звітів, вдосконаленням розробки та випуску всіх форм державних статистичних спостережень на закріпленій ділянці;
- проводить консультаційну роботи для забезпечення партнерських взаємовідносин з респондентами, готує оглядові листи за результатами державних статистичних спостережень;
- ефективно взаємодіє з колегами, респондентами та користувачами;
- організовує та проводить перевірки достовірності первинних та статистичних даних, вивчає стан первинного обліку та статистичної звітності, складає протоколи про адміністративні правопорушення;
- бере участь у інформаційно-публікаційній діяльності та підготовці аналітичних матеріалів для користувачів статистичної інформації;
- консультує спеціалістів відокремлених підрозділів статистики з питань статистики фінансів підприємств, структурної статистики та статистики

ділової активності підприємств, готує методичні вказівки, оглядові листи за результатами розробок державних статистичних спостережень;

- бере участь у наданні тимчасового доступу до первинних фінансових та статистичних звітів;
- здійснює постійний моніторинг якості статистичних даних відповідно до компонентів якості;
- здійснює постійний моніторинг діяльності та самооцінки досягнутих результатів, проводить внутрішні й, у разі потреби, зовнішні аудити.
- регулярно проводить перегляд довгострокової програми розвитку державної статистики, а також завдань та функцій органів державної статистики.
- здійснює підготовку та здачу до архіву справ постійного зберігання;
- забезпечує відповідно до законодавства збереження отриманих первинних звітів тощо;
- проводить заняття з цивільної оборони та техніки безпеки;
- виконує інші роботи, що відносяться до компетенції відділу, за дорученням начальника відділу, начальника управління.

2.2 Акт обстеження

2.2.1 Обстеження ОІД

Органи державної статистики області є складовою єдиної системи органів державної статистики України, важливою ланкою системи державного та регіонального управління, невід'ємною частиною загальнодержавної інформаційної системи.

Органи державної статистики у Дніпропетровській області представлені Головним управлінням статистики, в якому діють 23 структурних та 15 відокремлених підрозділів – управління (відділи, сектори) статистики у 4 містах та 11 районах.

Будівля відділу статистики Дніпровської районної державної адміністрації знаходиться у центрі міста, за адресой: вул. Столярова, 3. Територія будівлі складає 1га.

Штат працівників складає більш ніж 150 робітників. Біля будівлі знаходиться навчальний заклад будівельно-монтажний технікум та розважальний боулінг-клуб «Панорама».

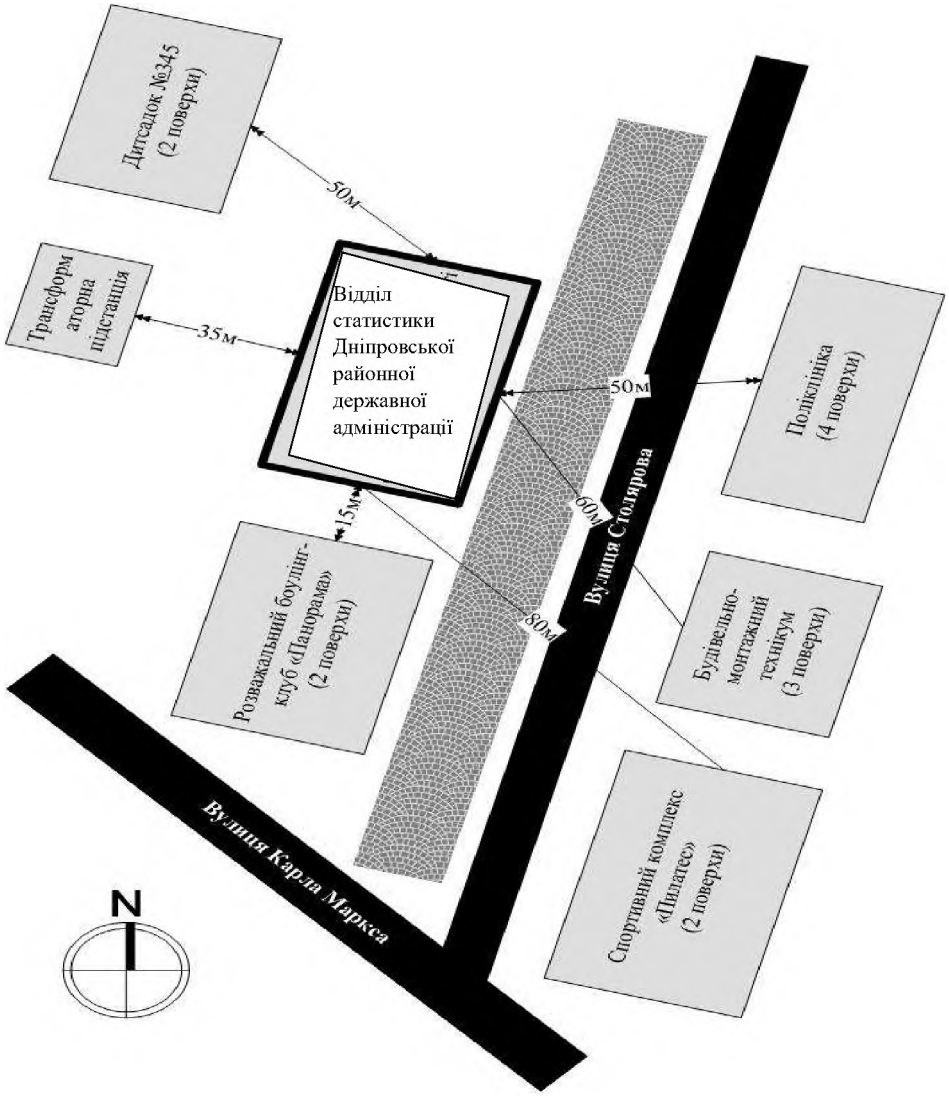


Рисунок 2.1- Ситуаційний план

На ситуаційному плані показано розташування відділу статистики щодо об’єктів місцевості.

Будівлі, які знаходяться безпосередньо поруч:

- Будівельно-монтажний технікум;
- Спортивний комплекс «Пилатес»;
- Розважальний боулінг-клуб «Панорама»;
- Дитячий садочок №345;

- Поліклініка №1.

ОІД (відділ даних статистики фінансів підприємств) знаходиться на 5 поверсі будівлі, в кімнаті під номером 505.

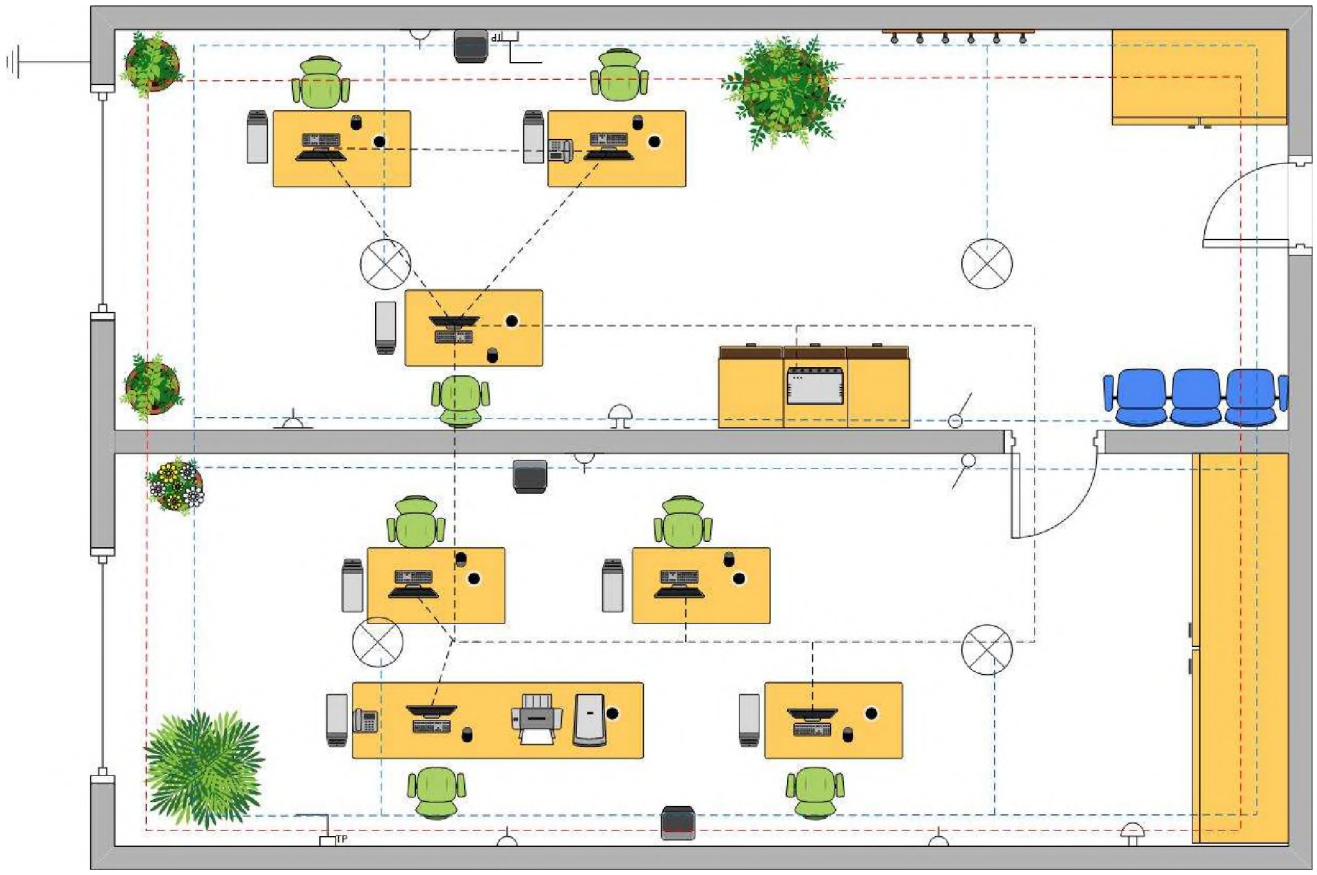


Рисунок 2.2 - Генеральний план об’єкта інформаційної діяльності

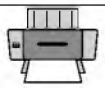
До КЗ мають доступ тільки співробітники даного відділу, тому що на дверях встановлений кодовий замок. В деяких випадках керівник відділу вирішує кому надати допуск.

Таблиця 2.1

Умовні позначення до рисунку 2.2

Позначка на плані	Значення
—	Система опалення
—	Локальна мережа
—	Сис. електороподачі
⏚	Система заземлення
⊗	Кімнатне освітлення

Продовження таблиці 2.1

	Вимикач
	Розетка
	Сканер
	Персональний комп'ютер
	Принтер
	Монітор с клавіатурою
	Телефонна розетка
	Концентратор

2.2.2 Структура обчислюваної системи

На ОІД обробляється відкрита інформація та інформація з обмеженим доступом. Щодо першої потрібно забезпечувати цілісність і доступність, щодо другої ще і конфіденційність.

Складовими обчислюваної системи є: 7 робочих станцій, які підключені до однієї локальної мережі. Використовується для створення внутрішніх документів та обробки статистичної інформації, яка являється інформацією з обмеженим доступом. Вихід до Інтернету не має жодна зі встановлених станцій.

Технічні засоби прийому, обробки, передачі та зберігання інформації: принтер та сканер.

Допоміжні технічні засоби і системи (ДТЗС): лінії пожежної сигналізації, лінії Інтернет, кабелі телефонного зв'язку, лінії мережі електроживлення, 7 ламп денного світла.

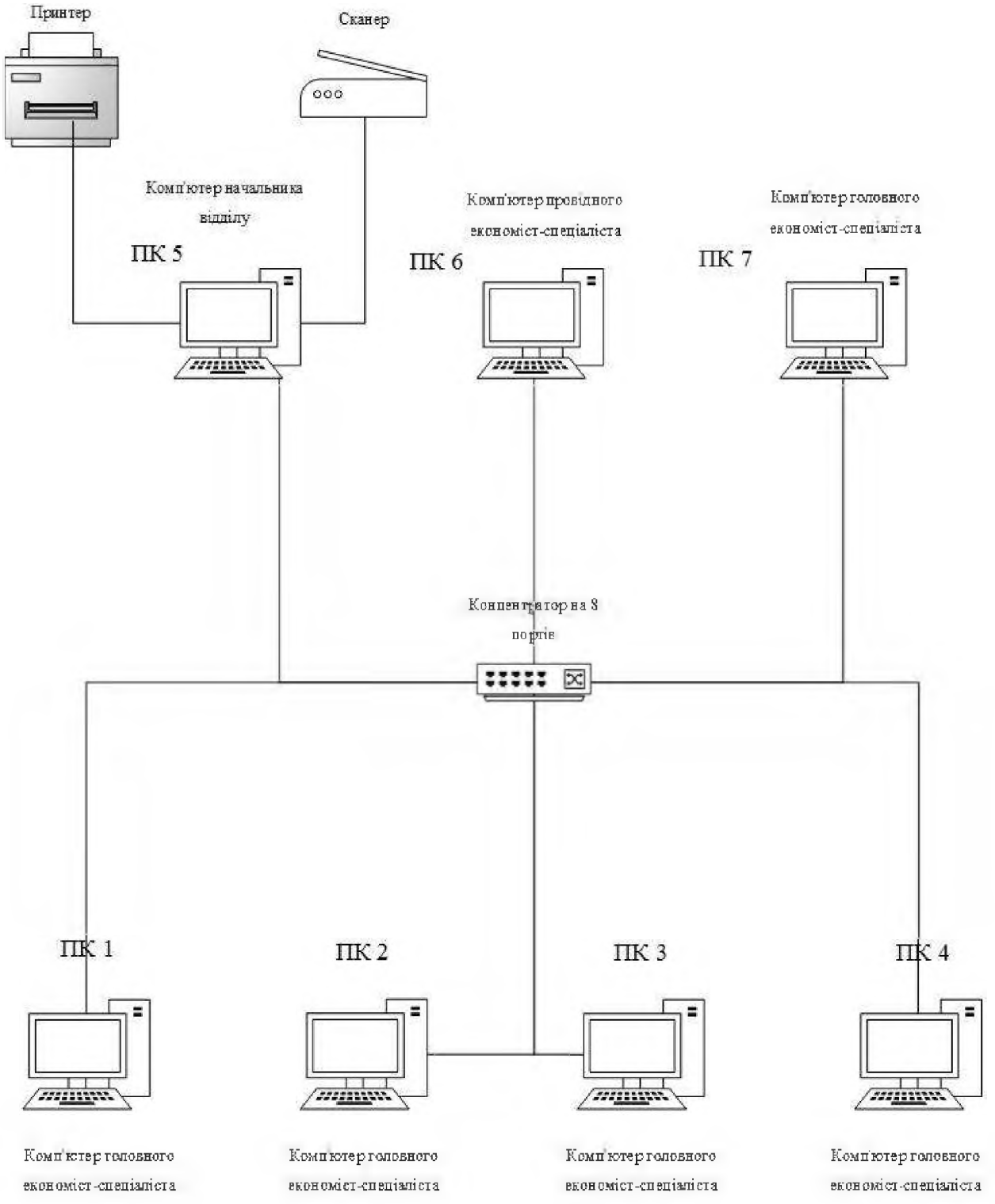


Рисунок 2.3 - Схема інформаційно-комунікаційної системи

Таблиця 2.2

Апаратне забезпечення

Назва	Характеристика	Кількість
Принтер	Модель: Samsung Light D200	1
Сканер	Модель: Philips tr234 Pro	1
Робоча станція	Asus : Intel Celeron G550 (2.6 ГГц)/ RAM 4ГБ / HDD 500 ГБ / AMD Radeon R2	7
Монітор	*18.5* LG 19MN43D-PZ	7
Клавіатура	Logitech Keyboard K270	7
Миша	Logitech Mouse M185 Grey USB (910-002238)	7
Телефон	Philips HomeTelephone xc54	1
Концентратор	TP-LINK TL-SG108	1

Таблиця 2.3

Програмне забезпечення

Тип ПЗ	Назва
ОС	Windows 10 Ultimate (ПК) Номер ліцензії: wer4-fgkk-45gk-3kg5
Прикладне ПЗ	Microsoft Office 2013 (проф.)
	Total Commander ver.2.4.1
	Adobe Reader PDF ver.7.5
	WinRar ver.2.3

Продовження таблиці 2.3

Тип ПЗ	Назва
Спеціальне ПЗ	Комплекс електронної обробки інформації «Міжгалузева статистика підприємств»
	Комплекс електронної обробки інформації «Реєстрація подання статистичної звітності»
	Matrix – перелік звітів якими повинне звітувати підприємство
Антивірус	ESET Endpoint Antivirus

2.2.3 Інформаційні потоки на підприємстві

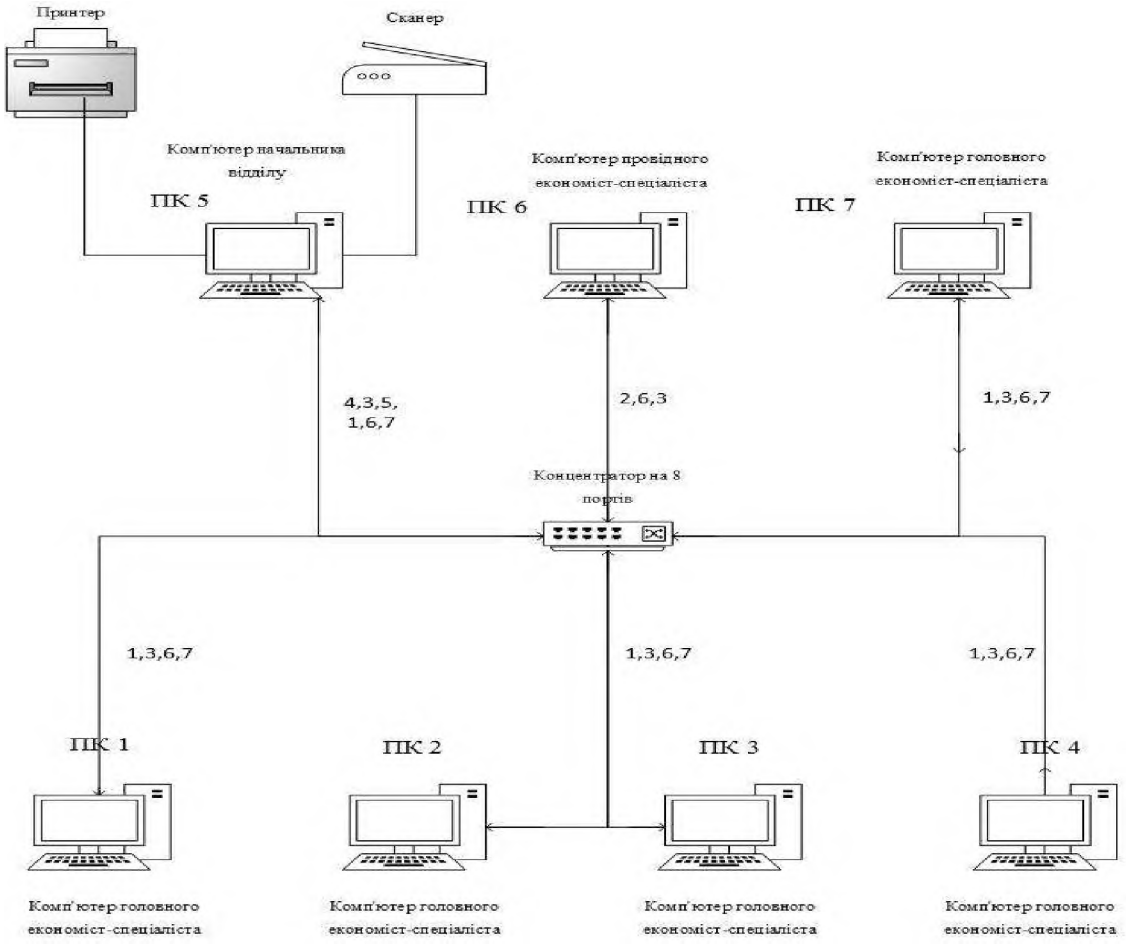


Рисунок 2.4 - Інформаційні потоки на підприємстві

1. Первинні звіти за різними формами.

2. Анкети ділової активності підприємств.
3. Внутрішні документи.
4. Інструктивна інформація по заповненню статистичних форм.
5. Архівні данні.
6. Статистична інформація.
7. Реєстр статистичних одиниць.

2.2.4 Опис фізичного середовища

Таблиця 2.4

Система комунікацій підприємства

Система комунікації	Пояснення
Сис. електороподачі	Підключена до трансформаторної станції, яка знаходиться за межами КЗ.
Сис. опалення	Підключена до міської системи опалення.
Сис. заземлення	Всі прилади, комп'ютери заземлені до загального контуру заземлення, який замкнутий і виходить за межі КЗ.
Тел. лінія і Інтернет	Інтернет Фрегат. Підключений за допомогою супутникової мережі. Телефонна мережа – Укртелеком.
Сис. вентиляції	Приточно-витяжна.
Протипожежна безпека	Складається з системи оповіщення і датчиків, дані з яких обробляються протипожежним приймально-контрольним пристроєм, який знаходиться за межами КЗ.

2.3 Аналіз ризиків

Таблиця 2.5

Класифікація інформації, циркулюючої на ОІД

№	Інформація	Режим доступу	Правовий режим	Вимоги	Вид представлення
1	Первинні звіти від респондентів за формою 1-підприємництво (річна)	ІзОД	Конфіденційна	К3,Ц3,Д1	Електронний та паперовий
2	Первинні звіти від респондентів за формою 1-підприємництво (річна-коротка)	ІзОД	Конфіденційна	К3,Ц3,Д1	Електронний та паперовий
3	Фін. звіти від респондентів за формами: 1-баланс 2-звіт фін. результатів 3-рух грош. коштів 4-власний капітал 5-примітки до фін. звітності 1-м-баланс малого підприємства 1-мс-баланс мікро-підприємства 2-мс- звіт про фінансові результати мікро-підприємства	ІзОД	Конфіденційна	К3,Ц3,Д1	Електронний та паперовий

Продовження таблиці 2.5

4	Первинні звіти від респондентів за формою 1-б Звіт про взаєморозрахунки з нерезидентами	ІзОД	Конфі-денційна	К3,Ц3,Д1	Електронний та паперовий
5	Анкета ділової активності підприємств: Послуг; Промисловості; Сільського господарства; Будівництва; Торгівлі.	ІзОД	Конфі-денційна	К3,Ц3,Д1	Електронний та паперовий
6	Внутрішні документи (накази, посадові інструкції, положення про відділ, листування з респондентами, листування з територіальними органами статистики).	ІзОД	Конфі-денційна	К2,Ц2,Д1	Електронний
7	Інструктивна інформація по заповненню статистичних форм	Відкрита		Ц1,Д2	Друкований

Продовження таблиці 2.5

8	Архівні данні	ІзОД	Конфі-денційна	К1,Ц2,Д1	Електронний та паперовий
9	Статистична інформація (прес-випуски, щорічник, бюлетені, збірники, доповіді)	Відкрита		Ц1,Д1	Друкований та електронний
10	Реєстр статистичних одиниць	ІзОД	Конфі-денційна	К2,Ц2,Д2	Електронний

Таблиця 2.6

Умовні позначення до таблиці 2.5

Вимоги	Низький рівень	Середній рівень	Високий рівень
Конфіденційність	К1	К2	К3
Цілісність	Ц1	Ц2	Ц3
доступність	Д1	Д2	Д3

Таблиця 2.7

Матриця доступу

Посада / Інформація	Начальник відділу	Провідний економіст-спеціаліст	Головний економіст-спеціаліст
1	R,W	R	R

Продовження таблиці 2.7

Посада / Інформація	Начальник відділу	Провідний економіст-спеціаліст	Головний економіст-спеціаліст
2	R,W	R	R
3	R,W	R	R
4	R,W	R	R
5	R,W	R	R
6	R,W,D	R,W	R,W
7	R	R	R
8	R,D	R	R
9	R,W,D	R,W	R,W
10	R	R	R

R – право на читання.

W – право модифікацію.

D – право на видалення.

2.3.1 Аналіз загроз

Загрозами безпеки інформації є:

- розкрадання інформації;
- знищення інформації;
- модифікація інформації;
- порушення доступності інформації;
- нав'язування неправдивої інформації.

Джерелами загроз безпеки є:

- антропогенні;
- техногенні;
- стихійні (маловірогідні, тому не враховуються).

Таблиця 2.8

Аналіз загроз та класифікація порушників

Джерело (антропогенний)	Загроза	Наслідки
Керівники різних рівнів посадової ієрархії (4)	Навмисне втручання у систему (4)	Виток перв. даних(5) Знищення перв. даних (5)
Співробітники (4)	Необережне поводження з інформацією при роботі з клієнтами та різними підприємствами (4)	Передача фінансових звітів зацікавленим особам (5) Виток перв. даних (5)
	Винесення за межі КЗ, переносних пристроїв без перевірки (4)	
	Поширення інформації про данні підприємств (5)	
	Підкуп працівника (5)	
Співробітники ІТ відділу (3)	Не оновлення антивірусу (3)	Збій роботи системи (4) Виток або знищення перв.даних (5) Передача фінансових звітів зацікавленим особам (5) Не виконання завдань відділу (3)
	Встановлення вірусів навмисно (5)	
	Можливість особистої зацікавленості (3)	
	Невірна інсталяція ПЗ, ОС (4)	
Відвідувачі (3)	Встановлення пристроїв прослуховування інформації (4)	Використання отриманої звітної інформації в особистих цілях (4) Виток перв. даних (5)
	Підкуп працівника (5)	

Продовження таблиці 2.8

Джерело (антропогенний)	Загроза	Наслідки
Технічний персонал, який обслуговує будівлю та приміщення (електрики, сантехніки, прибиральники тощо) (1)	Навмисне втручання у систему (4)	Передача фінансових звітів зацікавленим особам (5) Виток перв. даних (5)
	Підкуп працівника (4)	
Персонал, який обслуговує технічні засоби (інженери, техніки) (2)	Навмисне втручання у систему (4)	Збій роботи системи (4) Не виконання завдань відділу (3) Передача фінансових звітів зацікавленим особам (5)
	Підкуп працівника (5)	
	Встановлення пристроїв прослуховування інформації (4)	

K1 – можливість появи джерела

K2 – готовність джерела

K3 – наслідки виявленої загрози

Таблиця 2.9

Оцінка антропогенних ризиків

	K1	K2	K3	K загрози
Керівники різних рівнів посадової ієрархії	4	4	5	0.64
Співробітники	5	4	5	0.8
Співробітники IT відділу	3	3.75	4.25	0.382
Відвідувачі	3	4.5	4.5	0.486

Продовження таблиці 2.9

	K1	K2	K3	K загрози
Технічний персонал, який обслуговує будівлю та приміщення	1	4	5	0.16
Персонал, який обслуговує технічні засоби	2	4.33	4	0.277

Таблиця 2.10

Аналіз загроз та класифікація порушників

Джерело (техногенний)	Загроза	Наслідки
Дисковий накопичувач (4)	Винесення дискового накопичувача (5)	Втрата перв. даних та фінансових звітів або їх знищення (5)
	Відсутність шифрування (3)	
Система лінії зв'язку (4)	Відсутність зв'язку (4)	Втрата перв. даних та фінансових звітів або їх знищення (5))
Неякісні програмні засоби обробки інформації (4)	Збій в роботі автоматизованої системи (4)	Можливість знищення цінної фін. та стат. інформації (5)
Мережі інженерних комунікацій (4)	Обрив лінії із-за стихійної події (2)	Перехоплення зведених даних (4)
	Ушкодження носіїв і обчислювальної техніки (4)	Втрата зведених даних, знищення документів (4)

Таблиця 2.11

Оцінка техногенних ризиків

Оцінка ризиків	K1	K2	K3	K загрози
Дисковий накопичувач	4	4	5	0.64
Система лінії зв'язку	4	4	5	0.64
Неякісні програмні засоби обробки інформації	4	4	5	0.64
Мережі інженерних комунікацій	4	3	4	0.384

2.4 Обґрунтування необхідності створення КСЗІ

Необхідність забезпечення захисту інформації (а саме створення комплексної системи захисту інформації (КСЗІ) в автоматизованих системах 1-ого, 2-ого та 3-ого класу: НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем») визначається передусім вимогами нормативно-правових документів. Нижче наведено перелік нормативно-правових документів, на підставі яких створюються КСЗІ:

- закон України «Про інформацію» регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації;
- закон України «Про захист інформації в інформаційно-телекомунікаційних системах» стаття 8 «Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження

відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством»;

- «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» затверджені постановою Кабінету Міністрів України від 29 березня 2006р. № 373 п.16 свідчить про те, що для забезпечення захисту інформації в системі створюється комплексна система захисту інформації, яка призначається для захисту інформації від: витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій; несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів; спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування;
- 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;
- 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.

Згідно з законом України «Про державну статистику», розділ 5 «Забезпечення конфіденційності статистичної інформації», стаття 21 «Гарантії органів державної статистики щодо забезпечення конфіденційності статистичної інформації»:

Первинні дані, отримані органами державної статистики від респондентів під час проведення статистичних спостережень, а також адміністративні дані щодо респондентів, отримані органами державної статистики від органів, що займаються діяльністю, пов'язаною із збиранням та використанням адміністративних даних, є конфіденційною інформацією, яка охороняється Законом і використовується виключно для статистичних цілей у зведеному знеособленому вигляді. Поширення статистичної інформації, на підставі якої можна визначити конфіденційну статистичну інформацію щодо конкретного респондента, забороняється. Статистична інформація, отримана органами державної статистики у процесі статистичних спостережень, не може вимагатися державними органами, органами місцевого самоврядування, іншими юридичними особами, об'єднаннями громадян, посадовими та іншими особами з метою використання для прийняття рішень до конкретного респондента.

2.5 Розробка політики безпеки

Політика безпеки розробляється згідно з положеннями НД ТЗІ 1.1-002 та рекомендаціями НД ТЗІ 1.4-001.

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. Чим дрібніше об'єкт, відносно якого застосовується даний термін, тим конкретнішими і формальніше стають правила. Далі для скорочення замість словосполучення «політика безпеки інформації» може використовуватись словосполучення «політика безпеки», а замість словосполучення «політика безпеки інформації, що реалізується послугою» — «політика послуги» і т. ін.

Політика безпеки інформації в АС є частиною загальної політики безпеки організації і може успадковувати, зокрема, положення державної політики у галузі захисту інформації. Для кожної АС політика безпеки інформації може бути індивідуальною і може залежати від технології обробки інформації, що

реалізується, особливостей ОС, фізичного середовища і від багатьох інших чинників. Тим більше, одна й та ж сама АС може реалізовувати декілька різноманітних технологій обробки інформації. Тоді і політика безпеки інформації в такій АС буде складеною і її частини, що відповідають різним технологіям, можуть істотно відрізнятись.

Політика безпеки повинна визначати ресурси АС, що потребують захисту, зокрема установлювати категорії інформації, оброблюваної в АС. Мають бути сформульовані основні загрози для ОС, персоналу, інформації різних категорій і вимоги до захисту від цих загроз. Як складові частини загальної політики безпеки інформації в АС мають існувати політики забезпечення конфіденційності, цілісності і доступності оброблюваної інформації. Відповідальність персоналу за виконання положень політики безпеки має бути персоніфікована.

Політика безпеки інформації, що реалізуються різними КС будуть відрізнятися не тільки тим, що реалізовані в них функції захисту можуть забезпечувати захист від різних типів загроз, але і в зв'язку з тим, що ресурси КС можуть істотно відрізнятись. Так, якщо операційна система оперує файлами, то СУБД має справу із записами, розподіленими в різних файлах.

Частина політики безпеки, яка регламентує правила доступу користувачів і процесів до ресурсів КС, складає правила розмежування доступу.

Функціональний профіль захищеності

Виходячи з цих даних та вимог забезпечення конфіденційної інформації різних рівнів та відкритої інформації, можна зробити висновок, що найліпше для даної АС другого класу відповідає стандартний функціональний профіль захищеності з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації:

2.КЦД.2 = { КД-2, КА-2, КО-1,ЦД-1, ЦА-2, ЦО-1,ДР-1, ДВ-1,НР-2, НК-1, НЦ-2, НТ-2, НИ-2, НО-2 };

НД ТЗІ 2.5-008-2002 «Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2»

Довірча конфіденційність

КЗЗ повинен реалізувати рівень КД-2.

Ця послуга застосовується для розмежування доступу користувачів до захищених об'єктів і дозволяє користувачу керувати потоками інформації в АС від захищених об'єктів, що належать його домену, до інших користувачів.

Політика довірчої конфіденційності поширюється на: користувачів усіх категорій; об’єкти, які містять конфіденційну інформацію, за умови визначення в АС груп користувачів з однаковими повноваженнями стосовно такої інформації і тільки в межах цих груп; об’єкти, які містять технологічну інформацію КСЗІ або управління АС і можуть використовуватися тільки користувачами, яким надано однакові повноваження відповідних адміністраторів, в межах свого домену; всі інші об’єкти, які підлягають захисту, але не належать до зазначених вище видів, - і забезпечує взаємодію зазначених об’єктів.

Політика довірчої конфіденційності, що реалізується КЗЗ, стосується слабо- та сильно зв’язаних об’єктів, які створюються користувачем у процесі виконання ним функціональних обов’язків. Користувач, який створив об’єкт, має право визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від цього об'єкта.

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

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта.

КЗЗ повинен надавати користувачу як власнику процесу, можливість визначати конкретних користувачів і/або групи користувачів, які мають право ініціювати цей процес.

Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації.

Ця послуга може реалізовуватися лише у разі необхідності та у доповнення до послуги КА-2, яка визначає основний механізм розмежування доступу до конфіденційної інформації в АС класу 2.

Адміністративна конфіденційність

КЗЗ повинен реалізувати рівень КА-2.

Ця послуга дозволяє адміністраторові безпеки (уповноваженим співробітникам СЗІ) та/або користувачам, яким надано повноваження інших адміністраторів, керувати потоками інформації від захищених об'єктів, що зберігаються й циркулюють в АС, до користувачів. Політика адміністративної конфіденційності поширюється на: користувачів усіх категорій; сильно- та слабо зв'язані об'єкти, що містять службову інформацію; системне та функціональне програмне забезпечення, що використовується для оброблення службової інформації; технологічну інформацію КСЗІ; технологічну інформацію щодо управління АС; доступ користувачів до окремих видів периферійних пристроїв (принтерів, накопичувачів на змінних машинних носіях інформації тощо), задіяних в обробці службової інформації, - і забезпечує взаємодію зазначених об'єктів. Стосовно об'єктів, для яких додатково в межах визначених доменів реалізується послуга КД-2, ця послуга застосовується для розмежування доступу до інформації користувачів на рівні доменів та для розмежування доступу до інформації користувачів різних доменів. Якщо послуга КД-2 не використовується, то політика адміністративної конфіденційності повинна поширюватися, крім зазначених вище, і на інші об'єкти, яких стосувалася послуга КД-2.

Розмежування доступу користувачів усіх категорій до захищеного об'єкта здійснюється засобами КЗЗ на підставі атрибутів доступу користувача й захищеного об'єкта. Призначення атрибутів доступу користувачам і процесам здійснюється адміністратором безпеки та/або уповноваженим на це співробітником СЗІ, на основі аналізу функціональних обов'язків окремих користувачів або груп користувачів та процесів і об'єктів, що відносяться до їх компетенції.

КЗЗ повинен надавати можливість користувачам, що мають відповідні повноваження - адміністраторам операційних систем, адміністраторам СКБД, адміністраторам мережевого обладнання, адміністраторам сервісів, - права доступу до процесів, що забезпечують ведення системних процесів щодо

адміністративного супроводження функціонування АС в цілому, окремих її компонентів та сервісів. КЗЗ повинен надавати тільки адміністратору безпеки та/або уповноваженим співробітникам СЗІ права доступу до процесів, що забезпечують актуалізацію, супроводження та аналіз технологічної інформації КСЗІ.

Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністратора безпеки (уповноваженого співробітника СЗІ) або користувачів, яким надані повноваження інших адміністраторів.

КЗЗ повинен надавати можливість адміністратору безпеки (уповноваженому співробітнику СЗІ) або користувачам, яким надано повноваження інших адміністраторів, для кожного процесу визначати конкретних користувачів і/або групи користувачів, що мають право ініціювати процес, через керування належністю користувачів і процесів до відповідних доменів.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації.

Повторне використання об'єктів

КЗЗ повинен реалізувати рівень КО-1.

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

Політика повторного використання об'єктів, що реалізується КЗЗ, стосується тільки тих об'єктів АС, які містять службову інформацію і ресурси яких поділяються між користувачами АС та прикладними процесами, що виконуються в АС.

Вимоги цієї послуги поширюються на сегменти оперативної пам'яті робочих станцій та серверів (усіх без виключення типів) та носії інформації на жорстких магнітних дисках, якими укомплектовані робочі станції й сервери, і використовуються системними та функціональними процесами під час

оброблення службової інформації, а також на окремі види периферійних пристроїв, які мають власну пам'ять і задіяні під час експорту (імпорту) службової інформації з (в) АС та створенні «твердих» копій тощо.

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

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

Вимога цієї послуги в повному обсязі поширюється і на розділювані одночасно декількома користувачами процеси.

Довірча цілісність

КЗЗ повинен реалізувати рівень ЦД-1

Ця послуга застосовується для захисту оброблюваної інформації від несанкціонованої модифікації і дозволяє користувачу будь-якої категорії керувати потоками інформації в АС від інших користувачів до захищених об'єктів, що належать його домену.

Умови реалізації в АС послуги ЦД-1 повністю співпадають з умовами реалізації послуги КД-2, а політика довірчої цілісності стосується тих самих об'єктів, що і політика довірчої конфіденційності.

Політика довірчої цілісності, що реалізується КЗЗ, поширюється на слабо- та сильно зв'язані об'єкти, які створюються користувачем у процесі виконання ним функціональних обов'язків. Користувач, який створив об'єкт, має право визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати цей об'єкт.

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

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації.

Ця послуга може реалізовуватися лише у разі необхідності та у доповнення до послуги ЦА-2 (ЦА-1), яка визначає в АС класу 2 основний механізм захисту від несанкціонованої модифікації об’єктів, які містять службову інформацію.

Базова адміністративна цілісність

Політика базової адміністративної цілісності поширюється на: користувачів усіх категорій; сильнозв'язані об'єкти, що містять службову інформацію; призначене для оброблення цих об'єктів системне та функціональне програмне забезпечення, а також створену в процесі обробки сильнозв'язаних об'єктів технологічну інформацію КСЗІ та технологічну інформацію щодо управління АС, і забезпечують взаємодію зазначених об’єктів.

Право визначати множину об'єктів АС, цілісність яких забезпечується КЗЗ, а також визначати атрибути доступу процесу й захищеного об'єкта, на підставі яких КЗЗ буде здійснювати розмежування доступу, надається тільки адміністратору безпеки (уповноваженому співробітнику СЗІ).

Розмежування доступу здійснюється в межах певного процесу наданням користувачу права (встановленням заборони) за допомогою функціональних можливостей цього процесу модифікувати об’єкт.

КЗЗ повинен обробляти запити на зміну атрибутів доступу процесів і захищених об'єктів тільки в тому випадку, якщо вони надходять від адміністратора безпеки або від уповноваженого співробітника СЗІ. КЗЗ повинен надавати можливість адміністратору безпеки (уповноваженому співробітнику СЗІ) або користувачам, яким надано повноваження інших адміністраторів, для кожного захищеного об'єкта (сукупності сильнозв'язаних об'єктів або певним чином виділеної підмножини їх, об'єкта, окремого стовпчика або окремого поля запису структурованого об'єкта) визначити домен, якому повинні належати ті процеси і/або групи процесів, що мають право модифікувати об’єкт. Тільки їм надається право включати й вилучати процеси та об'єкти до/з конкретних доменів.

КЗЗ повинен надавати можливість адміністратору безпеки (уповноваженому співробітнику СЗІ) або користувачам, яким надано повноваження інших адміністраторів, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації.

Відкат

КЗЗ повинен реалізувати рівень ЦО-1.

Ця послуга забезпечує можливість відмінити окрему операцію або послідовність операцій й повернути захищений об'єкт, з яким маніпулював користувач, до попереднього наперед визначеного стану.

Політика обмеженого відкату поширюється на: користувачів усіх категорій; сильно- та слабозв'язані об'єкти, які містять службову інформацію і в процесі обробки яких передбачається можливість їхньої модифікації користувачем, а також технологічну інформацію КСЗІ і забезпечує взаємодію зазначених об'єктів.

Компоненти КЗЗ повинні мати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певну множину операцій, що вже виконані над захищеним об'єктом за певний проміжок часу.

Факт використання користувачем послуги має реєструватись в системному журналі. Відміна операції не повинна призводити до видалення з журналу запису про операцію, яка пізніше була відмінена, якщо остання підлягала реєстрації відповідно до вимог послуги безпеки НР-2.

Використання ресурсів

КЗЗ повинен реалізувати рівень ДР-1.

Ця послуга дозволяє керувати використанням користувачами послуг та ресурсів.

Політика використання ресурсів, що реалізується КЗЗ, поширюється на: сильно- та слабозв'язані об'єкти, що містять інформацію будь-яких категорій; файлову систему (логічні диски, каталоги, підкаталоги тощо); системне та

функціональне програмне забезпечення; технологічну інформацію щодо управління АС; окремі периферійні пристрої (принтери, накопичувачі інформації, змінні носії інформації і т.п.); обчислювальні ресурси АС і забезпечує взаємодію зазначених об'єктів, передбачаючи можливість встановлення обмежень на їх використання користувачами всіх категорій.

Обмеження щодо використання окремим користувачем та/або процесом обсягів обчислювальних ресурсів АС або кількості об'єктів встановлюються адміністратором безпеки або користувачами, яким надано повноваження інших адміністраторів. Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів.

Спроби користувачів перевищити встановлені обмеження на використання ресурсів повинні реєструватися в системному журналі.

Відновлення після збоїв

КЗЗ повинен реалізувати рівень ДВ-1.

Політика відновлення після збоїв, що реалізується КЗЗ, поширюється на: системне та функціональне програмне забезпечення; засоби захисту інформації та засоби управління КСЗІ; засоби адміністрування та управління обчислювальною системою АС; окремі периферійні пристрої (принтери, накопичувачі інформації, змінні носії інформації і т.і.), які задіяні для обробки службової інформації, - і забезпечує взаємодію зазначених об'єктів.

Послуга гарантує повернення АС у відомий захищений стан після відмов або переривання обслуговування, спричинених помилковими діями користувачів, неврахованою функціональною недостатністю програмного та апаратного забезпечення (наприклад, можливою наявністю не виявлених під час проектування незадекларованих функцій), іншими непередбачуваними ситуаціями.

Політикою відновлення після збоїв повинна бути визначена й задокументована множина типів відмов і переривань обслуговування АС або окремих її компонентів, після яких можливе повернення у відомий захищений

стан без порушення політики безпеки. Для кожної з відмов повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція АС.

Після відмови АС або окремих її компонентів, або переривання обслуговування КЗЗ повинен перевести АС або окремі її компоненти до стану, із якого повернути до нормального функціонування може тільки адміністратор безпеки, інші адміністратори або співробітники СЗІ.

Повинні бути визначені повноваження адміністратора безпеки, уповноважених співробітників СЗІ, інших адміністраторів (адміністратора операційної системи, адміністратора баз даних, адміністраторів сервісів та ін.) та множина виконуваних ними допустимих операцій з метою повернення АС у відомий захищений стан.

Повернення АС (окремих компонентів) із режиму, що визначається погіршеними характеристиками обслуговування, в режим нормального функціонування повинно здійснюватися за допомогою ручних (не автоматизованих) процедур.

Реєстрація

Послуга реєстрації рівня НР-2 дозволяє контролювати небезпечні для АС дії зі сторони користувачів будь-яких категорій відносно процесів і об'єктів, що існують в АС і стосуються захищених об’єктів.

Політика реєстрації поширюється на: користувачів усіх категорій; сильно- та слабозв'язані об'єкти, що містять службову інформацію; системне та функціональне програмне забезпечення, призначене для оброблення цих об'єктів; використання периферійного обладнання, задіяного для оброблення службової інформації; використання обчислювальних ресурсів АС, а також створену в процесі обробки сильно- та слабозв'язаних об'єктів технологічну інформацію КСЗІ та технологічну інформацію щодо управління АС, - і забезпечує взаємодію зазначених об’єктів.

КЗЗ повинен забезпечувати реєстрацію всіх подій, які мають безпосереднє відношення до його безпеки. До таких відносяться наступні класи подій:

- вхід/вихід або намагання входу/виходу в/із системи користувачів будь-яких категорій;
- реєстрація та видалення або намагання реєстрації та видалення користувачів будь-якої категорії із системи;
- зміна паролю користувачем будь-якої категорії;
- отримання або намагання отримання доступу користувачем будь-якої категорії до будь-яких процесів і об'єктів АС, що мають ступінь обмеження доступу на рівні службової інформації;
- виведення користувачем будь-якої категорії документа або службової інформації на призначений для цього пристрій друку, або намагання виведення користувачем будь-якої категорії документа або службової інформації на пристрій друку, що для роботи зі службовою інформацією не призначений;
- копіювання наборів даних із службової інформацією на запам'ятовуючих пристроях, які працюють зі змінними носіями, що здатні записувати інформацію, і виділені спеціально для виконання процесів копіювання, або намагання копіювання службової інформації на запам'ятовуючих пристроях, які згідно з політикою безпеки для цього не призначені;
- виявлення і реєстрація фактів порушення цілісності КЗЗ;
- інші події, обов'язковість реєстрації яких передбачена політикою реалізації окремих послуг безпеки інформації.

Реєстрація всіх подій, що мають безпосереднє відношення до безпеки, здійснюється в журналі реєстрації, який містить інформацію щодо дати, часу, місця (адреси робочої станції в АС), імені користувача, типу й успішності чи неуспішності кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію достатню для однозначної ідентифікації робочої станції, користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події.

Адміністратор безпеки і користувачі, яким надано повноваження інших адміністраторів, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації, а КЗЗ повинен забезпечувати захист журналу реєстрації від

несанкціонованого доступу, модифікації або руйнування.

Достовірний канал

КЗЗ повинен реалізувати рівень НК-1.

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

Політика достовірного каналу поширюється на користувачів усіх категорій, окремі компоненти системного та функціонального програмного забезпечення, які задіяні для реалізації механізмів КЗЗ, і забезпечує взаємодію зазначених об’єктів.

Достовірний канал повинен використовуватися для початкової ідентифікації та автентифікації. Зв'язок із використанням даного каналу повинен ініціюватися виключно користувачем.

Цілісність комплексу засобів захисту

КЗЗ повинен реалізувати рівень НЦ-2.

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

Політика цілісності КЗЗ поширюється на: адміністратора безпеки та/або уповноважених співробітників СЗІ; окремі компоненти системного та функціонального програмного забезпечення, які задіяні для реалізації механізмів КЗЗ; засоби захисту інформації, а також технологічну інформацію КСЗІ - і забезпечує взаємодію зазначених об’єктів.

Політика реалізації послуги повинна гарантувати, що усі послуги безпеки доступні тільки через інтерфейс КЗЗ й усі запити в АС на доступ до захищених об'єктів контролюються КЗЗ. Якщо існують якісь обмеження, недотримання яких може призвести до надання послуг в обхід інтерфейсу КЗЗ і порушення політики безпеки, то такі обмеження повинні бути описані і задокументовані. Порядок дотримання користувачами цих обмежень визначається і контролюється

адміністратором безпеки або уповноваженим співробітником СЗІ. З метою захисту від зовнішніх впливів КЗЗ повинен визначати й підтримувати власний домен виконання, який є відмінним від доменів виконання усіх інших процесів, а також повинен мати механізми, що використовуються для реалізації розмежування доменів.

У власному домені повинен забезпечуватися захист від несанкціонованої модифікації механізмів КЗЗ і/або втрати керування КЗЗ.

Повинен бути визначений механізм контролю цілісності компонентів, що входять до складу КЗЗ. У разі виявлення порушення цілісності будь-якого зі своїх компонентів КЗЗ повинен повідомити щодо цього адміністратора безпеки або уповноваженого співробітника СЗІ і перевести АС до стану, в якому забороняється обробка службової інформації. Повернути АС до нормального функціонування може тільки адміністратор безпеки або уповноважений співробітник СЗІ після відновлення відповідності цього компонента КЗЗ еталону.

Самотестування

КЗЗ повинен реалізувати рівень НТ-2.

Самотестування дозволяє КЗЗ перевірити й на підставі цього гарантувати правильність функціонування і цілісність множини функцій АС, що забезпечуються захистом.

Політика самотестування поширюється на: адміністратора безпеки та/або уповноважених співробітників СЗІ; компоненти системного та функціонального програмного забезпечення, які задіяні для реалізації механізмів КЗЗ; засоби захисту інформації, а також технологічну інформацію КСЗІ - і забезпечує взаємодію зазначених об’єктів.

До складу КЗЗ повинен входити набір тестових процедур, достатній для оцінки правильності виконання в АС всіх критичних для безпеки службової інформації та технологічної інформації КСЗІ функцій, а сам КЗЗ повинен бути здатним контролювати їх виконання.

Тести повинні виконуватися при ініціалізації КЗЗ за запитом адміністратора безпеки або уповноважених співробітників СЗІ.

У разі некоректного виконання якогось із тестів КЗЗ повинен перевести АС до стану, в якому забороняється обробка службової інформації взагалі, або до стану, в якому забороняється обробка службової інформації з використанням послуг безпеки, для яких тест не було виконано. Повернути АС до нормального функціонування може тільки адміністратор безпеки або уповноважений співробітник СЗІ після відновлення працездатності КЗЗ і повторного виконання повного набору тестів.

Ідентифікація та автентифікація

КЗЗ повинен реалізувати рівень НИ-2.

Ідентифікація та автентифікація дозволяють визначити й перевірити особу користувача будь-якої категорії, що намагається одержати доступ до АС або до захищених об’єктів, та повинні гарантувати, що доступ може бути надано тільки авторизованому користувачу.

Політика ідентифікації та автентифікації поширюється на: усіх осіб, які намагаються одержати доступ до АС; користувачів усіх категорій, які намагаються одержати доступ до сильно- та слабозв'язаних об'єктів, що містять службову інформацію, призначену для оброблення цих об'єктів системного та функціонального програмного забезпечення, периферійного обладнання, задіяного для обробки службової інформації, створеної у процесі обробки сильно- та слабозв'язаних об'єктів, технологічної інформації КСЗІ та технологічної інформації щодо управління АС, і забезпечує взаємодію зазначених об’єктів.

Кожний користувач, що отримує доступ до АС, повинен ідентифікуватися КЗЗ на підставі присвоєного йому імені.

Дозвіл на виконання будь-яких дій, що контролюються КЗЗ, користувач отримує тільки після автентифікації його КЗЗ на підставі введеного ним пароля.

Механізм реалізації послуги повинен відповідати умовам надійного та однозначного виконання ідентифікації та автентифікації.

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

Розподіл обов'язків

КЗЗ повинен реалізувати рівень НО-2.

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

Політика розподілу обов'язків, що реалізується КЗЗ, поширюється на користувачів усіх категорій і повинна визначати щонайменше такі ролі:

- адміністратора безпеки;
- не менше, ніж одного іншого адміністратора (адміністратора баз даних, адміністратора мережевого обладнання, адміністратора сервісів та ін.);
- користувачів, яким надано право доступу до службової інформації.

Ролі адміністраторів можуть дублюватися уповноваженими на це користувачами. Кількість таких користувачів повинна бути мінімальною.

Функції, що притаманні кожній із зазначених категорій адміністраторів, повинні бути максимально розмежовані й мінімізовані таким чином, щоб обмежити їх коло тільки тими, що необхідні для виконання ними функціональних обов'язків, що передбачаються експлуатаційною документацією на відповідні компоненти АС.

Адміністратор безпеки повинен мати доступ до технологічної інформації КСЗІ та системного й функціонального програмного забезпечення, яке реалізує механізми захисту. Інший адміністратор повинен мати доступ до технологічної інформації щодо управління АС та системного й функціонального програмного забезпечення, яке реалізує ці функції. Усім іншим користувачам доступ до цих об'єктів повинен бути заборонений.

Повинен заборонятися доступ адміністраторів до сильно та слабозв'язаних об'єктів, що містять службову інформацію, за виключенням випадків, коли їхніми функціональними обов'язками передбачено суміщення адміністративних повноважень та повноважень щодо обробки службової інформації.

КЗЗ повинен присвоювати користувачу атрибути, якими однозначно

характеризується надана йому роль. Користувач може виступати в певній ролі тільки після того, як він виконає дії, що підтверджують прийняття ним цієї ролі.

Правила політики безпеки

У будівлі є один вхід і один вихід, організовано цілодобовий контрольно-пропускний пункт охорони на вході (КПП). При проході через КПП кожному співробітнику видається пропуск. Для проходу через КПП людям не є співробітниками також видається пропуск за наявності посвідчення особи і заноситься відповідний запис у журнал відвідувань. Кожного співробітника та відвідувача перевіряють метало-детектором на наявність несанкціонованих засобів зчитування, обробки та передачі інформації.

Основні організаційні заходи

1. Організаційні заходи щодо керування доступом повинні передбачати:

- визначення порядку доступу користувачів у захищене приміщення, до технічних засобів, носіїв інформації, програмного та інформаційного забезпечення;
- визначення порядку внесення/вилучення даних щодо атрибутів доступу користувача до АС установи;

2. Організаційні заходи щодо реєстрації та обліку МНІ та документів

Організаційні заходи щодо реєстрації та обліку повинні передбачати визначення порядку:

- обліку, використання і зберігання машинних носіїв інформації (МНІ);
- організації зберігання, використання і знищення документів і носіїв, що містять інформацію з обмеженим доступом, відповідно до вимог нормативних документів.

3. Організаційні заходи щодо забезпечення цілісності інформації

Організаційні заходи щодо забезпечення цілісності інформації повинні передбачати:

- резервне копіювання на МНІ еталонних копій операційних систем і функціональних програм;
- облік, видачу, використання і зберігання МНІ, що містять еталонні і

резервні копії операційних систем і функціональних програм;

- контроль цілісності системного програмного забезпечення;
- контроль цілісності КЗЗ АС.

4. Організаційні заходи щодо антивірусного захисту інформації

Організаційні заходи антивірусного захисту інформації в АС повинні передбачати:

- використання ліцензійного антивірусного програмного забезпечення на всіх ПК, що входять до складу АС;
- організацію постійного та своєчасного оновлення антивірусних баз.

5. Резервне копіювання, архівування та відновлення інформації

Для забезпечення відновлюваності інформації у випадку збоїв системи або помилок користувачів в АС повинно здійснюватися періодичне резервне копіювання.

Резервному копіюванню підлягає:

- ІзОД, яка зберігається у файлах користувачів;
- ІзОД, яка зберігається у БД;
- настройки ОС, БД та КЗЗ;
- журнали реєстрації.

Розробка правил політики безпеки для програмних засобів

Все програмне забезпечення, встановлене у відділі статистики Дніпровської районної державної адміністрації на комп'ютерному обладнанні, є власністю Дніпровської районної державної адміністрації і використовується виключно у виробничих цілях.

Всі комп'ютери повинні захищатися паролем при завантаженні системи. Паролі повинні бути довжиною більш ніж 8 символів та з використанням символів написаних верхнім регістром. Паролі повинні обновлятися кожні 3 місяці.

Програмне забезпечення впливає на швидкість і якість передачі даних. Також тип ПЗ залежить від типу переданої інформації. Слід уважно вибирати ПЗ

для підприємства. Не дотримання цього правила може призвести до втрати даних, зайвим витратам на встановлення нового ПЗ, втрати інформації.

Правила для програмних засобів:

- програмне забезпечення, що використовується на підприємстві, а також документація, що поставляється з ним, враховані;
- на ПК встановлено ліцензійне ПЗ;
- установку обладнання виробляє спеціально навчена людина;
- перед установкою ПЗ тестується;
- перед початком використання ПЗ, співробітників навчають правильному використанню;
- кожен користувач відповідно до договору, знає які права інтелектуальної власності він може порушити;
- оновлення та їх установка (виповнюється відповідальною за це особою);
- використовує програмний засіб особа, яка має на це права;
- забезпечити оптимальні умови для роботи обладнання.

Захист програмних засобів ведеться як від помилок програм, так і від помилок користувача. Резервування та архівування - надійні способи зберігання інформації. Варто уважно простежити яким саме чином буде проходити резервування даних.

Забезпечити якість і збереження архівної інформації. При використанні певних програмних засобів (бази даних, файловий сервер і т.д.) передбачається автоматичне резервування даних на окремому носії.

Зберігання даних не залежить від системи. Запис резервуються даних ведеться на окремих машинах. Передбачений резервне джерело живлення для виключення непереборних ситуацій не пов'язаних з виробництвом. У міру запису даних ведеться їх архівування.

Термін зберігання інформації призначається на вимогу керівника і відповідно до документацією. Дані зберігаються в окремому приміщенні, і в спеціально відведеному місці.

Доступ до резервування, архівування, зберігання, утилізації даних мають тільки спеціальні особи, які мають на це допуск.

На всіх персональних комп'ютерах повинні бути встановлені програми, необхідні для забезпечення захисту інформації:

- персональний міжмережевий екран;
- антивірусне програмне забезпечення;
- програмне забезпечення шифрування жорстких дисків;
- програмне забезпечення шифрування поштових повідомлень;
- всі комп'ютери, які підключені до локальної мережі, повинні бути оснащені системою антивірусного захисту;

Співробітники відділу статистики не повинні:

- блокувати антивірусне програмне забезпечення;
- встановлювати інше антивірусне програмне забезпечення;
- змінювати налаштування і конфігурацію антивірусного програмного забезпечення.

Розробка правил для політики безпеки управління доступом

Засоби управління доступом зводяться не тільки до автентифікації, але з їх допомогою визначається, хто має доступ до ресурсів організації. Засоби управління доступом передбачають кілька способів реалізації. Найбільш поширені алгоритми прив'язані до тих, що пропонуються операційними системами або програмним забезпеченням, що підтримує роботу підприємства.

Для кожного користувача повинні бути розробленні певні правила можливостей роботі в АС та розподілені повноваження для запобігання витоку ІзОД при некоректному поводженні та через випадкові помилки.

Розробка правил політики безпеки антивірусного захисту

Кожен працівник зобов'язаний виконувати правила експлуатації антивірусного ПЗ і вимоги антивірусної безпеки щодо зовнішніх джерел і носіїв інформації, негайно припиняти роботу при підозрах на вірусне зараження.

Антивірусний захист забезпечується використанням спеціалізованого ліцензійного антивірусного програмного забезпечення.

Для зниження впливу людського фактору, виключення можливості відключення або не оновленої антивірусних засобів, контроль і управління антивірусним програмним забезпеченням, а також усунення виявлених вразливостей в системному програмному забезпеченні проводиться в автоматизованому режимі.

Система антивірусного захисту мережі призначена для вирішення наступних завдань:

- Безперервний антивірусний моніторинг та періодичне антивірусне сканування всіх робочих станцій;
- Автоматичне реагування на зараження комп'ютерними вірусами і на вірусні епідемії, що включає в себе: оповіщення, лікування вірусів, видалення троянських програм і очищення системи, що зазнала зараженню;

Дисциплінарні заходи, відповідальність співробітників за порушення безпеки

Дисциплінарна відповідальність один з різновидів юридичної відповідальності. Її зміст становить обов'язок суб'єкта перетерплювати за свої неправомірні дії певні несприятливі наслідки. Дисціплінарна відповідальність застосовується лише у трудових правовідносинах.

Дисциплінарна відповідальність - це реакція на правопорушення у сфері трудових відносин, що виявляється у застосуванні санкцій несприятливого характеру до порушників встановленого порядку. Дисциплінарна відповідальність являє собою наслідок невиконання або неналежного виконання трудових обов'язків конкретним працівником, тобто недотримання ним трудової дисципліни.

Основні ознаки дисциплінарного проступку:

- дії або бездіяльність працівника, які визначені в законі як невиконання або неналежне виконання трудових обов'язків;
- наявність вини - обов'язкова ознака дисциплінарного проступку (відповідальність настає виключно за винні дії, бездіяльність);
- працівником не виконані саме трудові обов'язки;

- наявність обставин, які роблять можливим застосування дисциплінарного стягнення.

Головний спеціаліст-економіст несе відповідальність у межах, визначених чинним законодавством України за неякісне або несвоєчасне виконання посадових завдань та обов'язків, бездіяльність або невикористання наданих йому прав, порушення норм етики поведінки державного службовця та обмежень, пов'язаних з прийняттям на державну службу та її проходженням.

Провідний спеціаліст-економіст несе відповідальність згідно з чинним законодавством про працю України та правилами внутрішнього трудового розпорядку.

Начальник відділу несе відповідальність згідно з чинним законодавством про працю України та правилами внутрішнього трудового розпорядку.

Дисциплінарні стягнення застосовуються до державного службовця за невиконання чи неналежне виконання службових обов'язків, перевищення своїх повноважень, порушення обмежень, пов'язаних з проходженням державної служби, а також за вчинок, який порочить його як державного службовця або дискредитує державний орган, в якому він працює.

До службовців, крім дисциплінарних стягнень, передбачених чинним законодавством про працю України, можуть застосовуватися такі заходи дисциплінарного впливу:

- попередження про неповну службову відповідність;
- затримка до одного року у присвоєнні чергового рангу або у призначенні на вищу посаду.

Інструкції використання робочої станції користувачем

- робоче місце для працюючих з відео терміналами необхідно розташувати таким чином, щоб до поля зору працюючого не потрапляли вікна, освітлювальні прилади, поверхні які мають властивість віддзеркалювання. Поверхня робочого столу не повинна бути полірованою. Для попередження відблисків на екрані відео моніторів, особливо влітку та у сонячні дні, екран

відео монітора слід розміщувати так, щоб світло від вікна падало збоку, бажано зліва;

- файли з документами необхідно зберігати тільки в директорії, яку визначає уповноважена особо. Вказана директорія має бути розміщена не на системному розділі жорсткого диску;
- забороняється зберігати документи безпосередньо на робочому столі операційної системи Windows;
- забороняється працювати в режимі корегування документів, які знаходяться не на жорсткому диску персонального комп'ютера;
- забороняється залишати інформацію з обмеженим доступом у вільно доступних місцях(принтері, столі та інші);
- забороняється залишати записані паролі на робочому місці у будь-якому вигляді;
- інформацію з обмеженим доступом треба зберігати у замкнутому ящику стола або у сейфі;
- обмін інформацією між робочими станціями в локальній мережі здійснюється тільки через директорію, яку визначає уповноважена особа. Після використання файлів в цій директорії, вони повинні бути знищені;
- перед копіюванням або відкриттям будь-якого файлу, який відсутній на жорсткому диску персонального комп'ютера, його необхідно перевірити на наявність вірусів за допомогою антивірусної програми;
- забороняється використовувати дискети, машинні носії інформації або CD-диски, які мають ознаки фізичного пошкодження;
- забороняється робити на жорсткий диск копії файлів, які не мають безпосереднього відношення до характеру роботи користувача персонального комп'ютера;
- забороняється допускати до роботи за персональним комп'ютером сторонніх користувачів;
- забороняється проводити на неатестованому персональному комп'ютері обробку інформації, що містить інформацію з обмеженим доступом;

- забороняється проводити інсталяцію додаткових програм без відома керівника або уповноваженої особи.

2.6 Аналіз ризиків після впровадження політики безпеки

Після впровадження політики безпеки ми можемо зробити висновки, що рівень ризиків К зменшився у значному обсязі, тож впровадження політики безпеки інформації можна назвати доцільним з точки зору зниження імовірності реалізації загроз.

K1 – можливість появи джерела

K2 – готовність джерела

K3 – наслідки виявленої загрози

Таблиця 2.12

Оцінка антропогенних ризиків

Антропогенні	K1	K2	K3	K загрози
Керівники різних рівнів посадової ієрархії	2	4	3	0.192
Співробітники	3	3	3	0.216
Співробітники IT відділу	3	3.75	4.25	0.382
Відвідувачі	1	4.5	4.5	0.162
Технічний персонал, який обслуговує будівлю та приміщення	1	4	5	0.16
Персонал, який обслуговує технічні засоби	2	4.33	4	0.277

Таблиця 2.13

Оцінка техногенних ризиків

Техногенні	K1	K2	K3	K загрози
Дисковий накопичувач	3	2	3	0.144
Система лінії зв'язку	4	4	2	0.256
Неякісні програмні засоби обробки інформації	1	3	3	0.072
Мережі інженерних комунікацій	3	2	3	0.144

2.7 Висновки до другого розділу

Для досягнення максимальної ефективності системи захисту необхідно використовувати ряд організаційних та інженерно-технічних заходів в комплексі.

В даному розділі було детально проаналізовано:

- загальні відомості підприємства;
- проведено обстеження ОІД;
- проведено класифікацію циркулюючої інформації;
- визначено основні загрози та порушники;
- створено елементи політики безпеки;
- розроблені інструкції щодо використання робочих станцій;

- проведено аналіз загроз після впровадження політики безпеки;

Розроблено рекомендації для користувачів і обслуговуючого персоналу, які є основою при проведенні організаційних заходів щодо захисту інформації. Також було обрано найбільш відповідний профіль захищеності для локальної мережі та обрано спеціальне програмне забезпечення для реалізації політики безпеки.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Обґрунтування витрат на реалізацію політики безпеки

Метою виконання економічного розділу кваліфікаційної роботи є економічне обґрунтування доцільності впровадження політики безпеки інформації інформаційно-комунікаційної системи відділу статистики Дніпровської районної державної адміністрації.

Для цього визначено економічну ефективність використання основних результатів, що отримані в результаті виконання роботи.

Економічна доцільність визначається розрахунками:

- капітальних витрат, що потребує розроблена політика безпеки;
- експлуатаційних витрат;
- річного економічного ефекту від впровадження інформаційної політики безпеки.

Запропонована політика інформаційної безпеки передбачає необхідність витрат на її реалізацію. Заходами, що потребують витрат, є:

- оновлення ліцензій програмного забезпечення;
- навчання персоналу в питаннях інформаційної безпеки.

3.2 Розрахунок капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Фіксовані витрати на впровадження системи розраховуватимуться за формулою:

$$К = К_{пр} + К_{навч} + К_{н} + К_{зпз}, \text{ грн.} \quad (3.1)$$

де $К_{пр}$ – вартість впровадження, грн.;

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

$К_{н}$ – витрати на встановлення та налагодження ПЗ, грн.;

$К_{зпз}$ – вартість закупівель, грн.

Розрахунок капітальних витрат буде проводитися на прикладі впровадження засобів захисту інформації та додаткового програмного забезпечення: резервне копіювання, контроль стану обладнання, інструктаж з ІБ, встановлення і налаштування ПЗ тощо.

Розрахунок заробітної плати системного адміністратора

Обліком носіїв інформації, резервним копіюванням, встановленням фаєрволу, антивірусу, налагодженням та встановленням ПЗ та обліком носіїв інформації займається системний адміністратор.

Заробітна плата при простій часовій системі оплати праці визначається за формулою:

$$З = ТС* Ф, \quad (3.2)$$

де ТС – тарифна ставка привласненого робітникові кваліфікаційного розряду в одиницю часу (година, день, місяць), грн.;

Ф – фактично відпрацьований час;

Почасова тарифна ставка системного адміністратора складає ТС = 200 грн/год.

Час на налагодження резервного копіювання займає 8 год.:

$$З = ТС* Ф = 200*8 = 1600 \text{ грн.}$$

Час на розробку алгоритму захисту від витоку інформації займає 10 год.:

$$З = ТС* Ф = 200*10 = 2000 \text{ грн.}$$

Час на впровадження запропонованої методики займає 6 год.:

$$З = ТС* Ф = 200*6 = 1200 \text{ грн.}$$

Час на встановлення AD RMS Windows Server 2019 займе 4 год.:

$$З = ТС* Ф = 200*8 = 1600 \text{ грн.}$$

Час на встановлення антивірусного захисту ESET NOD32 займе 4 год.:

$$З = ТС* Ф = 200*4 = 800 \text{ грн.}$$

Розрахунок капітальних витрат

В таблиці 3.1 наведена кількісно-вартісна характеристика заходів, що впроваджується на підприємстві.

Таблиця 3.1 – Кількісно-вартісна характеристика заходів

Міри	Характеристика	Вартість, грн.
Резервне копіювання	Kingston USB3.2 Gen 2 DataTraveler Max (DTMAX/512GB) (2849 грн. * 4 шт.)	11396
Сервер	AD RMS Windows Server 2019	19500
Антивірусний захист	ESET NOD32 (4700 грн.)	4700

Фіксовані витрати на проєктування та впровадження заходів захисту інформації складатимуть:

Резервне копіювання:

$$К = 1600 + 11396 = 12996 \text{ грн.}$$

Розробка алгоритму захисту від витоку інформації:

$$К = 2000 \text{ грн.}$$

Впровадження запропонованої методики:

$$К = 1200 \text{ грн.}$$

AD RMS Windows Server 2019:

$$К = 1600 + 19500 = 21100 \text{ грн.}$$

Антивірусний захист ESET:

$$К = 800 + 4700 = 5500 \text{ грн.}$$

Загальні затрати складуть:

$$К = 42796 \text{ грн.}$$

3.3 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проєктування за визначений період (наприклад, рік), що виражені у грошовій формі.

Під «витратами на керування системою» маються на увазі витрати, пов'язані з керуванням й адмініструванням компонентів системи інформаційної безпеки. До цієї статті витрат можна віднести наступні витрати:

- навчання адміністративного персоналу й кінцевих користувачів;
- амортизаційні відрахування від вартості обладнання та ПЗ;
- заробітна плата персоналу;
- навчальні курси й сертифікація обслуговуючого персоналу;
- технічне й організаційне адміністрування й сервіс.

До експлуатаційних витрат віднесено:

- заробітну плату співробітника системного адміністратора;
- витрати на ліцензію антивірусу;
- витрати на резервне копіювання;
- витрати на розробку та впровадження алгоритму захисту;
- витрати на ліцензію іншого ПЗ.

Річні поточні витрати на функціонування системи заходів протидії загрозам інформації визначаються за формулою (3.3):

$$C = C_1 + C_2 + \ldots + C_n, \text{ грн}, \quad (3.3)$$

де С – вартість підтримки заходу протидії загрозам інформації;

n – порядковий номер заходів протидії загрозам інформації.

Обліком носіїв інформації, резервним копіюванням, підтримкою антивірусу та інших ПЗ займається системний адміністратор.

Заробітна плата системного адміністратора складає $З_{СА} = 200$ грн/год.

Час на резервне копіювання займе 2 год/тиждень:

$$C = ТС^* Ф = 200*1*50 = 10000 \text{ грн.}$$

Час на підтримку AD RMS Windows Server 2019 займе 1 год/тиждень, затрати:

$$C = ТС^* Ф = 200*1*50 = 10000 \text{ грн.}$$

Час на підтримку антивірусного захисту займе 1 год/тиждень, затрати:

$$C = ТС^* Ф = 200*1*50 = 10000 \text{ грн.}$$

Час на коригування алгоритму - 1 год/тиждень:

$$C = ТС^* Ф = 200*1*50 = 10000 \text{ грн.}$$

Затрати на продовження ліцензії AD RMS Windows Server 2019 складають 19500 грн.

Затрати на продовження ліцензії ESET NOD32 складають 0 грн.

Значення загальних річних поточних витрат складає:

$$C = 10000 + 10000 + 10000 + 10000 + 19500 = 59500 \text{ грн.}$$

3.4 Визначення збитку від поломок обладнання

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

Вихідні дані для підрахунку збитку:

- час простою внаслідок поломки, $t_п$ (в годинах), $t_п = 3$ год.;
- час відновлення після поломки, $t_в$ (в годинах), $t_в = 3$ год.;
- час повторного введення втраченої інформації, $t_{ви}$ (в годинах), $t_{ви} = 3$ год.;
- заробітна плата обслуговуючого персоналу, Z_0 (грн. в місяць з податками), $Z_0 = 25000$ грн.;
- заробітна плата співробітників, Z_c (грн. в місяць з податками), $Z_c = 20000$ грн.;
- кількість обслуговуючого персоналу, N_0, $N_0 = 2$;
- число співробітників, N_c, $N_c = 7$;
- прибуток, O (грн. на рік), $O = 9000000$ грн.;
- вартість заміни обладнання та запасних частин, виправлення помилок в роботі системи, $П_{зч}$ (грн.), $П_{зч} = 5000$ грн;
- число зламаного обладнання, I, $I = 2$;
- число поломок на рік, n, $n = 4$.

Вартість втрат від зниження продуктивності співробітників несправного обладнання розраховується за формулою 3.4:

$$П_п = \frac{\sum Z_c}{\frac{N_c}{160}} \cdot t_п, \text{ грн.,} \quad (3.4)$$

де місячний фонд робочого часу при 40-а годинному робочому тижні 160 годин.

Підставивши вихідні дані отримаємо:

$$П_п = (7*20000/160)*3 = 2625 \text{ грн.}$$

Вартість відновлення зламаного обладнання розраховується за формулою 3.5:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \text{ грн.} \quad (3.5)$$

де $П_{ви}$ – вартість повторного введення інформації (формула 3.6),

$П_{пв}$ – вартість відновлення обладнання (формула 3.7).

$$П_{ви} = \frac{\sum Z_c}{\frac{N_c}{160}} \cdot t_{ви}, \text{ грн.} \quad (3.6)$$

$$П_{пв} = \frac{\sum Z_o}{\frac{N_o}{160}} \cdot t_в, \text{ грн.} \quad (3.7)$$

Отримаємо:

$$П_{ви} = (7*20000/160)*3 = 2625 \text{ грн.}$$

$$П_{пв} = (2*25000/160)*3 = 937,5 \text{ грн.}$$

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

$$П_{зч} = 5000 \text{ грн.}$$

Підставивши отримані результати в загальну формулу отримаємо:

$$П_в = 2625 + 937,5 + 5000 = 8562,5 \text{ грн.}$$

Втрачена вигода від простою зламаного обладнання становить та розраховується за формулою 3.8 й 3.9 відповідно:

$$U = П_п + П_в + V, \text{ грн.} \quad (3.8)$$

$$V = \frac{O}{Fг} \cdot (t_п + t_в + t_{ви}), \text{ грн,} \quad (3.9)$$

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

V = (9000000/2080)*(3+3+3) = 38942,31 грн.

U = 2625 + 8562,5 + 38942,31 = 50129,81 грн.

Таким чином, загальний збиток від поломки обладнання, повторного введення інформації в системі, виявлення та усунення помилок в системі складе (формула 3.10):

$$ОУ = \sum_n \sum_I U, \text{ грн.} \quad (3.10)$$

ОУ = 4 * 2 * 50129,81 = 401038,48 грн.

3.5 Загальний ефект від впровадження моделі

Загальний ефект від впровадження алгоритму для компанії визначається за формулою 3.11 з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = ОУ \cdot R - C, \text{ грн,} \quad (3.11)$$

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

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

C – щорічні витрати на експлуатацію моделі підтримки прийняття рішень оцінки загроз інформаційній безпеці для підприємства, грн.

Таким чином, загальний ефект від впровадження становить:

E = 401038,48 * 0,25 – 59500 = 40759,62 грн.

3.6 Визначення та аналіз показників економічної ефективності моделі

Оцінка економічної ефективності моделі здійснюється на основі визначення та аналізу коефіцієнта повернення інвестицій *ROSI* (Return on Investment for Security) за формулою 3.12 та терміну окупності капітальних інвестицій T_o за формулою 3.13.

$$ROSI = \frac{E}{K}, \text{ частки одиниці,} \qquad (3.12)$$

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

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

Підставивши відповідні значення, маємо:

$$\text{ROSI} = 40759{,}62 / 42796 = 0{,}95$$

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

Проєкт визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості.

Отже, проєкт є економічно доцільним.

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI}, \text{ років.} \qquad (3.13)$$

Підставимо значення:

$$T_o = 1 / 0{,}95 = 1 \text{ рік.}$$

3.7 Висновок

У даному розділі було доведено економічну доцільність і обґрунтовано впровадження інформаційної політики безпеки, що показано шляхом розрахунку:

– капітальних витрат на придбання та установку програмного забезпечення;

– експлуатаційних витрат на утримання та обслуговування програмного забезпечення;

– передбачуваних збитків від атак.

Розрахунки показали, що у випадку атаки на корпоративну мережу підприємства вартість збитків буде значно вищою, ніж вартість запропонованих засобів захисту.

Термін окупності капітальних інвестицій складатиме 1 рік. Отже, економічна доцільність обґрунтована і впровадження інформаційної політики безпеки може бути ефективним та успішним.

ВИСНОВКИ

З розвитком інформаційних технологій, зокрема інформаційних систем, змінилися базові концепції щодо їх управління. Аналіз розвитку комерційних програм мережного і системного адміністрування дозволяє зробити висновок, що ідея адміністрування зводиться до аналізу поводження інформаційної системи, або окремих її компонентів з метою своєчасного прийняття запобіжних засобів, що, в свою чергу, дає змогу не допустити розвиток подій по найгіршому сценарію.

Мета інформаційної безпеки — забезпечити безперебійну роботу організації і звести до мінімуму збиток від подій, що таять загрозу безпеці, за допомогою їх запобігання і зведення наслідків до мінімуму.

В даній кваліфікаційній роботі було детально проаналізовано нормативно-правову базу України у сфері захисту інформації. Було обрано основні нормативні документи щодо захисту статистичної інформації. Було визначено основні задачі щодо забезпечення конфіденційності статистичних даних.

У спеціальній частині було проведено детальне обстеження об'єкта інформаційної діяльності. В підрозділі 2.3 Аналіз ризиків було наведено детальну класифікацію щодо циркулюючої інформації та визначені основні загрози.

Процес розробки політики дуже важливий, тому що дуже велику частину загроз можна суттєво знизити за допомогою організаційних заходів, без витрачання великої кількості грошей на технічні засоби захисту інформації. Також було прораховано скільки потрібно бути витрати коштів для впровадження даної політики безпеки.

Таким чином було самостійно розроблено елементи політики безпеки для відділу статистики, що спрямовані на:

- розмежування доступу;
- правила політики безпеки для програмних засобів;
- правила політики безпеки антивірусного захисту.

ПЕРЕЛІК ПОСИЛАНЬ

1. НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».
2. ДСТУ 3396.0-96 «Захист інформації. Технічний захист інформації. Основні положення».
3. ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт».
4. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.
5. КСЗІ_3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».
6. Закон України «Про інформацію».
7. Закон України «Про державну статистику».
8. Закон України «Про державну таємницю».
9. Закон України «Про захист інформації в автоматизованих системах».
10. Стандарт ISO 27001.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	1	
4	А4	Вступ	2	
5	А4	Розділ 1	16	
6	А4	Розділ 2	47	
7	А4	Розділ 3	9	
8	А4	Висновки	1	
9	А4	Перелік посилань	1	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	2	

ДОДАТОК Б. Перелік документів на оптичному носії.

1. Презентація_ Сидоренко.ppt
2. Кваліфікаційна робота_ Сидоренко.doc

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (прізвище, ініціали)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-20-2 Сидоренка Д.О. на тему: «Розробка політики безпеки інформації інформаційно-комунікаційної системи відділу статистики Дніпровської районної державної адміністрації»

Пояснювальна записка містить 87 сторінок, 4 рисунки, 14 таблиць, 4 додатки, 10 джерел.

Метою даної кваліфікаційної роботи є розробка політики безпеки інформації ІКС відділу статистики Дніпровської районної державної адміністрації.

В даній кваліфікаційній роботі були вирішені наступні питання: дана характеристика об'єкта захисту та існуючої системи безпеки, детально проаналізовано нормативно-правову базу України у сфері захисту інформації; обрано основні нормативні документи щодо захисту статистичної інформації; визначено основні задачі щодо забезпечення конфіденційності статистичних даних.

У спеціальній частині було проведено детальне обстеження об’єкта інформаційної діяльності, наведено детальну класифікацію щодо циркулюючої інформації та визначені основні загрози, а також розроблено інструкції щодо захисту статистичної інформації.

В економічному розділі визначені витрати на розробку і впровадження системи захисту інформації, та проведено аналіз її економічної ефективності.

Практичне значення роботи полягає в підвищенні рівня захищеності статистичної інформації, що циркулює у відділі статистики Дніпровської районної державної адміністрації.

В якості недоліків слід відзначити окремі невідповідності вимогам при оформленні та нечітке розкриття теми ризиків.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Сидоренко Д.О. заслуговує на оцінку « » та присвоєння кваліфікації «Бакалавр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
д.т.н., проф. **Корнієнко В.І.**