РЕФЕРАТ

Пояснювальна записка: 97 с., 13 табл., 9 додатків, 5 рис., 20 джерел.

Об’єкт: інформаційно-телекомунікаційна система приватного підприємства «Оберіг-сервіс».

Предмет: політика безпеки інформації інформаційно-телекомунікаційної системи приватного підприємства «Оберіг-сервіс».

Мета кваліфікаційної роботи: розробка політики безпеки щодо захисту ресурсів в інформаційно-телекомунікаційній системі приватного підприємства «Оберіг-сервіс».

В першому розділі розглянуті питання актуальності захисту інформації взагалі. Проведено аналіз нормативно-правової бази у сфері захисту інформації. Виконано постановку задач кваліфікаційної роботи.

В другому розділі описані та проаналізовані середовища функціонування інформаційно-телекомунікаційної системи компанії. Проведено класифікацію джерел загроз та вразливостей. Складені модель порушника та модель загроз. Розроблені політики безпеки для приватного охоронного підприємства «Оберіг-сервіс».

В третьому розділі визначено економічну доцільність впровадження ПБ. Проведено розрахунки капітальних витрат, поточних витрат, оцінки величини збитку та загальний ефект від впровадження КСЗІ

ПОЛІТИКА БЕЗПЕКИ, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА ОХОРОННИХ ПІДПРИЄМСТВ, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА.

РЕФЕРАТ

Пояснительная записка: 97 с., 13 табл., 9 прилож., 5 рис., 20 источников.

Объект: информационно-телекоммуникационная система частного предприятия «Оберег-сервис».

Предмет: политика безопасности информации информационно-телекоммуникационной системы частного предприятия «Оберег-сервис».

Цель квалификационной работы: разработка рекомендаций по защите ресурсов в информационно-телекоммуникационной системе частного предприятия «Оберег-сервис».

В первом разделе рассмотрены вопросы актуальности защиты информации вообще. Проведен анализ нормативно-правовой базы в сфере защиты информации. Выполнена постановка задач квалификационной работы.

Во втором разделе описаны и проанализированы среды функционирования информационно-телекоммуникационной системы компании. Проведена классификация источников угроз и уязвимостей. Составлены: модель нарушителя и модель угроз. Разработаны политики безопасности для частного охранного предприятия«Оберег-сервис».

В третьем разделе определена экономическая целесообразность внедрения ПБ. Проведены расчеты капитальных затрат, текущих расходов, оценки величины ущерба и общий эффект от внедрения КСЗИ.

ПОЛИТИКА БЕЗОПАСНОСТИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОХРАННЫХ ПРЕДПРИЯТИЙ, ОБЪЕКТ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ, МОДЕЛЬ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ.

ABSTRACT

An explanatory Note: 97p., 13 tables., 9 applications, 5 pic., 20 sources

The object is information and telecommunication system of “Oberig-service” PE.

The subject: information security policy of information activity object.

The purpose of the study: developing the security policy in information and telecommunication system.

The first part of the study contains an analysis of regulatory documentation in information security, set tasks for the implementation of the information security system for information activity object where the information circulates.

The second part of the study considers the general statements about the enterprise; organizational structure of the computer system are contained.Information activity object`s environment for the functioning; risk assessment; threat analysis of information security; main elements of the information security policy ofinformation and telecommunication system are analyzed; the main regulations of the security policy are formulated.

In third part defines economic feasibility of implementing an information security policy. The calculations of capital (fixed) costs, current (operational) costs, a calculation of loss and the effect of the implementation of information security. Economic efficiency indicators of information system security are analyzed.

The analyses provide the opportunity to use the developed security policy for implementation in the information and telecommunication system of the enterprise.

SECURITY POLICY, INFORMATION SECURITY, INFORMATION SECURITY OF SECURITY COMPANY, INFORMATION ACTIVITY OBJECT, MODEL OF THREATS, USER VIOLATOR MODEL

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ЕОТ – електронно-обчислювальна техніка;

ЗУ – закон України;

ІБ – інформаційна безпека;

ІТС – інформаційно-телекомунікаційна система;

КСЗІ – комплексна система захисту інформації;

НСД – несанкціонований доступ;

ОІД – об'єкт інформаційної діяльності;

ОС – операційна система;

ПБ – політика безпеки;

ПЕОМ – персональна електронно-обчислювальна машина;

ПЗ – програмне забезпечення;

ПП – приватне підприємство;

ТЗІ – технічні засоби інформації.

ЗМІСТ

ВСТУП..... 9
РОЗДІЛ 1.СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ..... 10
1.1 Стан питання..... 10
1.2 Аналіз нормативно-правової бази у сфері захисту інформації..... 12
1.3 Постановка задачі..... 18
Висновки до розділу 1..... 19
РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА..... 20
2.1 Загальні відомості про приватне підприємство «Оберіг-сервіс»..... 20
2.2 Обґрунтування необхідності створення КСЗІ..... 20
2.3 Обстеження на об’єкті інформаційної діяльності..... 21
2.4 Аналіз загроз інформації, що циркулює на ОІД..... 32
2.4.1 Визначення інформаційних ресурсів на підприємстві, що потребують захисту..... 32
2.4.2 Визначення переліку загроз..... 35
2.4.3 Визначення переліку порушників..... 42
2.4.4 Визначення каналів несанкціонованого доступу до ІТС..... 45
2.4.5 Вибір заходів захисту інформації в ІТС підприємства..... 46
2.4.6 Критерії впровадження системи..... 51
2.5 Розробка політики безпеки для підприємства..... 63
2.5.1 Політика безпеки для системного адміністратора..... 63
2.5.2 Політика антивірусного захисту..... 66
2.5.3 Політика чистого столу..... 67
Висновок до розділу 2..... 68

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА……...…70
3.1 Необхідність обґрунтування витрат на реалізацію політики безпеки……70
3.2 Визначення трудомісткості розробки політики безпеки 70
3.3 Розрахунки капітальних (фіксованих) витрат 72
3.4 Розрахунки поточних (експлуатаційних) витрат 73
Висновок до розділу 3 78
ВИСНОВКИ 79
ПЕРЕЛІК ПОСИЛАНЬ 80
ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ КВАЛІФІКАЦІЙНОЇ РОБОТИ 83
ДОДАТОК Б. СИТУАЦІЙНИЙ ПЛАН 84
ДОДАТОК В. ГЕНЕРАЛЬНИЙ ПЛАН 86
ДОДАТОК Г. СХЕМА ПІДКЛЮЧЕННЯ МЕРЕЖІ 89
ДОДАТОК Ґ. СХЕМА ІНФОРМАЦІЙНИХ ПОТОКІВ 91
ДОДАТОК Д. НАКАЗ НА СТВОРЕННЯ КСЗІ 93
ДОДАТОК Е. ПЕРЕЛІК ДОКУМЕНТІВ НА ОПТИЧНИМУ НОСІЇ 94
ДОДАТОК Ж. ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ 95
ДОДАТОК З. ВІДГУК КЕРІВНИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ 96

ВСТУП

У сучасному суспільстві процес інформатизації набув глобального змісту. Інформатизація охоплює увесь спектр поточних і перспективних проблем – економічних, організаційних, соціальних, розвиток культури та освіти, діяльності всіх ланок соціального управління. Вона сприяє забезпеченню національних інтересів, поліпшенню керованості економікою, розвитку наукових виробництв та високих технологій, зростанню продуктивності праці, вдосконаленню соціально-економічних відносин. Тому питання державного регулювання сфери інформатизації стає усе більш актуальним та важливим у сучасному житті суспільства та держави.

В Україні процес інформатизації здійснюється згідно з Національною програмою інформатизації, яка визначає стратегію розв'язання проблеми забезпечення інформаційних потреб та інформаційної підтримки соціально-економічної, екологічної, науково-технічної, оборонної, національно-культурної та іншої діяльності у сферах загальнодержавного значення. Майже в кожній інформаційній системі знайдеться така інформація, розголошення якої стороннім особам може нанести збитків її власнику або ж людині, якої стосується інформація. Особливо актуальним стає питання інформаційної безпеки (ІБ) на підприємствах, організаціях, в яких обробляється інформація з обмеженим доступом.

Одним з етапів побудови КСЗІ є розробка політики безпеки. Чим правильніше та точно буде створена політика безпеки, тим простіше буде адміністраторам безпеки розробити комплекс заходів для того, щоб запобігти атакам. Важливу роль в розробці політики безпеки є визначення можливих загроз та порушень у організаціях і підприємствах.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Швидкий розвиток інформаційних технологій призвів до зростання відносної важливості окремих аспектів суспільного життя. На сьогоднішній день, однією з основних цінностей для суспільства взагалі й окремої людини зокрема стала інформація.

На забезпечення інформаційної безпеки мільйони підприємств по всьому світові витрачають чимало грошей. Це обумовлено поступовим зростанням рівня інформаційної злочинності. Але аналізуючи сучасний стан та тенденцій розвитку вітчизняного інформаційного простору слід зазначити, що рівень інформаційної безпеки в Україні, за окремими показниками, дуже низький.

З розвитком комерційної та підприємницької діяльності збільшилась кількість спроб несанкціонованого доступу (НСД) до ІзОД, а проблеми її захисту значно підвищили потребу у фахівцях із захисту інформації.

За опублікованими даними, порушення захисту комп'ютерних систем через НСД відбувається лише у 2 % випадків. У 3 % – через укорінення вірусів, у 20 % – за технічних відмов апаратури мережі, ще у 20 % – через цілеспрямовані дії персоналу та у 55 % – через помилки персоналу обумовлені недостатнім рівнем кваліфікації.

Таким чином, незважаючи на важливість захисту інформації від НСД, все ж таки, більших збитків може нанести саме персонал.

Останнім часом набувають особливої актуальності підприємства, що займаються забезпеченням охорони та захисту, в тому числі й інформації. Охоронні підприємства є об'єктивним досягненням сучасного суспільства, без котрих неможливо в наш час почуватися безпечно та забезпечувати надійне та всебічне збереження майна та інформації. На сучасному етапі розвитку України як незалежної держави особливого значення набуває рівень регулювання охоронних підприємств. На сьогодні в Україні сформована певна нормативно-

правова база, на основі якої здійснюється охоронна діяльність. Але її аналіз свідчить про те, що вона значною мірою застаріла, суперечлива, містить багато прогалин, не відповідає сучасній практиці охоронної діяльності, науковим розробкам в цій сфері. У нашій державі немає закону, який би охоплював усі можливі аспекти здійснення охоронної діяльності, повноваження суб'єктів охоронної діяльності, гарантії правового і соціального захисту персоналу охорони, гарантії прав замовників охоронних послуг, фізичних і юридичних осіб під час здійснення охоронної діяльності, порядок контролю над її здійсненням, а також загальні принципи взаємодії суб'єктів охоронної діяльності з державними органами правопорядку і боротьби із злочинністю. Процес створення єдиної комплексної системи забезпечення безпеки, що охоплює державні правоохоронні органи та недержавні охоронні структури відстає від темпів криміналізації економіки країни і потребує інтенсифікації. Необхідне створення та прийняття законів, які б регулювали здійснення охоронної діяльності, у тому числі і приватної, та створювали б необхідні рівні умови всім суб'єктам охоронної діяльності, включаючи Закони «Про охоронну діяльність», «Про охоронну діяльність суб’єктів недержавної форми власності», «Про зброю» та інші Закони, створення комплексної системи нормативних документів всіх рівнів. На даний час в Україні тема захищеності охоронних підприємств ще не знайшла належного наукового дослідження, тому практично не існує сформованих наукових організацій, які б займалися дослідженням даної проблеми так, як цього вимагає життя. Ефективне регулювання безпеки охоронних підприємств, як і будь якої іншої сфери діяльності можливе лише за наявності комплексної системи нормативних документів, що охоплює державний, галузевий (відомчий) і виконавчий (охоронного підприємства) рівні. На практиці ж є лише документи державного рівня. Але і вони не охоплюють всі необхідні аспекти проблеми захисту підприємництва у сфері охоронної діяльності. Нормативних документів інших рівнів практично немає.

Такі підприємства є найбільш вразливими, бо мають велику кількість персональних даних та конфіденційної інформації, котрою бажає заволодіти зловмисник. Тому виникає необхідність перегляду підходів до забезпечення інформаційної безпеки таких підприємств та передбачає необхідність створення відповідних систем її захисту.

1.2 Аналіз нормативно-правової бази у сфері захисту інформації

Нормативно-правове забезпечення щодо захисту інформації - сукупність законів, нормативних актів та інших документів, що регламентують загальну організацію робіт, створення і функціонування конкретних систем захисту інформації.

Головною складовою правового забезпечення у сфері захисту інформації є стандартизація, метою якої є:

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

– сталість вимог по захисту інформації в засобах обчислювальної техніки, в інформаційно-телекомунікаційних системах.

Тобто, нормативно-правове забезпечення визначає порядок захисту визначених політикою безпеки властивостей інформації (конфіденційності, цілісності та доступності) під час створення та експлуатації інформаційної мережі; регламентує порядок ефективного знешкодження і попередження загроз для ресурсів шляхом побудови комплексної системи захисту інформації; статус інформаційної системи з точки зору інформаційної безпеки; права, обов'язки й відповідальність персоналу роботи яких пов’язані з інформаційною безпекою; етапи побудови КСЗІ [27,с.9]. Під час створення комплексної системи захисту інформації, як сукупності організаційних і інженерних заходів, програмно-апаратних засобів, слід керуватися низкою нормативно-правових документів та актів.

Захист інформації в інформаційно-телекомунікаційній системі визначається:

– законами України, іншими нормативно-правовими актами України;

– державними стандартами та іншими нормативними документами з стандартизації;

– нормативно-правовими актами і нормативними документами системи технічного захисту інформації в Україні;

– нормативними, організаційно-розпорядчими та іншими документами, чинними у межах ІТС або організації.

Закони України, інші нормативно-правові акти України, державні стандарти, нормативно-правові акти і нормативні документи системи технічного захисту інформації в Україні формують та впроваджують єдиний в державі порядок забезпечення захисту інформації в ІТС.

Нормативні, організаційно-розпорядчі та інші документи, що використовуються у межах окремої організації або ІТС, враховують особливості та умови технології обробки інформації в цій організації або ІТС. Ці документи розробляються власником або розпорядником ІТС.

Розробленню підлягають документи, визначені політикою безпеки інформації. При розробленні цих документів дозволяється поєднувати декілька з них у вигляді окремих розділів в одному документі [7].

В усіх нижчезазначених нормативних документах, а також у роботі в цілому, використовуються терміни і визначення, що відповідають встановленим нормативним документом ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» [18], або в інших нормативних документах з технічного захисту інформації, що вказані у розділі «Визначення».

Правовою основою забезпечення безпеки інформації в Україні є ряд документів, серед яких слід виділити:

– Закон України «Про інформацію» [4];

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [2];

– Закон України «Про захист персональних даних» [3];

– стандарти ДСТУ ISO/IEC, що основані на міжнародних стандартах і відповідно до вимог, що висуваються до захисту інформації на підприємстві;

– нормативні документи з технічного захисту інформації, опис яких приведено нижче;

– ДСТУ 3396.1-96 - Технічний захист інформації. Порядок проведення робіт [1];

– Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 № 373;

– Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ЕОТ-95);

– Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 р. №1229.

Закон України «Про інформацію»[4] визначає основи одержання, використання, поширення і збереження інформації. Він 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. У статтях закону визначаються категорії інформації і режим доступу до неї.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»[2] регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах; визначає об`єкти та суб`єкти захисту в системі; встановлює відносини між власником системи, користувачами та володільцем інформації.

НД ТЗІ 1.1-002-99 [5] визначає концепцію вирішення завдань захисту інформації в комп'ютерних системах та має за мету вирішення питань:

– визначення вимог щодо захисту комп'ютерних систем від несанкціонованого доступу;

– створення захищених комп'ютерних систем і засобів їх захисту від несанкціонованого доступу;

– оцінки захищеності комп'ютерних систем і їх придатності для вирішення завдань споживача.

НД ТЗІ 1.1-005-07 [7] визначає основи організації та етапи виконання робіт щодо створення комплексу на ОІД підприємства, яке має забезпечувати захист від витоку інформації з обмеженим доступом.

Зміст цього документу можуть використовуватися під час обґрунтування, організації розроблення, впровадження заходів захисту ІзОД від загроз.

НД ТЗІ 1.4-001-2000 [8] із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806, встановлює вимоги до структури та змісту нормативного документу, що регламентує діяльність служби захисту інформації в автоматизованій системі. Документ призначений для власників ІТС та користувачів, діяльність яких пов’язана з обробкою в автоматизованих системах інформації, що підлягає захисту згідно з нормативно-правовими актами, а також для розробників комплексних систем захисту інформації в автоматизованих системах.

Використання цього НД ТЗІ створює умови для запровадження єдиного підходу щодо визначення і формування завдань, функцій, структури, повноважень служби захисту інформації, а також організації її робіт з захисту автоматизованих на підприємстві.

В документі визначені функції служби захисту інформації з організації навчання персоналу з питань забезпечення захисту інформації; під час створення комплексної системи захисту інформації; під час експлуатації комплексної системи захисту інформації. Прописані права, обов`язки та відповідальність працівників служби захисту інформації.

НД ТЗІ 1.6-005-2013 [9] визначає загальні вимоги з категоріювання, ознаку, за якою здійснюється категоріювання, а також порядок категоріювання об’єктів інформаційної діяльності, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.

Положення є обов’язковим для підприємств незалежно від форми власності, на об’єктах яких обробляється технічними засобами та/або озвучується інформація з обмеженим доступом, що не становить державної таємниці.

НД ТЗІ 3.1-001-07 [12] визначає основні положення щодо проведення передпроектних робіт при створенні на об'єкті інформаційної діяльності підприємства ТЗІ, який має забезпечувати захист від витоку інформації з обмеженим доступом технічними каналами.

Цим НД встановлюються порядок та зміст проведення передпроектних робіт на ОІД, які вже функціонують або модернізуються, вимоги до оформлення акта обстеження на ОІД, а також вимоги до порядку розроблення та оформлення технічного завдання на створення комплексу ТЗІ.

НД ТЗІ 3.3-001-07 [13] визначає порядок проведення робіт під час створення комплексу ТЗІ на об’єкті інформаційної діяльності підприємства на етапі розроблення та впровадження заходів із захисту від витоку інформації з обмеженим доступом технічними каналами.

НД ТЗІ 3.7-003-05 [15] визначає основи організації та порядок виконання робіт із захисту інформації в інформаційно-телекомунікаційних системах - порядок прийняття рішень щодо складу комплексної системи захисту інформації в залежності від умов функціонування ІТС і видів оброблюваної інформації, визначення обсягу і змісту робіт, етапності робіт, основних завдань та порядку виконання робіт кожного етапу.

Нормативний документ призначений для суб'єктів інформаційних відносин, діяльність яких пов'язана з обробкою інформації, що підлягає захисту; розробників комплексних систем захисту інформації в ІТС; для постачальників компонентів ІТС, а також для фізичних та юридичних осіб, які здійснюють оцінку захищеності оброблюваної інформації на відповідність вимогам ТЗІ.

Встановлений цим НД ТЗІ порядок є обов'язковим для всіх суб'єктів системи ТЗІ в Україні незалежно від їхньої організаційно-правової форми та форми власності, в ІТС яких обробляється інформація, яка належить до державних інформаційних ресурсів, належить до державної чи іншої таємниці або окремих видів інформації, необхідність захисту якої визначено законодавством. Якщо в ІТС обробляються інші види інформації, то вимоги цього нормативного документа суб'єкти системи ТЗІ можуть використовувати як рекомендації.

ДСТУ 3396.1-96 [1] установлює вимоги до порядку проведення робіт з технічного захисту інформації, що є обов`язковими для підприємств та установ усіх форм власності й підпорядкування.

Необхідність впровадження на реальному підприємстві комплексної системи захисту інформації продиктована вимогами стандартів України з управління інформаційною безпекою.

Відповідно до Закону України «Про інформацію», на підприємстві може циркулювати інформація відкрита та інформація з обмеженим доступом (ІзОД). Остання має бути захищена від несанкціонованого доступу. Такий поділ за

режимами доступу здійснюється виключно на підставі ступеня конфіденційності інформації. Поряд з конфіденційністю істотними характеристиками інформації є її цілісність і доступність, проте на сьогоднішній день іншої класифікації інформації, крім наведеної, не запроваджено. З метою збереження загальності викладу далі в тексті замість терміну «інформація з обмеженим доступом» використовується термін «інформація», який має на увазі будь-яку інформацію, щодо якої регламентовані певні вимоги до забезпечення її конфіденційності, цілісності та доступності.

Поняття інформація з обмеженим доступом встановлено у НД ТЗІ 1.1-005-07 [7] зі змінами згідно наказу Адміністрації Держспецзв`язку від 03.11.2011 №93/ДСК «Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення»: ІзОД – інформація, що становить державну або іншу передбачену законом таємницю, а також службова інформація, а також конфіденційна інформація, яка перебуває у володінні розпорядників інформації та інша конфіденційна інформація, вимога щодо захисту якої встановлена законом.

1.3 Постановка задачі

На даний час в Україні досить високий рівень кіберзлочинності, саме через те підприємства, що займаються забезпеченням безпеки підлягають високому ризику витоку інформації за межі тих самих підприємств. Для підприємств, що займаються охоронною діяльністю, важливо завжди бути на крок попереду злочинців.

Тож, з огляду на важливість забезпечення інформаційної безпеки, в роботі повинна бути розроблена політика безпеки інформації інформаційно-телекомунікаційної система приватного підприємства "Оберіг-сервіс" для чого необхідно:

- провести обстеження фізичного середовища підприємства;

- провести обстеження інформаційного середовища та обчислювальної системи;
- провести обстеження середовища користувачів;
- провести класифікацію джерел загроз та вразливостей;
- скласти модель загроз та порушника;
- розробити політику безпеки підприємста та економічно обгунтувати доцільність її впровадження.

Висновки до розділу 1

У даному розділі розглянуто актуальний стан злочинів в сфері інформаційної безпеки та виявлено значне збільшення інцидентів порушення інформаційної безпеки на території України.

В розділі приведено перелік нормативно-правових документів в сфері захисту інформації, зазначено основні положення.

Розглянуто основні небезпеки інформаційній безпеці підприємств, що займаются охоронною діяльністю та особливості створення політик безпеки для цих підприємств, виконано постановку задачі.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про приватне підприємство «Оберіг-сервіс»

“Оберіг-сервіс” – приватне охоронне підприємство, що надає спеціалізовані галузеві і комплексні послуги з фізичної, технічної, інформаційної, банківської, пожежної та техногенної безпеки.

Адреса: 51200, м. Новомосковськ, вул. Леваневського 54.

Специфікація діяльності ОІД:

Технічний відділ працює за програмним забезпеченням інформаційно-комунікаційних системи приватного підприємства "Оберіг-сервіс"

Час роботи понеділок-п’ятниця з 8:00 – 17:00, перерва 12:00 – 13:00, субота – неділя вихідні дні.

2.2 Обґрунтування необхідності створення КСЗІ

Підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства, які встановлюють обов’язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, або прийняте власником інформації рішення щодо цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд.

«Згідно ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах» умови обробки інформації в системі визначаються власником системи відповідно договору з власником інформації, якщо інше не передбачено законодавством. Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються власником інформації.»

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

2.3 Обстеження на об’єкті інформаційної діяльності

Об’єктом інформаційної діяльності (далі ОІД) є інформаційно-телекомунікаційних система приватного підприємства "Оберіг-сервіс"

Обстеження на об’єкті інформаційної діяльності проведено відповідно до Методичних вказівок щодо структури та змісту Плану захисту інформації в автоматизованій системі – НД ТЗІ 1.4-001-2000 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 – Типове положення про службу захисту інформації в АС, здійснено обстеження середовищ функціонування. Акт оформлено відповідно до Додатку А. «Форма та зміст акта обстеження на об'єкті інформаційної діяльності стосовно створення комплексу ТЗІ, НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи». Порядок проведення обстеження відповідає ДСТУ 3396.1.

Під час обстеження розглянуто середовище функціонування ІТС: обчислювана система, фізичне середовище, середовище користувачів та оброблювана інформація. Приводиться опис кожного середовища функціонування ІТС.

Відповідно до НД ТЗІ 1.6-005-2013 «Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці», ОІД, що розглядається встановлюється категорія IV (четверта) адже на об'єкті технічними засобами обробляється інформація з обмеженим доступом, що не становить державної таємниці.

Обстеження фізичного середовища: характеристика ОІД, де розташована та функціонує інформаційно-телекомунікаційна система.

ІТС розміщена в приміщенні за адресою: 51200, м. Новомосковськ, вул. Леваневського 54.

Будівля одноповерхова, ОІД розташований в орендованому офісі загальною площею 40.3 $м^2$. На території діє пропускний режим та є цілодобова охорона.

Схема розташування ОІД та об'єктів навколо нього наведена на ситуаційному плані (Додаток Б. рисунок 1). На генеральному плані зазначені схеми відеоспостереження та охоронної сигналізацій (Додаток Г. рисунок 2).

Характеристика складових ОІД:

– висота стель – 420 м;

– перекриття – 500 мм;

– стінні перегородки – 150 мм;

– стіни зовнішні з цегли – 500 мм.

Вікна: двостулковий метало-пластиковий склопакети у всіх приміщеннях розміром 1400х1320 мм. Віконні отвори обладнані регульованими пристроями типу: ролетні жалюзі.

Двері в приміщення металеві 2700х900. Дверні петлі захищені анти зрізами. Захисна металева внутрішня розсувна решітка на двері при вході до ОІД.

Система електроживлення (освітлення): мережа 220В; автономний агрегат електроживлення відсутній; світильники з LED лампами. Кабельне підключення до Інтернет – екранована віта пара UTP 4х2х0,5 5е в коробі.

Система опалювання – автономна. Система вентиляції – проточно-витяжна. Заземлення – наявне. Системи сигналізації:

– пожежна – димовий сповіщувач СПД 3, ручний пожежний сповіщувач, шлейфи по стелі, прибор Лунь 7П, сигнальні пристрої;

– охоронна – магнітно-контактні датчики на відкриття дверей та вікон, оптичні датчики руху Swan – 2, клавіатура, централь.

Підключення – екранований дріт 4х2.

Будівля обладнана системами електроживлення, опалення, водопостачання та каналізації, автоматичною пожежною сигналізацією.

Живлення систем освітлення, електропостачання та опалення здійснюється через підключення до міських комунальних мереж. Система пожежної сигналізації підключена на центральний пульт.

На вході до будівлі розташована відомча охорона, що забезпечує пропускний режим до приміщень та здійснює цілодобову охорону. На фасаді приміщення встановлена система відеоспостереження з візуальним контролем охороною приміщення на вході в будівлю.

Таблиця 2.1 - Системи комунікації

Електропостачання	Підключено до трансформаторної підстанції №3, яка має сторонніх споживачів і знаходиться за межами КЗ
Система опалення	Підключена до міської мережі опалення, знаходиться за межами КЗ (пластикові труби, однотрубна вертикальна система опалення)
Система каналізації	Підключена до міської мережі, яка знаходиться за межами КЗ
Система водопостачання	Підключена до міського водоканалу, яка знаходиться за межами КЗ (пластикові труби, однотрубна вертикальна система опалення)
Заземлення	Всі прилади, комп'ютери заземлені на спільний контур заземлення, який є замкнутий і виходить за межі КЗ
Система вентиляції	Приточно-витяжна
Internet	Кабельне підключення, що виходить за межі ОІД

Штат співробітників підприємства складається з 19 осіб: директор, бухгалтер, системний адміністратор, чотири диспетчери, 12 охоронників. На рисунку 2.1 зображена організаційна структура робітників підприємства.

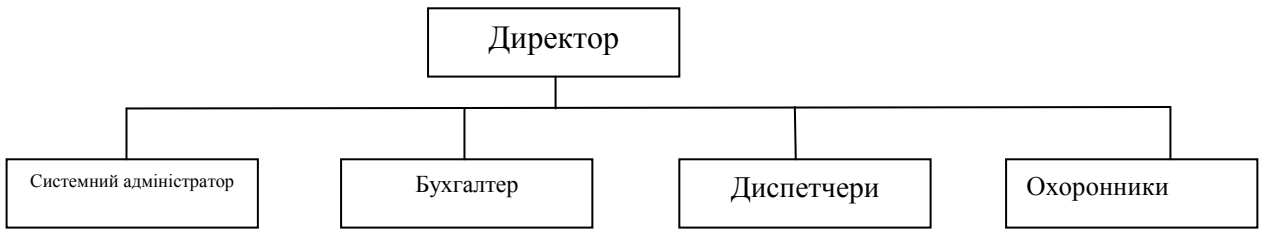


Рисунок 2.1 Організаційна структура

Відповідно до рівня повноважень с приводу доступу до інформації, характеру робіт, які виконуються у процесі функціонування ІТС, користувачі системи мають різний рівень доступу до ІТС.

Обов'язки персоналу зазначені в їх посадових інструкціях відповідно до посади, яку вони займають.

Обов'язки директора:

– приймати рішення в рамках своїх функціональних обов'язків, визначених у Статуті підприємства, та згідно з діючим законодавством України;

– здійснення добору та розстановки персоналу;

– визначати, формулювати і координувати всі види діяльності підприємства;

– визначати напрями розвитку підприємства в усіх видах діяльності;

– здійснення кадрової роботи;

– розробляти посадові інструкції, внутрішні документи та інші документи.

Обов’язки системного адміністратора:

– здійснення інсталяції, налагодження системного програмного забезпечення;

– проводження комп'ютерних антивірусних заходів;

– адміністрування локальної обчислювальної мережі підприємства;

– організація супроводження договорів із сторонніми організаціями, що надають послуги по комунікаційнім, програмному й апаратному оснащенню підприємства;

– усування аварійні ситуації, пов'язані з ушкодженням програмного забезпечення;

– адміністрування ІТС, розмежовує доступ користувачів в системі.

Обов’язки бухгалтера:

– ведення бухгалтерського обліку, з урахуванням особливостей діяльності підприємства;

– оформлення та подання до обліку первинних документів;

– складання звітів про фінансовий стан, результати діяльності та рух коштів підприємства;

– забезпечення перерахування податків та зборів, передбачених законодавством;

– ведення інвентаризаційної роботи на підприємстві;

– підготовка оброблених документів, реєстрів і звітності для їх зберігання;

– ведення складського обліку.

Обов’язки диспетчерів:

– контроль за об’єктами, що знаходяться під охороною підприємства, в онлайн режимі;

– виклик групи реагування у випадку спрацювання сигналізації.

Обстеження функціонуваня ІТС:

Обстеження інформаційного середовища включає в себе інформацію, що планується до обробки за допомогою ІТС.

Власником інформації виступає директор. В автоматизованій системі відсутня таємна, службова інформація, а також інформація, що є власністю держави або відомості, які становлять державну таємницю.

За режимом доступу інформація, яка обробляється за допомогою ІТС поділяється на:

– інформація з обмеженим доступом (ІзОД);

– відкрита, що потребує захисту;

– відкрита, не потребує захисту.

ІзОД буде представлена в ІТС у вигляді електронних документів створених за допомогою пакету прикладних програм Microsoft Office 2010, Adobe Reader або у роздрукованому паперовому вигляді. Паперові носії інформації зберігаються в сейфі.

Правила доступу до інформації встановлені директором. Доступ до ІзОД мають тільки зареєстровані в системі користувачі. Інформація з обмеженим

доступом має цінність, тому втрата або передача може завдати підприємству матеріальний збитків.

ІзОД, що циркулює в ІТС, буде зберігатися:

– на жорсткому магнітному диску;

– на паперових носіях.

Документи, в яких містяться ІзОД, будуть друкуватися за допомогою принтерів, які входять до складу ІТС. Копіювання на гнучкі носії та флеш накопичувачі заборонені. Перелік відомостей, що становлять ІзОД, а також всі відомості за режимом доступу, за правовим режимом, а також за типом представлення в ІТС приведені та класифіковані у таблиці 2.4. Вимоги захисту встановлено власником згідно з вимогами нормативно-правових актів.

Для всіх видів інформації, представлених в таблиці, встановлюється адміністративне керування доступом. Атрибути доступу присвоюються в момент створення документа в системі. Інформація може зберігатися в системі у форматах doc,docx, xls, pdf.

Імпорт та експорт інформації в ІТС здійснюється за допомогою використання електронної пошти, сканування паперових носіїв, друку документів.

Таблиця 2.2 – Класифікація інформації

№	Опис	Правовий режим	Режим доступу	Тип представлення	Вимоги до захисту	Доступ мають
1	Організаційно-розпорядча документація	Конфіденційна	ІзОД	Зберігається в кабінеті у директора на паперовому носії та на сервері	Ц,Д	Директор, системний адміністратор
2	Облік внутрішніх документів	Конфіденційна	ІзОД	Зберігаються в кабінеті у директора на паперовому носії	К,Ц,Д	Директор, бухгалтер
3	Інформація про надання послуг, тарифи, контактна інформація підприємства	-	Відкрита, не потребує захисту	Текстова та числова інформація в цифровому та паперовому вигляді.	Ц,Д	Директор, системний адміністратор, бухгалтер
4	Інформація про робітників	Конфіденційна	ІзОД	Зберігаються в кабінеті у директора на паперовому носії	К,Ц,Д	Директор, Бухгалтер
5	Статутні документи підприємства	-	Відкрита, не потребує захисту	Зберігається в кабінеті у директора на паперовому носії	Ц.Д	Усі працівники
6	Облік та реєстрація вхідних та вихідних документів організації	Конфіденційна	ІзОД	Зберігається в кабінеті у директора на паперовому носії та на сервері	К,Ц,Д	Директор, системний адміністратор

Обстеження обчислювальної системи:

Обчислювальна система є локальною– з’єднуються пристрої, що розташовані в межах ОІД. Локальна мережа створена для забезпечення внутрішніх потреб підприємства. Існує підключення до глобальної мережі Internet для забезпечення взаємодії з зовнішніми організаціями (Державна фіскальна служба, інші фонди тощо). Канал зв’язку в межах корпоративної мережі та підключення до мережі Internet забезпечує провайдер «Київстар», який надає послуги з побудови, надання та підтримки відомчої телекомунікаційної мережі у відповідності до Договорів між «Оберіг-сервіс» та «Київстар».

Обладнання АС, за допомогою якого обробляється інформація на ОІД: робочі станції директора; робоча станція диспетчера; робоча станція системного адміністратора; робоча станція бухгалтера; БФП, що підключений до робочої станції директора; принтер формату А4, підключений до робочої станції директора та бухгалтера;. Всі робочі станції підключені до мережі Internet кабельним підключенням; роутер Wi-Fi забезпечує підключення до мережі Internet.

Спосіб з'єднання мережевих пристроїв за топологією відноситься до типу зірка. Всі комп'ютери мережі приєднані до центрального вузла, тобто роутера.

Таблиця 2.3 – Характеристика складових ІТС наявних у системі

№	Назва	Умовне позначення на схемі	IP адреса пристрою	Серійний номер	Характеристика
1	Робоча станція 1 (директора) HP Z440 (T4K25EA)	ПК3	192.168.0.104	UTY13UT76R	Intel Core i5-8400 (2.8 - 4.0 ГГц) / RAM 16 ГБ / HDD 2 ТБ + SSD 240 ГБ / Intel UHD Graphics 630 / без ОД / LAN

Продовження таблиці 2.3

№	Назва	Умовне позначення на схемі	IP адреса пристрою	Серійний номер	Характеристика
2	Робоча станція 2 (бухгалтера) HP Z440 (T4K25EA)	ПК2	192.168.0.103	KTY13UT80D	Intel Core i5-8400 (2.8 - 4.0 ГГц) / RAM 16 ГБ / HDD 2 ТБ + SSD 240 ГБ / Intel UHD Graphics 630 / LAN
3	Робоча станція 3 (системного адміністратора) HP Z440 (T4K25EA)	ПК1	192.168.0.101	RRY13UT87R	
4	Робоча станція 4 (диспетчера) HP Z440 (T4K25EA)	ПК4	192.168.0.102	RTY13RR80D	
5	Сервер	S1	192.168.111	DDY12UT87F	Dell PowerEdge R510 2 x XEON 4 Core E5620 2.4 GHz 24GB DDR3 12 слотов под диски 3.5" SATA/SAS PERC H700

Продовження таблиці 2.3

№	Назва	Умовне позначення на схемі	IP адреса пристрою	Серійний номер	Характеристика
5	БФП, підключений до ПК 3 Brother HL-L2365DWR	P1	-	JNZNR0013	Максимальна роздільна здатність друку 600x2400 dpi Технологія друку Лазерний (ч/б) Стандартний лоток: A4, Letter, A5, A6, Executive Швидкість друку: до 30 стр/хв;
6	БФП, підключений до ПК 2 Brother HL-L2365DWR	P2	-	TY JNR0013	Максимальна роздільна здатність друку 600x2400 dpi Технологія друку Лазерний (ч/б) Стандартний лоток: A4, Letter, A5, A6, Executive Швидкість друку: до 30 стр/хв;
7	БФП, підключений до ПК 1 Brother HL-L2365DWR	P3	-	UTY NR0013	Максимальна роздільна здатність друку 600x2400 dpi Технологія друку Лазерний (ч/б) Стандартний лоток: A4, Letter, A5, A6, Executive Швидкість друку: до 30 стр/хв;

Продовження таблиці 2.3

№	Назва	Умовне позначення на схемі	IP адреса пристрою	Серійний номер	Характеристика
8	Принтер, підключений до ПК 1 HP LaserJet Pro M102	РК1	-	SN03PRC05	Максимальна роздільна здатність друку 600x600 dpi Технологія друку Лазерний (ч/б) Інтерфейс USB 2.0
9	Принтер, підключений до ПК 3 Epson L1800 A3	РК2	-	CN684JZ20M	Максимальна роздільна здатність друку 5760x1440 dpi Технологія друку Струменевий Інтерфейс USB 2.0
10	Комп'ютерна миша, підключена до: ПК 1; ПК 2; ПК 3; ПК 4 Logitech Wireless Mouse M185 (910-002238) Grey	-	-	910-002238 910-003501 910-002256 910-002257	Джерело живлення 1 x AA Тип датчика Оптичний Кількість кнопок 2 Інтерфейс Wireless

Продовження таблиці 2.3

№	Назва	Умовне позначення на схемі	IP адреса пристрою	Серійний номер	Характеристика
11	Монітор, підключений до: ПК 1; ПК 2; ПК 3; ПК 4 Philips V-line 203V5LSB26 /10/62	-	-	PE19HS4P60 PE19TR5K30 PE19HS4S45 PE19NY4R69	Діагональ дисплея 19.5" Тип матриці TN+film Максимальна роздільна здатність дисплея 1600 x 900 Покриття Матове
12	Клавіатура, підключена до: ПК 1; ПК 2; ПК 3; ПК 4 Logitech K120 USB Black	-	-	C-8940 C-8745 C-8170 C-8952	Інтерфейс USB Кількість кнопок: 104 Тип: мембранна

2.4 Аналіз загроз інформації, що циркулює на ОІД

2.4.1 Визначення інформаційних ресурсів на підприємстві, що потребують захисту

Для ІТС підприємства "Оберіг-сервіс" необхідний захист наступного інформаційного ресурсу:

– файли, набори даних, які оброблюються, зберігаються і передаються в ІТС;

– системне та функціональне ПЗ;

– база даних з конфіденційними даними підприємства.

Інформаційні ресурси в ІТС циркулюють в обчислювальних засобах, а

саме оперативно-запам’ятовуючий пристрій, дисплей, принтер, сканер, клавіатура, мережеве обладнання, які являються об’єктами захисту.

Таблиця 2.4 – Визначення рівня конфіденційності, цілістності та доступності інформації

№	Інформація	Рівень конфіденційності	Рівень цілісності	Рівень доступності
1	Організаційно-розпорядча документація (зберігається в кабінеті у директора на паперовому та електронному носії)	К2	Ц4	Д4
2	Облік внутрішніх документів (накази, службові записки, інструкції) (зберігаються в кабінеті у директора на паперовому та електронному носії)	К1	Ц4	Д3
3	Інформація про надання послуг, тарифи, контактна інформація підприємства	К4	Ц3	Д3
4	Інформація про робітників (зберігається в кабінеті у директора на паперовому та електронному носії)	К1	Ц4	Д3
5	Статутні документи підприємства (документи, що дозволяють займатися підприємницькою діяльністю) (зберігається в кабінеті у директора на паперовому та електронному носії)	К4	Ц3	Д4
6	Облік та реєстрація вхідних та вихідних документів організації	К4	Ц4	Д3
7	Трудові договори робітників (зберігається в кабінеті у директора на паперовому та електронному носії)	К4	Ц4	Д2
8	Записи файлів відеоспостереження	К5	Ц5	Д5

Конфіденційність:

– К0 - розголошення інформації призводить до краху роботи суб'єкта або дуже великих матеріальних втрат;

– К1-розголошення призводить до значних матеріальних втрат, якщо не буде вжито заходів;

– К2 - розголошення призведуть до деяких матеріальних втрат;

– К3 - Приносить матеріальний збиток в певних випадках;

– К4 - може принести малозначний збиток в рідкісних випадках.

Цілісність:

– Ц0 - призводить до неправильної роботи суб'єкта в цілому або значної його частини і наслідки зміни незворотні;

– Ц1 - несанкціоновані зміни призведуть до неправильної роботи суб'єктів через деякий час, якщо не буде вжито заходів. Наслідки незворотні;

– Ц2 – несанкціоновані зміни призведуть до неправильної роботи суб'єктів через деякий час, якщо не буде вжито заходів. Наслідки оборотні;

– Ц3 – несанкціоновані зміни не приведуть до збою в роботі суб'єкта, наслідки оборотні;

– Ц4 - несанкціоновані зміни не відражатимуться на роботі системи.

Доступність:

– Д0 – у разі порушення доступності інформації даного типу підприємство не понесе матеріального збитку, робота підприємства не буде порушена, бажано впровадження, зміни в існуючих технологічних процесах;

– Д1 – у разі порушення доступності інформації даного типу підприємство понесе мінімальний збиток матеріального прибутку, робота підприємства не буде порушена, загальний дохід залишиться без зміни;

– Д2 – у разі порушення доступності інформації даного типу підприємство понесе середній збиток матеріального прибутку за поточний квартал, робота підприємства не буде порушена, можливі відставання від конкурентних підприємств;

– Д3 – у разі порушення доступності інформації даного типу підприємство понесе збиток матеріального прибутку, робота підприємства буде ускладнена, загальний дохід може знизиться до половини існуючого;

– Д4 – у разі порушення доступності інформації даного типу підприємство понесе максимально велику шкоду матеріального прибутку протягом декількох кварталів, необхідно прийняття радикальних рішень стосовно доступності інформації на підприємстві.

2.4.2 Визначення переліку загроз

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

Загрози в залежності від виду впливів на інформацію й НСД до неї можна розділити на випадкові й навмисні.

До випадкових загроз варто віднести:

– відмови й збої апаратури;

– перешкоди на лінії зв'язку від впливів зовнішнього середовища;

– помилки людини як ланки системи;

– системні й системотехнічні помилки розробників;

– структурні, алгоритмічні й програмні помилки;

– аварійні ситуації й інші впливи.

– відмова від функціонування ІТС в цілому, наприклад вихід з ладу електроживлення;

– стихійні лиха: пожежа, повінь, землетрус, урагани, удари блискавки й т.д.

Навмисні загрози пов'язані з діями людини, причинами яких можуть бути певне невдоволення своєю життєвою ситуацією, сугубо матеріальний інтерес або проста розвага із самоствердженням своїх здатностей, як у хакерів, й т.д.

Всі джерела загроз мають різну ступінь небезпеки (Коп) і, яку можна кількісно оцінити, провівши їх ранжування. При цьому, оцінка ступеня небезпеки проводиться за непрямими показниками.

В якості критеріїв порівняння (показників) можна, вибрати:

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

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

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

Кожен показник оцінюється експертно-аналітичним методом за п'ятибальною системою. Причому, 1 відповідає мінімальному обсязі впливу оцінюваного показника на небезпеку використання джерела, а 5 – максимальної.

(Коп) і для окремого джерела можна визначити як відношення твори вищенаведених показників до максимального значення.

$$(K_{оп})_i = \frac{(K_1 * K_2 * K_3)}{125}$$

Таблиця 2.5 Рівень загроз та вразливостей на підприємстві «Оберіг-сервіс»

№	Вид загрози	Вразливості, що призведуть до реалізації загроз	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка загрози
1. Навмисні загрози (антропогенні та техногенні)							
1.1	НСД до даних з порушенням встановлених правил розмежування доступу внаслідок використання порушником відомих вразливостей системного та прикладного ПЗ	-недосконале або нове ПЗ; -помилки при розмежуванні доступу до системи.	2	К,Ц,Д,С	3	внутрішнє, зовнішнє	2,5
1.2	Порушення конфіденційності або цілісності інформації, що зберігається в ІТС, внаслідок навмисних дій авторизованого користувача	-відсутність резервних копій; -неправильний підбор персоналу; -неефективне розмежування прав доступу в системі.	1	К,Ц,Д,С	3	внутрішнє	2
1.3	Впровадження і використання комп'ютерних вірусів, закладних програм для порушення безпеки даних	-відсутність або неефективність антивірусного ПЗ; -наявність незахищеного з`єднання.	2	К,Ц,Д,С	3	внутрішнє, зовнішнє	2,5

Продовження таблиці 2.5

№	Вид загрози	Вразливості, що призведуть до реалізації загроз	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка загрози
1.4	Одержання технологічної інформації (атрибутів доступу адміністраторів або інших користувачів системи) іншим користувачем ІТС атрибутами доступу для розширювання своїх повноважень або маскування під іншого зареєстрованого	-необізнаність персоналу; -відсутність/неефективність ідентифікації та автентифікації користувача.	3	К,Ц,Д,С	2	внутрішнє	2,5
1.5	Одержання та використання атрибутів доступу системи сторонніми особами внаслідок необережного поводження користувачів	-передавання паролів у відкритому вигляді; -необізнаність персоналу в питання інформаційної безпеки.	2	К,Ц,Д,С	5	зовнішнє	3,5
1.6	Читання залишкової інформації з оперативної та зовнішньої пам’яті ЕОМ	-не реалізованість заборони повторного використання інформації.	2	К	3	внутрішнє	2,5

Продовження таблиці 2.5

№	Вид загрози	Вразливості, що призведуть до реалізації загроз	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка загрози
2. Випадкові загрози							
2.1	Ненавмисні дії користувачів, що призводять до відмови функціонування мережі чи окремих її елементів, пошкодження обладнання (телекомунікаційного, програмних та інформаційних ресурсів)	-необізнаність персоналу в питаннях інформаційної безпеки; -доступність до елементів систем, в якій немає необхідності.	2	К,Ц,Д,С	4	внутрішнє	3
2.2	Порушення цілісності інформації, що зберігається, внаслідок ненавмисних дій користувачів	-відсутність резервного обладнання	3	Ц,Д,С	4	внутрішнє	3,5
2.3	Ненавмисне пошкодження носіїв інформації чи інформації, яка зберігається на цих носіях	-недосвідченість персоналу	2	Ц,Д	3	внутрішнє	2,5
2.4	Неправомірна зміна режимів роботи обладнання, програмних засобів тощо, ініціювання процесів, які здатні призвести до незворотних змін у системі	-недосвідченість персоналу	1	К,Ц,Д,С	4	внутрішнє	2,5

Продовження таблиці 2.5

№	Вид загрози	Вразливості, що призведуть до реалізації загроз	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка загрози
2.5	Випадкове зараження програмних засобів комп'ютерними вірусами	-необізнаність персоналу; -неякісне антивірусне ПЗ.	4	К,Ц,Д,С	4	внутрішнє	4
2.6	Невиконання організаційних заходів, посадових і технологічних інструкцій щодо порядку та правил експлуатації чи використання мережевих ресурсів	-недбалість персоналу; -недосвідченість персоналу в питаннях інформаційної безпеки.	2	К,Ц,Д,С	2	внутрішнє	2
2.7	Неправомірне впровадження і використання забороненого політикою безпеки ПЗ (системне та прикладне ПЗ, навчальні та ігрові програми та ін.)	-недбалість персоналу	2	К,Ц,Д,С	1	внутрішнє	1,5
2.8	Порушенні цілісності інформації, що зберігається внаслідок апаратного або програмного збою	-відсутність резервного обладнання; -відсутність плану безперервної роботи.	3	Ц,Д,С	4	внутрішнє	3,5

Продовження таблиці 2.5

№	Вид загрози	Вразливості, що призведуть до реалізації загроз	Ймовірність	Що порушує	Рівень загрози	Джерело	Загальна оцінка загрози
3. Стихійні (впливи природних факторів)							
3.1	Зміна умов фізичного середовища (стихійні лиха, такі як землетрус, повінь, пожежа і аварії або інші випадкові події)	-наявність легкозаймистих матеріалів; -несправність каналізаційної системи; -старе приміщення.	2	Ц,Д,С	3	зовнішнє	2,5
3.2	Впливи природних завад (грозові розряди, іскріння в електромережах, під час електрозварювання тощо)	-відсутність захисту від блискавки; -неякісна електропроводка; -відсутність резервних каналів електроживлення.	2	Ц,Д,С	3	зовнішнє	2,5

2.4.3 Визначення переліку порушників

Порушник - це особа, яка помилково, внаслідок необізнаності, цілеспрямовано, за злим умислом або без нього, використовуючи різні можливості, методи та засоби, здійснила спробу виконати операції, які призвели або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки.

Відносно ІТС порушники можуть бути: внутрішніми (з числа персоналу або користувачів системи), або зовнішніми (сторонніми особами).

Користувач інформації в системі - фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;

За рівнем повноважень щодо доступу до інформації, характером та складом робіт, які виконуються в процесі ІТС, особи, що мають доступ до неї, поділяються на наступні категорії:

– користувачі, яким надано повноваження розробляти й супроводжувати систему захисту інформації, а також повноваження забезпечувати управління ІТС - адміністратор мережі;

– користувачі, яким надано право доступу до конфіденційної інформації одного або декількох класифікаційних рівнів – директор, начальник відділу кадрів, працівники відділу кадрів, головний економіст, економісти, секретар;

– розробники ПЗ, які здійснюють розробку та впровадження нових функціональних процесів, а також супроводження вже діючих;

– постачальники обладнання і технічних засобів ІТС та фахівці, що здійснюють його монтаж, поточне гарантійне й післягарантійне обслуговування;

– технічний персонал, що здійснює повсякденне підтримання життєдіяльності фізичного середовища ІТС - інженер, електрики, технічний персонал з обслуговування будівель, ліній зв’язку.

Модель порушника – абстрактний формалізований або неформалізований опис порушника. Модель порушника відображає його практичні та потенційні

можливості, апріорні знання, час та місце дії тощо.

Таблиця 2.6 – Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Основні ознаки порушника
К0	Не знає функціональні особливості системи, основні закономірності формування масивів даних та потоків запитів до них, має навички щодо користування штатними засобами системи.
К1	Знає функціональні особливості системи, основні закономірності формування масивів даних та потоків запитів до них, має навички щодо користування штатними засобами системи.
К2	Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації автоматизованих інформаційних систем.
К4	Знає структуру, функції й механізми дії засобів захисту, їх недоліки.
К5	Знає недоліки та “вади” механізмів захисту, які вбудовані у системне програмне забезпечення та його не документовані можливості.
К6	Є розробником програмних та програмно-апаратних засобів захисту або системного програмного забезпечення.

Таблиця 2.7 – Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника
Ч1	До впровадження АС або її окремих компонентів.
Ч2	Під час бездіяльності компонентів системи (в неробочий час, під час планових перерв у роботі, перерв для обслуговування і ремонту і т.д.).
Ч3	Під час функціонування АС (або компонентів системи).
Ч4	Як у процесі функціонування АС, так і під час зупинки компонентів системи.

Таблиця 2.8 – Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника
Д1	Без доступу на контрольовану територію організації.
Д2	З контрольованої території без доступу у будинки та споруди.
Д3	Усередині приміщень, але без доступу до технічних засобів АС.
Д4	З робочих місць користувачів АС.
Д5	З доступом у зони даних (баз даних, архівів й т.ін.).
Д6	З доступом у зону керування засобами забезпечення безпеки АС.

Таблиця 2.9 – Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення
М1	Безвідповідальність
М2	Самозатвердження
М3	Корисливий інтерес

Таблиця 2.10 – Модель порушника

Посада	Можливий мотив	Категорія обізнаності порушника	Можливе місце дії	Можливий час дії
Внутрішні				
Директор	М2,М3	К1	Д6	Ч4
Диспетчер	М2,М3	К2	Д5	Ч4
Бухгалтер	М1,М2, М3	К1	Д4	Ч3
Системний адміністратор	М2, М3	К5	Д6	Ч4
Прибиральниця	М2, М3	К0	Д3	Ч2
Зовнішні				

Продовження таблиці 2.10

Посада	Можливий мотив	Категорія обізнаності порушника	Можливе місце дії	Можливий час дії
Представники організацій, що взаємодіють з питань технічного забезпечення	М3	К5	Д2	Ч1
Представники організацій, що взаємодіють з питань ПЗ	М3	К4	Д3	Ч1
Злочинці (хакери)	М2, М3	К3	Д1	Ч3

2.4.4 Визначення каналів несанкціонованого доступу до ІТС

Несанкціонований доступ до інформації – доступ до інформації, за якого порушуються встановлений порядок його здійснення та (чи) правові норми.

Доступ порушенням посадових повноважень співробітника, доступ до закритої для публічного доступу інформації з боку осіб, котрі не мають дозволу на доступ до цієї інформації. Також іноді несанкціонованим доступом називають одержання доступу до інформації особою, що має право на доступ до цієї інформації в обсязі, що перевищує необхідний для виконання службових обов'язків.

Витік інформації – неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання (ДСТУ 3396.2-97 [4]).

Основними каналами витоку інформації в ІТС на ОІД є :

- змінні носії, та носії на які здійснюється архівування;
- робочі станції працівників відділів;
- робоча станція адміністратора системи;
- засоби вводу\виводу інформації;
- канали передачі інформації в ІТС;
- комутатор.

2.4.5 Вибір заходів захисту інформації в ІТС підприємства

Забезпечення безпеки інформації в ІТС досягається шляхом застосування комплексу заходів щодо захисту інформації: організаційних, організаційно-технічних, застосування програмних, апаратних та програмно-апаратних засобів захисту, застосування технічних засобів захисту.

Згідно НД ТЗІ 1.1-003-99 матриця доступу — n-мірна таблиця, вздовж кожного виміру якої відкладені ідентифікатори об’єктів КС одного типу (об’єктів-користувачів, об’єктів-процесів чи пасивних об’єктів), і містить визначені права доступу суб’єктів до кожного із типів об’єктів.

Згідно з Законом України „Про захист інформації в інформаційно-телекомунікаційних системах”.

Доступ до інформації в системі - отримання користувачем можливості обробляти інформацію в системі;

Основними видами інформаційної діяльності є створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації.

Таблиця 2.11 – Матриця керування доступом

	О1	О2	О3	О4	О5	О6	О7	О8	О9
1	Ч,З,Д,ЗМ,ЗН,К	Ч,З, Д	Ч,З,Д,ЗМ,ЗН,К	Ч,З,Д,ЗН,ЗМ	Ч,З,Д,К,ЗН,ЗМ	Ч,З,Д,К,ЗМ,ЗН	Ч,З,Д,К,ЗН,ЗМ	Ч,З,Д,К,ЗН,ЗМ	Ч,З,Д,К,ЗН,ЗМ
2	-	Ч,З,Д	Ч,З,Д,	-	Ч,К	-	Ч,З,Д,К,ЗН	Ч,З,Д,К,ЗН,ЗМ	Ч,З,К,Д,ЗМ,ЗМ
3	-	-	Ч,З,Д,	Ч,З,Д,ЗН,ЗМ	Ч,З,Д,К	-	Ч,З,Д,К,ЗН,ЗМ	-	-
4	-	-	-	-	Ч,З	-	Ч,З,К,Д	Ч,З,Д,К	Ч,З,Д,К
	О10	О11	О12	О13	О14	О15	О16	О17	О18
1	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,З,ЗМ,ЗН	Ч,З,К,Д	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН
2	Ч,З,К,Д,З	Ч,З,К,Д	-	-	-	-	-	Ч,З,К,Д,ЗМ,ЗН	-
3	-	-	Ч,З,К,Д	-	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ
4	-	Ч,З,К,Д	-	Ч,З,К,Д,ЗМ,ЗН	-	-	-	-	-

Продовження таблиці 2.11

	О19	О20	О21	О22	О23	О24	О25	О26	О27
1	Ч,З,К,Д,ЗМ,ЗН	Ч,З,Д,К,	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ
2	Ч,З,К,Д	Ч,З,Д,К	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ
3	Ч,З,К,Д	Ч,З,К,Д	Ч,З,К,Д	-	-	-	-	-	-
4	Ч,З,К,Д	Ч,З,К,Д	Ч,З,К,Д	-	-	-	Ч,З,К,Д,ЗМ	Ч,З,К,Д	Ч,З,К,Д
	О28	О29	О30						
1	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН						
2	Ч,З,К,Д,ЗМ	Ч,З,К,Д	Ч,З,К,Д						
3	-	-	-						

Продовження таблиці 2.11

	О28	О29	О30						
4	Ч,З,К,Д	Ч,З,К,Д	Ч,З,К,Д						

Позначення:

— **Суб’єкти доступу:**

S1 – директор;

S2 – системний адміністратор;

S3 – бухгалтер;

S4 – диспетчер;

— **Об’єкти доступу:**

O1 – організаційно-розпорядча документація;

O2 – облік внутрішніх документів (накази, службові записки, інструкції);

O3 – інформація про надання послуг, тарифи, контактна інформація підприємства;

O4 – Інформація про робітників;

O5 – Статутні документи підприємства (документи, що дозволяють займатися підприємницькою діяльністю);

O6 – Облік та реєстрація вхідних та вихідних документів організації;

O7 – Трудові договори робітників;

O8 – Договори про надання послуг клієнтам;

O9 – База даних клієнтів;

O10 – Заявки на підключення обладнання;

O11 – Акти прийому виконаних спеціалістом з монтажу робіт;

O12 – Дані про лицьові рахунки замовників;

O13 – Заявки на розірвання договору про надання послуг;

O14 – Відомості про фінанси підприємства;

O15 – Плани закупівель;

O16 – Відомості постачальників;

O17 – Зміст та характер договорів, контрактів однією із сторін яких виступає підприємство;

O18 – База вхідних цін;

O19 – Коди програмного обладнання;

O20 – Інформація по ліцензійне ПО;

О21 – Повна характеристика комп’ютерної техніки (серійний номер, заводський номер і т.д.);

О22 – Звіт про виконання ремонтних послуг офісної техніки;

О23 – База даних клієнтів;

О24 – Відомості про дату заключення договору між клієнтом та підприємством;

О25 – Відомості про створення сертифіката клієнта;

О26 – Відомості про генерацію ключів ЕЦП, формування сертифікатів відкритих ключів ключей ЕЦП;

О27 – Відомості про надання послуг приватним підприємствам;

О28 – Відомості про надання послуг державним підприємствам;

О29 – Формування та ведення реєстра форм звітних документів;

О30 – Формування та відправка пакетів звітності в електронному вигляді по електронній пошті з використання криптографічного захисту.

— **Операції з файлами:**

Ч – читання;

З – зберігання;

Д – друкування;

К – копіювання;

Зн – знищення;

Зм – змінення.

2.4.6 Критерії впровадження системи

В результаті проведеного аналізу загроз та вразливостей підприємства, був обраний профіль захищеності (опис послуг безпеки приведений у таблиці 2.12, критерії захищеності в таблиці 2.13): 3.КЦД.1 = { КД-2, КО-1, КВ-1,ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1,НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

Таблиця 2.12 – Профіль захищеності ІТС

Критерії	**Послуги безпеки**	**Вимоги до рівнів послуг безпеки**
	1	**2**
Конфіденційності	Довірча конфіденційність	КД-2 (базова довірча конфіденційність)
	Повторне використання об'єктів	КО-1 (повторне використання об'єктів)
	Конфіденційність при обміні	КВ-1(мінімальна конфіденційність при обміні)
Цілісності	Довірча цілісність	ЦД-1 (мінімальна довірча цілісність)
	Відкат	ЦО-1 (обмежений відкат)
	Цілісність при обміні	ЦВ-1 (мінімальна цілісність при обміні)
Доступності	Використання ресурсів	ДР-1 (квоти)
	Відновлення після збоїв	ДВ-1 (ручне відновлення)
Спостережності	Реєстрація	НР-2 (захищений журнал)
	Ідентифікація і автентифікація	НИ-2 (одиночна ідентифікація і автентифікація)
	Цілісність комплексу засобів захисту	НЦ-2 (КЗЗ з гарантованою цілісністю)
	Самотестування	НТ-2 (самотестування при старті)
	Ідентифікація і автентифікація при обміні	НВ-1(автентифікація вузла)

Таблиця 2.13 – Критерії захищеності

Критерії захищеності	**Чим реалізуються до впровадження політики безпеки**	**Чим реалізуються після впровадження політики безпеки**
КД-2	Розмежування прав доступу за допомогою Active Directory	Розмежування прав доступу за допомогою Active Directory
КО-1	Вбудовані засоби Windows	Вбудовані засоби Windows
КВ-1	Використання протоколу SSL	Використання протоколу SSL
ЦД-1	Розмежування прав доступу за допомогою Active Directory	Розмежування прав доступу за допомогою Active Directory
ЦО-1	Вбудовані засоби Windows	Вбудовані засоби Windows
ЦВ-1	-	Використання засобів криптозахисту
ДР-1	Вбудовані засоби Windows	Вбудовані засоби Windows
НР-2	Вбудований журнал реєстрації Windows	Вбудований журнал реєстрації Windows
НИ-2	Вбудовані засоби Windows	Вбудовані засоби Windows
НК-1	-	Мережевий протокол автентифікації
НО-2	-	Призначення адміністратора безпеки
НЦ-2	Вбудовані засоби Windows	Вбудовані засоби Windows
НТ-2	Вбудовані засоби Windows	Вбудовані засоби Windows
НВ-1	-	Мережевий протокол автентифікації

Базова довірча конфіденційність (КД-2)

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 наоб’єкти і забезпечує взаємодію зазначених об’єктів:

– 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;

– всі інші об’єкти, які підлягають захисту, але не належать до зазначених вище видів.

Політика довірчої конфіденційності, що реалізується КЗЗ, стосується об’єктів, які створюються користувачем у процесі виконання ним функціональних обов’язків.

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.

Повторне використання об’єктів (КО-1)

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 ЛОМ, які містять конфіденційну інформацію і ресурси яких поділяються між користувачами ЛОМ та прикладними процесами, що виконуються в ЛОМ.

Вимоги цієї послуги поширюються на сегменти оперативної пам'яті робочих станцій та серверів (усіх без виключення типів) та носії інформації на жорстких магнітних дисках (ЖМД), якими укомплектовані робочі станції й сервери, і використовуються системними та функціональними процесами під час оброблення конфіденційної інформації, а також на окремі види периферійних пристроїв, які мають власну пам’ять і задіяні під час експорту

(імпорту) конфіденційної інформації з (в) ЛОМ 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.

Мінімальна конфіденційність при обміні (КВ-1):

– політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься;

– політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності;

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

Мінімальна довірча цілісність (ЦД-1)

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

Політика довірчої цілісності, що реалізується КЗЗ, поширюється на слабо- та сильнозв’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.

Обмежений відкат (ЦО-1)

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 забезпечує взаємодію нижчезазначених об’єктів і поширюється на:

– користувачів усіх категорій;

– сильно та слабозв’язані об’єкти, які містять конфіденційну інформацію і в процесі обробки яких передбачається можливість їхньої модифікації користувачем, а також технологічну інформацію КСЗІ.

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 .

Мінімальна цілісність при обміні (ЦВ-1)

Дана послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Найчастіше ця послуга реалізується з використанням таких механізмів криптографічного захисту, як цифровий підпис і коди автентифікації повідомлень. Рівні даної послуги ранжируються на підставі

повноти захисту і вибірковості керування. Під повнотою захисту, як і для послуги конфіденційність при обміні, треба розуміти множину типів загроз, від яких забезпечується захист. Під ступенем захищеності об'єктів, що експортуються, як правило, слід розуміти крипостійкість використовуваних алгоритмів шифрування.

Використання ресурсів (ДР-1)

Послуга дозволяє керувати використанням користувачами послуг та ресурсів.

Політика використання ресурсів, що реалізується КЗЗ, поширюється на нижчезазначені об’єкти і забезпечує взаємодію цих 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.

Ручне відновлення після збоїв (ДВ-1)

Політика відновлення після збоїв, що реалізується КЗЗ, поширюється на нижчезазначені об’єкти та забезпечує їх взаємодію:

– системне та функціональне ПЗ;

– засоби захисту інформації та засоби управління КСЗІ;

– засоби адміністрування та управління обчислювальною системою;

– окремі периферійні пристрої (принтери, накопичувачі інформації, змінні носії інформації і т.і.), які задіяні для обробки конфіденційної інформації.

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 ЛОМ 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 автоматизованої системи.

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

Захищений журнал (НР-2)

Послуга реєстрації рівня НР-2 дозволяє контролювати небезпечні для АС дії зі сторони користувачів будь-яких категорій відносно процесів і об'єктів.

Політика реєстрації поширюється та забезпечує взаємодію користувачів усіх категорій.

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 конфіденційної інформації;

– виведення користувачем будь-якої категорії документа або інформації конфіденційного характеру на призначений для цього пристрій друку, або намагання виведення користувачем будь-якої категорії документа або інформації конфіденційного характеру на пристрій друку;

– копіювання наборів даних із інформацією конфіденційного характеру на запам’ятовуючих пристроях, які працюють зі змінними носіями, що здатні записувати інформацію, і виділені спеціально для виконання процесів копіювання, або намагання копіювання інформації конфіденційного характеру 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 НСД, модифікації або руйнування.

Одиночна ідентифікація та автентифікація (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 нижчезазначені об’єкти і забезпечує їх взаємодію .

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 НСД, модифікації або руйнування.

Однонаправлений достовірний канал (НК-1)

Послуга повинна гарантувати користувачу будь-якої категорії можливість безпосередньої взаємодії з КЗЗ, а також те, що ніяка взаємодія користувача з ЛОМ 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 ПЗ, 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.

Розподіл обов’язків адміністраторів (НО-2)

Послуга дозволяє розмежувати повноваження користувачів, визначивши категорії користувачів із певними й притаманними для кожної з категорій функціями. 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 конфіденційної інформації.

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

Адміністратор безпеки повинен мати доступ до технологічної інформації КСЗІ та системного й функціонального ПЗ, яке реалізує механізми захисту. Інший адміністратор повинен мати доступ до технологічної інформації щодо управління автоматизованої системи та системного й функціонального ПЗ, 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 конфіденційну інформацію, за виключенням випадків, коли їхніми функціональними обов’язками передбачено суміщення адміністративних повноважень та повноважень щодо обробки конфіденційної інформації.

КЗЗ з гарантованою цілісністю (НЦ-2)

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

Для рівня НЦ-2 необхідно, щоб КЗЗ підтримував власний домен виконання, відмінний від доменів виконання всіх інших процесів, захищаючи себе від зовнішніх впливів. Дана вимога є однією з вимог до реалізації диспетчера доступу. Як правило, реалізація даної вимоги повинна забезпечуватися можливостями апаратного забезпечення ОС.

Самотестування при старті (НТ-2***)***

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

Політика самотестування поширюється на нижчезазначені об’єкти і забезпечує їх взаємодію:

– адміністратора безпеки;

– компоненти системного та функціонального ПЗ, які задіяні для реалізації механізмів КЗЗ;

– засоби захисту інформації, а також технологічну інформацію КСЗІ.

До складу КЗЗ повинен входити набір тестових процедур, достатній для оцінки правильності виконання в ЛОМ всіх критичних для безпеки конфіденційної 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.

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

Автентифікація вузла (НВ-1)

Дана послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Найчастіше ця послуга реалізується з використанням таких механізмів криптографічного захисту, таких як цифровий підпис і коди автентифікації повідомлень. На включення даного рівня в свій рейтинг може претендувати система, що дозволить на підставі цифрового підпису перевіряти цілісність функціонуючого на ЕОМ ПЗ, або система електронної пошти, що забезпечує цифровий підпис повідомлень.

2.5 Розробка політики безпеки для підприємства

При розробці політики безпеки для підприємства, спираючись на наявність конфіденційної інформації, яка обробляється в ІТС, фінансових та матеріальних ресурсів, які є у розпорядженні власника ІТС, обрано принцип, при якому впровадження інформаційного захисту буде доцільним - досягнення необхідного рівня захищеності інформації за мінімальних затрат і допустимого рівня обмежень на технологію її обробки в ІТС.

Заходи, що представлені в політиці інформаційної безпеки, направлені на зниження ризиків реалізації загрози через вразливості ІТС, спираючись на існуючий аналіз ризиків.

2.5.1 Політика безпеки для системного адміністратора

1 Опис:

Політика включає в себе інструкції для системного адміністратора, його обов’язки та права.

2 Метою цієї політики захист підприємства від витоку та несанкціонованого доступу до інформації.

3 Галузь застосування:

Ця політика відноситься до системного адміністратора, хто є користувачами системи.

4 Інструкція політики

І. Загальні положення:

1. Системний адміністратор відноситься до категорії фахівців.

2. На посаду системного адміністратора призначається особа, яка має профільне професійну освіту, досвід технічного обслуговування і ремонту персональних комп'ютерів і оргтехніки, знає основи локальних мереж (стек протоколів TCP / IP, мережеве обладнання, принципи побудови локальних обчислювальних мереж).

3. Системний адміністратор повинен знати:

3.1 Технічні характеристики, призначення, режими роботи, конструктивні особливості, правила технічної експлуатації устаткування локальних обчислювальних мереж, оргтехніки, серверів і персональних комп'ютерів.

3.2 Апаратне та програмне забезпечення локальних обчислювальних мереж.

3.3 Принципи ремонту персональних комп'ютерів і оргтехніки.

3.4 Мови і методи програмування.

3.5 Основи інформаційної безпеки, способи захисту інформації від несанкціонованого доступу, пошкодження або навмисного спотворення.

3.6 Порядок оформлення технічної документації.

3.7 Правила внутрішнього трудового розпорядку.

3.8 Основи трудового законодавства.

3.9 Правила і норми охорони праці, техніки безпеки і протипожежного захисту.

1 Призначення на посаду системного адміністратора і звільнення з посади провадиться наказом директора .

2 Системний адміністратор підпорядковується безпосередньо директору підприємства «Оберіг-сервіс».

II. Посадові обов'язки системного адміністратора:

Системний адміністратор:

1 Встановлює на сервери і робочі станції операційні системи і необхідне для роботи програмне забезпечення.

2 Розроблює конфігурацію програмного забезпечення на серверах і робочих станціях.

3 Підтримує в працездатному стані програмне забезпечення серверів і робочих станцій.

4 Реєструє користувачів локальної мережі і поштового сервера, призначає ідентифікатори і паролі.

5 Розробляє технічну і програмну підтримку користувачів, консультує користувачів з питань роботи локальної мережі та програм, складає інструкції по роботі з програмним забезпеченням і доводить їх до відома користувачів.

6 Встановлює права доступу і контролює використання мережевих ресурсів.

7 Забезпечує своєчасне копіювання, архівування та резервування даних.

8 Приймає заходи по відновленню працездатності локальної мережі при збої або виході з ладу мережевого обладнання.

9 Виявляє помилки користувачів і програмного забезпечення та вживає заходів щодо їх виправлення.

10 Проводить моніторинг мережі, розробляє пропозиції щодо розвитку інфраструктури мережі.

11 Забеспечує мережеву безпеку (захист від несанкціонованого доступу до інформації, перегляду або зміни системних файлів і даних), безпека міжмережевої взаємодії.

12 Розроблює антивірусний захист локальної обчислювальної мережі, серверів і робочих станцій.

13 Підготавлює пропозиції з модернізації та придбання мережевого обладнання.

14 Контролює за монтаж обладнання локальної мережі фахівцями сторонніх організацій.

15 Повідомляє своєму безпосередньому керівнику про випадки порушення правил користування локальної обчислювальної мережею і вжиті заходи.

16 Повинен відвідувати курси підвищення кваліфікації не менш ніж 2 рази на 6 місяців.

III. Права системного адміністратора:

Системний адміністратор має право:

1 Встановлювати і змінювати правила користування локальною обчислювальною мережею.

2 Знайомитися з документами, що визначають його права та обов'язки за займаною посадою, критерії оцінки якості виконання посадових обов'язків.

3 Вносити на розгляд керівництва пропозиції щодо вдосконалення роботи, пов'язаної з передбаченими цією посадовою інструкцією обов'язками.

4 Вимагати від керівництва забезпечення організаційно - технічних умов, необхідних для виконання посадових обов'язків.

IV. Відповідальність системного адміністратора:

1 Системний адміністратор несе відповідальність за:

1.1 Порушення функціонування локальної обчислювальної мережі, серверів і персональних комп'ютерів внаслідок неналежного виконання своїх посадових обов'язків.

1.2 Несвоєчасну реєстрацію користувачів локальної обчислювальної мережі і поштового сервера.

1.3 Несвоєчасне повідомлення керівництва про випадки порушення правил користування локальної обчислювальної мережею.

2 Системний адміністратор несе відповідальність:

2.1 За неналежне виконання або невиконання своїх посадових обов'язків.

2.2 За правопорушення, скоєні в процесі своєї діяльності.

2.3 За завдання матеріальної шкоди компанії.

2.5.2 Політика антивірусного захисту

1 Опис

Політика включає в себе інструкції для користувачів із застосування антивірусного ПЗ.

2 Метою цієї політики захист системи від комп’ютерних вірусів.

3 Галузь застосування

Ця політика відноситься до всіх робітників підприємства, хто є користувачами системи.

4 Інструкція політики

1.1 Для директора:

а) забезпечення вчасного отримання ПЗ для антивірусного захисту;

б) контроль за виконанням перевірки робочих станцій перед початком роботи

1.2 Для системного адміністратора:

а) вчасне встановлення антивірусного ПЗ та оновлення

б)контроль за терміном дії ліцензії

в) контроль за виконанням перевірки робочих станцій перед початком роботи (за відсутності директора)

1.3 Для диспетчера та бухгалтера:

а) перевірка робочих станцій перед початком роботи

б) вчасно сповіщувати про некоректність роботи антивірусного ПЗ

в) завжди скануйте носії інформації та підозрілі файли або файли з невідомого джерела на наявність вірусів;

г) зберігайте резервні копії важливих даних в безпечному місці;

е) ніколи не завантажувати файли з невідомих чи підозрілих джерел; не відкривайте невідомі вам файли, що прикріплені до електронної пошти від невідомого, підозрілого або ненадійного джерела. Видаляйте ці вкладення відразу, «подвійним видаленням», шляхом спорожнення кошика.

2.5.3 Політика чистого столу

1 Опис

Дана політика визначає, в якому вигляді співробітники приватного підприємства повинні залишати свої робочі місця, коли вони залишають їх без нагляду або не використовують їх.

2 Метою даної політики є запобігання витоку або втрати інформації з обмеженим доступом

3 Галузь застосування

Вимоги даної політики поширюються на всіх співробітників підприємства.

4 Інструкція політики

– Співробітники зобов’язані забезпечувати збереження всієї інформації з обмеженим доступом у друкованому або електронному вигляді на своєму робочому місці, коли вони збираються покинути приміщення на короткий або тривалий проміжок часу.

– Персональні комп’ютери повинні бути заблоковані, якщо передбачається, що вони не будуть використовуватись деякий час.

– Персональні комп’ютери повинні бути повністю вимкнені в кінці робочого дня.

– Будь-яка інформація з обмеженим доступом повинна бути видалена з робочого місця і замкнена в ящику чи сейфі, коли стіл не зайнятий і в кінці робочого дня.

– Ключі, що використовуються для доступу до інформації з обмеженим доступом, не можна залишати без нагляду на столі.

– Паролі не можуть бути розміщені на комп’ютері, під ним або записані в нотатках.

– Інформація з обмеженим доступом, що була роздрукована, повинна бути негайно видалена з принтера.

– Інформація, що підлягає знищенню, повинна бути утилізована за допомогою шредера якнайшвидше.

5. Відповідальність

– Кожен співробітник повинен дотримуватись вимог даної політики.

– Відповідальність за виконання співробітниками вимог даної політики несе директор.

– Співробітники, що порушили дану політику, несуть відповідальність відповідно до внутрішніх нормативних документів підприємства.

Висновки до розділу 2

Інформація, наведена у пояснювальній записці, була частково змінена на вимогу власника з метою недопущення публікації матеріалів, що становлять службову таємницю.

У другому розділі виконано обстеження об'єкта інформаційної діяльності, яким є інформаційно-телекомунікаційна система підприємства «Оберіг-сервіс».

В результаті проведеного обстеження ОІД було:

- класифіковано інформацію, що зберігається і циркулює на підприємстві та потребує захисту;

- побудовано модель загроз та порушника, що діють на дану ІТС.

На основі аналізу моделі загроз було обрано найбільш актуальні загрози та для запобігання їх реалізації розроблені наступні політики безпеки:

- політика безпеки для системного адміністратора;
- політика антивірусного захисту;
- політика чистого столу.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Необхідність обґрунтування витрат на реалізацію політики безпеки

Метою розрахунків є економічне обґрунтування доцільності впровадження політики безпеки інформації. Для цього визначено економічну ефективність використання основних результатів, що отримані в ході виконання роботи.

Економічна доцільність визначається розрахунками:

– капітальних витрат, що потребує розроблена політика безпеки;

– експлуатаційних витрат;

– річного економічного ефекту від впровадження інформаційної політики безпеки.

Запропонована інформаційна політика безпеки передбачає необхідність витрат на її реалізацію. До заходів, що потребують витрат відносяться:

1 оновлення ліцензій антивірусного програмного забезпечення;

2 навчання персоналу в питаннях інформаційної безпеки;

3.2 Визначення трудомісткості розробки політики безпеки інформації

Трудомісткість розробки політики безпеки інформаціїї визначається за формулою 3.1:

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}, \text{ год} \quad (3.1)$$

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

$t_{в}$ – тривалість розробки концепції безпеки інформації у організації;

$t_{а}$ – тривалість процесу аналізу ризиків;

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

$t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$t_{д}$ – тривалість документального оформлення політики безпеки.

t = 5 год + 1 год +4 год + 1 год + 2 год + 2 год + 2 год = 17 год (3.1)

Розрахунок витрат на створення політики безпеки виконується за формулою 3.2:

$$К_{рп} = З_{зп} + З_{мч}\text{ , грн.} \quad (3.2)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

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

де t – загальна тривалість розробки політики безпеки, годин;

$Зіб$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

$З_{зп}$=17*798=13566 грн

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{Мч} = t \cdot С_{Мч},\text{ грн,} \quad (3.4)$$

де t – трудомісткість розробки політики безпеки інформації на ПК, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P \cdot t_{нал} \cdot Се + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}, \text{ грн} \qquad (3.5)$$

$$С_{мч}= 0,4*1,40+ (11000*0,5)/1920 + (1094*0,5)/1920=3,7 \text{ грн}$$

$$З_{мч} = t \cdot С_{мч} = 4*3,7=14,8 \text{ грн},$$

$$К_{рп}=З_{зп}+З_{мч}=13566+14,8=13580,8 \text{ грн}.$$

3.3 Розрахунок (фіксованих) капітальних витрат

Оновлення ліцензії антивірусного ПЗ ESET NOD32 Antivirus:

Необхідне оновлення для 4 комп'ютерів, вартість однієї ліцензії – 209 грн. Загальна вартість закупівель ліцензійного ПЗ:

Кзпз = 4*209 грн = 836 грн.

Вартість роботи системного адміністратора розраховується з урахуванням заробітної платні робітника в час та тривалістю його роботи:

Кса = 56 грн/ч*2 = 112 грн.

$К_{навч}$ (витрати на навчання системного адміністратора) становлять 1300 грн.

$К_{аз}$ вартість закупівлі апаратного забезпечення та допоміжних матеріалів, відсутня оскільки за розробленими політиками безпеки закупівля апаратного забезпечення не є необхідною.

$К_н$ витрати на встановлення обладнання та налагодження системи інформаційної безпеки, відсутні оскільки не закуповується апаратне забезпечення.

Таким чином, капітальні (фіксовані) витрати на впровадження системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{рп} + К_{аз} + К_{навч} + К_{н}\ , \qquad (3.6)$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

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

$К_{рп}$ – вартість розробки політики безпеки інформації, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

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

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

$$К = 13580{,}8 + 836 + 112 + 1300 = 15828{,}8 \text{ грн}$$

3.4 Розрахунок поточних (експлуатаційних) витрат

1 навчання персоналу в питаннях інформаційної безпеки;

2 витрати на керування системою інформаційної безпеки.

1 Витрати на навчання персоналу в питаннях інформаційної безпеки включають в себе послуги сторонніх організацій, що створюють політику безпеки інформації та відповідно до неї розробляють інструкції для персоналу, що є користувачами системи. Вартість навчання адміністративного персоналу й кінцевих користувачів розглянутої системи:

Со = 12000 грн – витрати навчання персоналу

2 Обов’язки з керування системою інформаційної безпеки виконує директор та системний адміністратор (за відсутності директора), тому річний

фонд заробітної плати складає додаткову заробітну плату директора та системного адміністратора за рік:

$$Сз = Зд+Зса, грн \quad (3.7)$$

$$С_З=1600+1240=2940грн. (за 1 місяць)$$

$$Сз= 2940*12=35280 грн (за 1 рік)$$

де Зд –заробітна плата директора, грн на місяць. Зса – заробітна плата системного адміністратора, грн. на місяць.

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року (Се), визначається за формулою 3.8:

$$Се = Р \cdot Fр \cdot Це,грн \quad (3.8)$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт ;

Fр = 12 міс * 20 робочих діб/міс * 8 робочих годин * 4 комп’ютера = 7680 год – річний фонд робочого часу системи інформаційної безпеки;

Це = 1,40 грн за 1 кВт/год – тариф на електроенергію на 01.04.2019 року.

$$Се = 7680*1,40*0,4 = 15052,8 грн.$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки (Стос) визначаються у відсотках від вартості капітальних витрат (2%).

$$Стос = К * 0,02 = 948*0,02 = 18,96 грн.$$

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

$$C = Co + Cпрд + Cз + Ce + Cтос, грн \quad (3.9)$$

$$C=12000+ 2940 + 15052,8 + 18,95 = 30011,24 грн$$

Розрахунок оцінки величини збитку:

Втрати від зниження продуктивності співробітників атакованої системи мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки ($П_п$).

Таблиця 3.1 – Зарплати робітників за місяць

Посада	Розмір заробітної платі, грн	Кількість співробітників	Витрати на заробітну плату на місяць, грн
директор	9200	1	9200
Системний адміністратор	8960	1	8960
бухгалтер	5100	1	5100
диспетчер	4600	4	18400
		Загалом	41600

Місячний фонд робочого часу складає 640 годин. Річний – 7680 годин. Час простою внаслідок атаки 4 години:

$$П_п = (41600/640)*4 = 260,37 грн$$

Витрати на відновлення працездатності системи включають кілька складових:

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

$П_{пв}$ – витрати на відновлення системи, грн;

$П_{зч}$ – вартість заміни частин системи, грн.

Витрати на повторне введення інформації розраховуються виходячи з розміру заробітної плати співробітників системи $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$ = 8 год:

$$П_{ви} = (41600/640)*8 = 520,75 \text{ грн}$$

Витрати на відновлення системи визначаються часом відновлення після атаки tв = 4 год і розміром середньогодинної заробітної плати адміністратора:

$$П_{пв} = (8960/640)*4 = 56 \text{ грн}$$

Витрати на відновлення працездатності системи розраховують за формулою 3.10:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \text{ грн} \qquad (3.10)$$

$$П_в=520,75 + 56 + 3400 = 3976,75 \text{ грн}$$

Пзч = 3400 грн;

О = 2100000 грн обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік;

Втрати від зниження працездатності атакованої системи:

$$V = О/1920 * (4+8+4) = 2100000/1920 * 16 = 17500 \text{ грн}$$

Таким чином, загальний збиток від атаки на ІТС підприємства при реалізації загрози складе:

$$U=Пп+Пв+V \quad (3.11)$$

$$U=260,37+3976,75+17500=21737,12 \text{ грн}$$

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

$$B=\sum_i\sum_n U \quad (3.12)$$

$$B=21737,12*12*1=260845,44 \text{ грн}$$

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням B – загального збитку від атаки;R – очікуваної ймовірності атаки на систему;C – щорічних витрат на експлуатацію системи інформаційної безпеки.

Якщо реалізація загроз найймовірніша 1 раз на 3 місяці, тобто 4 рази на рік, то R=0,25. Загальний ефект від впровадження політики безпеки розраховують за формулою 3.13:

$$E = B \cdot R – C \quad (3.13)$$

$$E= 260845,44 * 0,25 – 30011,24 = 35200,12 \text{ грн.}$$

Визначення та аналіз показників економічної ефективності системи інформаційної безпеки:

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

а) коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);

б) термін окупності капітальних інвестицій To.

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

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

Коефіцієнт ROSI розраховують за допомогою показників:

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

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

$$ROSI = 35200,12/30011,24 = 1,17$$

Термін окупності капітальних інвестицій показує, за скільки років інвестиції окупляться за рахунок загального ефекту від впровадження КСЗІ.

$$T_o = 1 / 8,37 = 0,9 \text{ року}=10 \text{ місяців}$$

3.5 Висновки до розділу 3

В розділі проаналізована доцільності впровадження політики безпеки інформації. Визначено економічну ефективність використання основних результатів, що отримані в ході виконання роботи. Капітальні витрати на впровадження інформаційної політики безпеки становлять 15828,8 грн. Експлуатаційні витрати на впровадження інформаційної політики безпеки становлять 30011,24 грн. Загальний збиток від атаки на вузол складає 260845,44 грн.Ефект від впровадження системи інформаційної безпеки становить 35200,12 грн.Термін окупності капітальних інвестицій складає 10 місяців.

Отже, економічна доцільність обґрунтована і впровадження інформаційної політики безпеки може бути ефективною та успішною.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було проаналізовано актуальні загрози інформаційній безпеці України, розглянуто мету та принципи створення політики безпеки та проаналізовано актуальну ситуацію в Україні щодо інформаційної безпеки. Також було проаналізовано нормативно-правову базу у сфері захисту інформації.

У другому розділі було проаналізовано умови функціонування інформаційно-телекомунікаційної системи приватного підприємства «Оберіг-сервіс», були складені моделі загроз та порушника, за результатами аналізу яких, було виявлено, що найбільші загрози виникають внаслідок неправильної експлуатації антивірусних програм, невиконання усіх службових обов'язким системним адміністратором та порушення режиму знищення виробничих відходів. Тому, було розроблено наступні політики безпеки інформації інформаційно-телекомунікаційної системи даного відділення:

- політика чистого столу;
- політика безпеки для системного адміністратора;
- політика антивірусного захисту.

Всі ці рішення направлені на зниження ймовірності реалізації загроз зараження ПК шкідливим ПЗ, викрадення та використання у власних цілях документації, що була залишена без нагляду та підлягала знищенню, відмови в доступі санкціонованому користувачу АС.

Запропоновані рекомендації є економічно ефективними, що було підтверджено в економічному розділі даної кваліфікаційної роботи, де було визначено, що капітальні витрати на реалізацію рекомендацій окупляться менш ніж за півтора роки. Тому, в даному випадку, ці рекомендації використовувати доцільно.

ПЕРЕЛІК ПОСИЛАНЬ

1. ДСТУ 3396.1-96 - Технічний захист інформації. Порядок проведення робіт; [Електронний ресурс] – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38911&cat_id=38836;

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»; [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80;

3. Закон України «Про захист персональних даних»; [Електронний ресурс] –Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17;

4. Закон України "Про інформацію" [Електронний ресурс]. – 101. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12;

5. НД ТЗІ 1.1-002-99 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 - Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс] – Режим доступу до ресурсу: www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106340;

6. НД ТЗІ 1.1-003-99 - Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу; [Електронний ресурс]– Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=46074&cat_id=38835;

7. НД ТЗІ 1.1-005-07 - Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення; [Електронний ресурс] – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102310&cat_id=46556&ctime=1344511142755;

8. НД ТЗІ 1.4-001-00 - Типове положення про службу захисту інформації в АС; [Електронний ресурс] – Режим доступу до ресурсу: www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106341;

9. НД ТЗІ 1.6-005-13 - Положення про категорювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці [Електронний ресурс] – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=107993&cat_id=89734&ctime=1366373635138;

10. НД ТЗІ 2.5-004- Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу; [Електронний ресурс] – Режим доступу до ресурсу: dsszzi.gov.ua/dsszzi/doccatalog/document?id=106342;

11. НД ТЗІ 2.5-005-99 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу; [Електронний ресурс] – Режим доступу до ресурсу: lib.univd.edu.ua/?controller=service&action;

12. НД ТЗІ 3.1-001-07 - Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи; [Електронний ресурс] – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102310&cat_id=46556&ctime=1344511142755;

13. НД ТЗІ 3.3-001-07 - Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації; [Електронний ресурс] – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102265&cat_id=46556&ctime=1344504841243;

14. НД ТЗІ 3.7-001-99 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 – Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в

автоматизованій системі; [Електронний ресурс] – Режим доступу до ресурсу: www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106350;

15. НД ТЗІ 3.7-003 -05 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 - Порядок проведення робіт із створення КСЗІ в ІТС; [Електронний ресурс] – Режим доступу до ресурсу: https://pda.litres.ru/vadim-grebennikov-15/kompleksni-sistemi-zahistu-informaciyi-proektuvannya/chitat-onlayn/page-2;

16. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 р. №1229; [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1229/99;

17. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 № 373; [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF;

18. ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» [Електронний ресурс] – Режим доступу до ресурсу: www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106343;

19. Вимоги до системи захисту інформації [Електронний ресурс] – Режим доступу до ресурсу: https://studfiles.net/preview/6012701/page:6/;

20. Проблеми та шляхи розвитку інформатизації в Україні [Електронний ресурс] – Режим доступу до ресурсу: https://studopedia.info/1-112574.html.

ДОДАТОК А. ВІДОМОСТЬ МАТЕРІАЛІВ КВАЛІФІКАЦІЙНОЇ РОБОТИ

№	Формат	Найменування	Кількість листів
1	А4	Реферат	3
2	А4	Список умовних позначень	1
3	А4	Зміст	2
4	А4	Вступ	1
5	А4	Розділ 1. Стан питання. Постановка задачі	10
6	А4	Розділ 2. Спеціальний розділ	50
7	А4	Розділ 3. Технічно-економічний розділ	9
8	А4	Висновки	1
9	А4	Перелік посилань	3
10	А4	Додаток А. Відомості матеріалів кваліфікаційної роботи	1
11	А4	Додаток Б. Ситауційний план	2
12	А4	Додаток В. Генеральний план	3
13	А4	Додаток Г. Схема підключення мережі	2
14	А4	Додаток Ґ. Схема інформаційних потоків	2
15	А4	Додаток Д. Наказ про створення КСЗІ	1
16	А4	Додаток Е. Перелік матеріалів на оптичному носії	1
17	А4	Додаток Ж. Відгук керівника економічного розділу	1
18	А4	Додаток З. Відгук керівника кваліфікаційної роботи	2

ДОДАТОК Б. СИТУАЦІЙНЙ ПЛАН

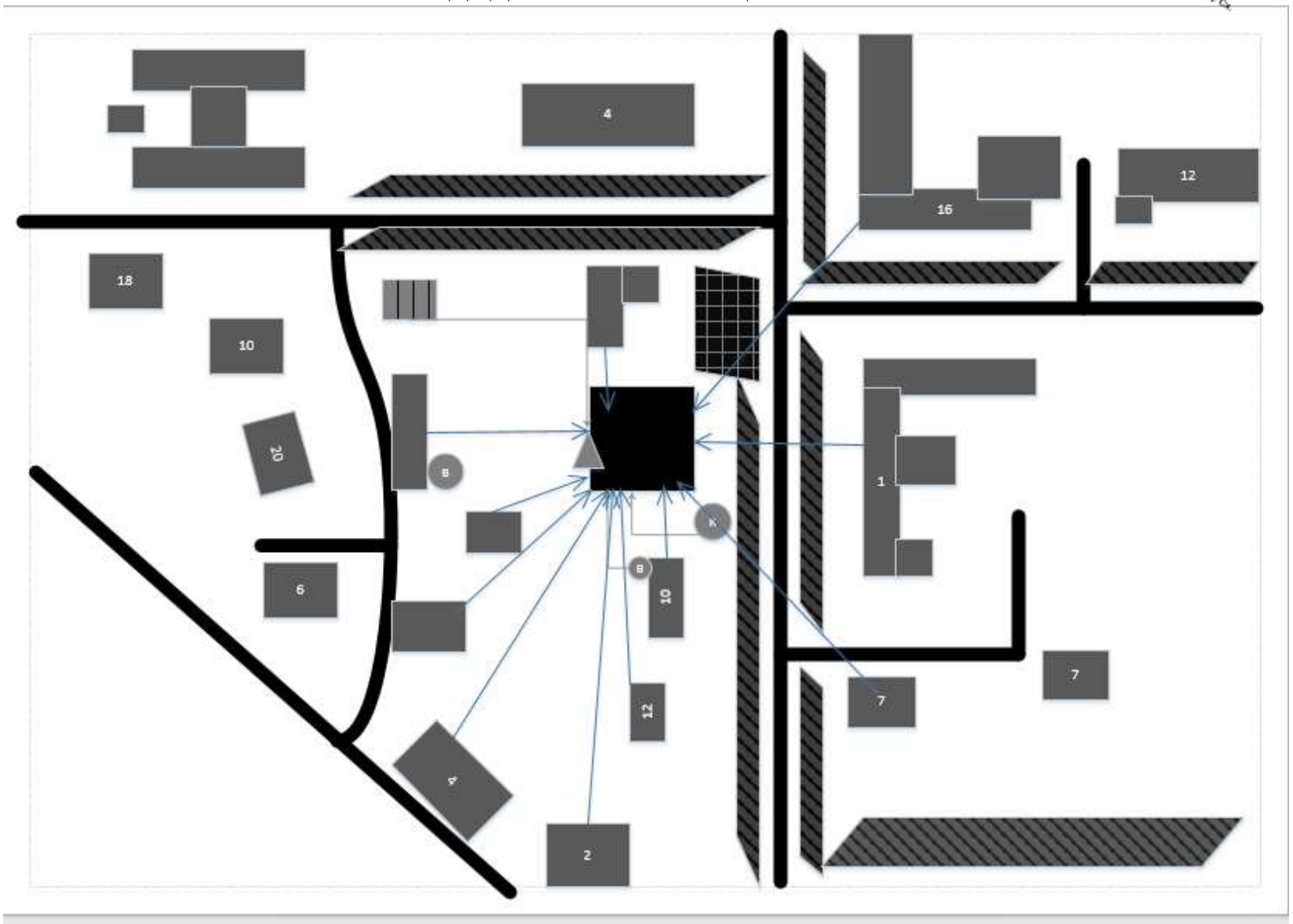


Рисунок 1. Ситуаційний план

Позначення	Пояснення
	Трансформаторна підстанція
	Лінії водопостачання, електропостачання
	Місця для паркування
	Будівля з об’єктом інформаційної діяльності
	Будівля
	Відстань до оід
	Дорога
	Вхід до ОІД
	Люк каналізації
	Люк водопостачання
	Зона росту дерев
	КЗ

ДОДАТОК В. ГЕНЕРАЛЬНИЙ ПЛАН

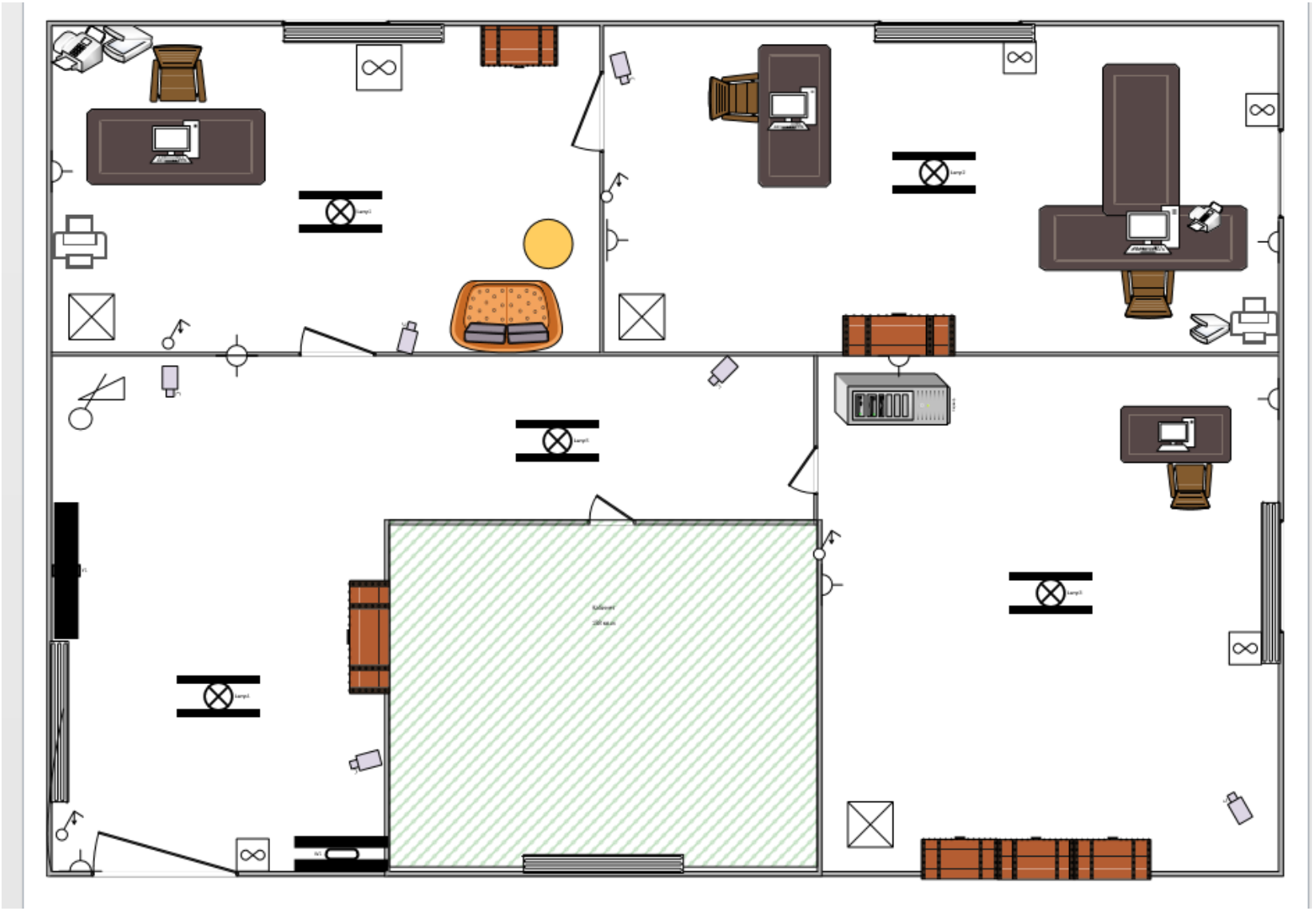
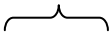
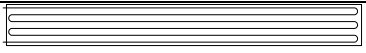


Рисунок 2. Генеральний план

Позначення	Тлумачення
	Решітки
	Факс
	Сканер
	Принтер
	Крісло
	Стіл
	Комп’ютер
	Місце очікування для відвідувачів
	Комбінований датчик на рух та розбиття
	Датчик руху
	ППК (Прилад приймально-контрольний)
	Шафа
	Ключ
	Датчик на відкриття
	Сервер
	Складське приміщення
	Батарея
	Розетка

	Лінія електропостачання
	Вимикач
	Освітлювач
	Лінія опалення
	Камера відеоспостереження

ДОДАТОК Г. СХЕМА ПІДКЛЮЧЕННЯ МЕРЕЖІ

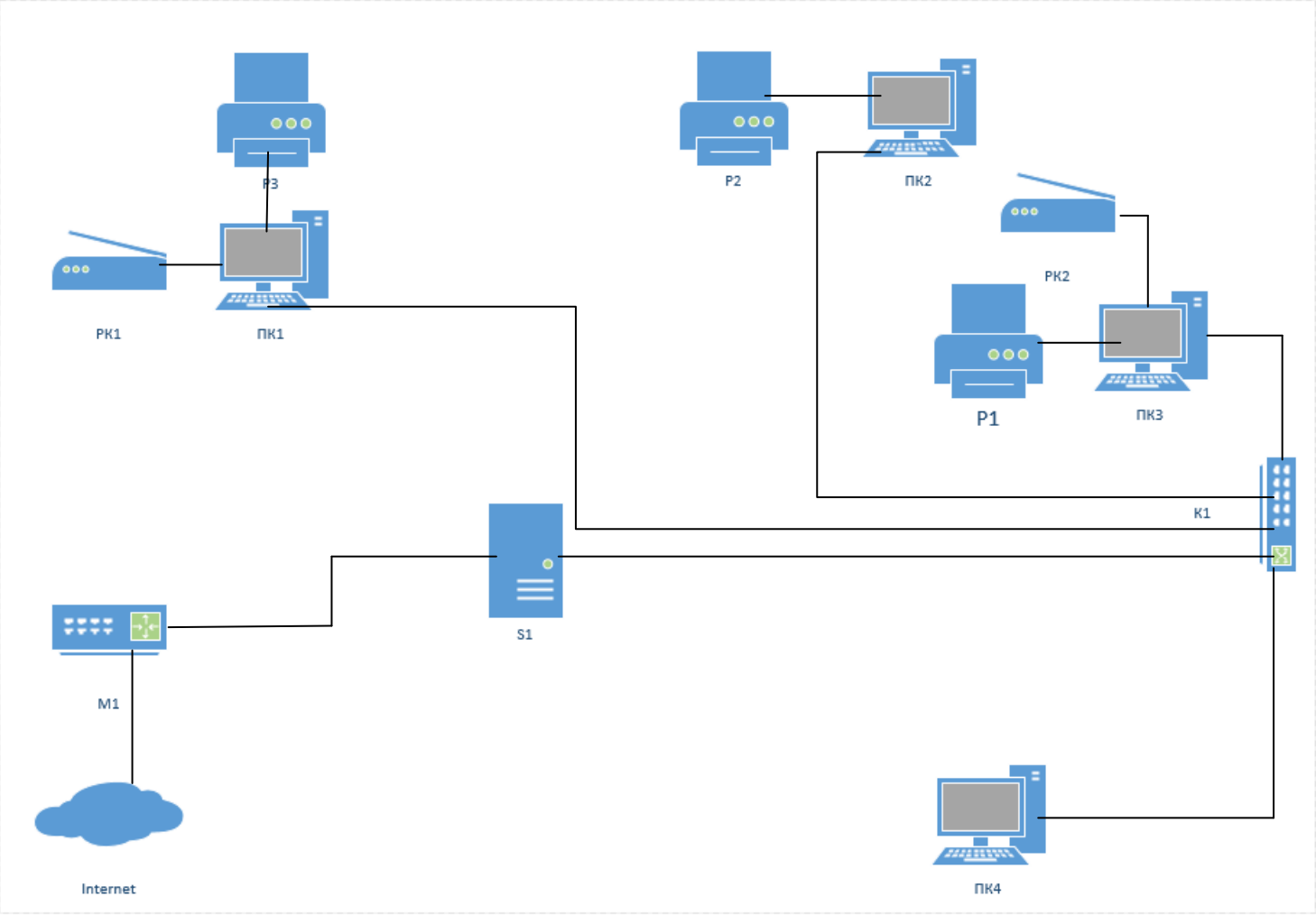
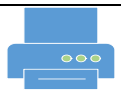


Рисунок 3. Схема підключення мережі

№	Позначення	Тлумачення
1		принтер
2		сканер
3		комп’ютер
4		комутатор
5		сервер
6		маршрутизатор
7		interner

ДОДАТОК Ґ. СХЕМА ІНФОРМАЦІЙНИХ ПОТОКІВ

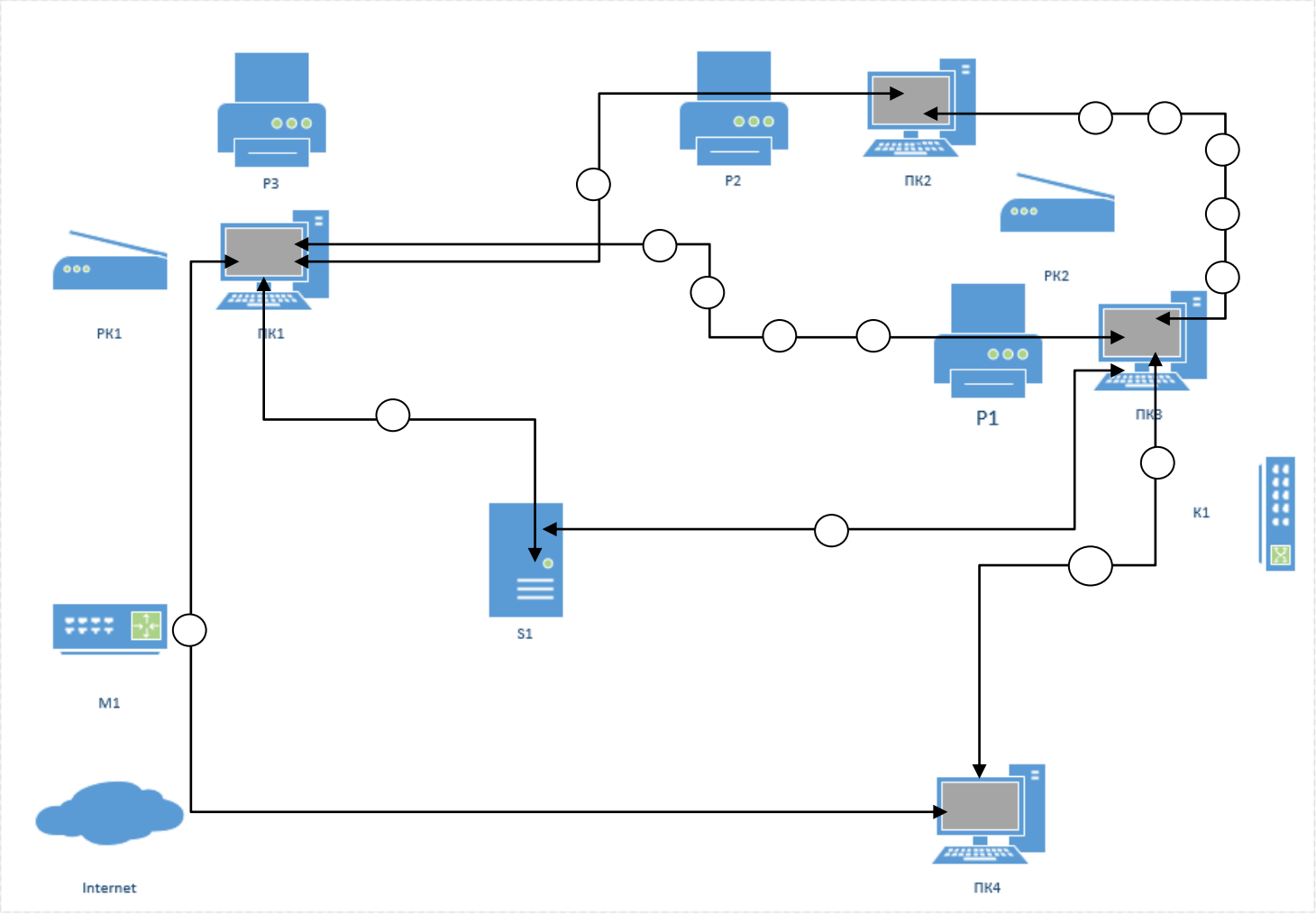


Рисунок 4. Схема інформаційних потоків

№	Позначення	Тлумачення
1	◯	Інформація
2	 ПК1	Робоча станція системного адміністратора
3	 ПК2	Робоча станція бухгалтера
4	 ПК3	Робоча станція директора
5	 ПК4	Робоча станція диспетчера
6		Сервер

ДОДАТОК Д. НАКАЗ НА СТВОРЕННЯ КСЗІ

Приватне підприємство «Оберіг-сервіс»

НАКАЗ

«___»_____ Новомосковськ №_____

Про створення КСЗІ
у приватному підприємстві
«Оберіг-сервіс»

З метою виконання вимог законів України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних», Положення про технічний захист інформації в Україні, затверджений від 27.09.1999 № 1229/99, Правил забезпечення захисту інформації в інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29.03.2006 № 373,

НАКАЗУЮ:

1. Провести обстеження складових інформаційно-телекомунікаційної системи приватного підприємства «Оберіг-сервіс» (далі – підприємство).
2. Створити комплексну систему захисту інформації підприємства.
3. Затвердити політики безпеки інформації інформаційно-телекомунікаційних системи підприємства.
4. Відповідальність за виконання наказу покладаю на себе.

Директор підприємства _____ Петров І.І

ДОДАТОК Е. ПЕРЕЛІК ДОКУМЕНТІВ НА ОПТИЧНОМУ НОСІЇ

1. Кваліфікаційна_робота_Колєснік_Убіт-15-1.docx
2. Презентація_ Колєснік_Убіт-15-1.ppt

ДОДАТОК Ж. ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

Керівник розділу _____ доц. Пілова Д.П.

ДОДАТОК З. ВІДГУК КЕРІВНИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

В І Д Г У К
на кваліфікаційну роботу бакалавра на тему:
"Розробка політики безпеки інформації інформаційно-телекомунікаційної системи приватного підприємства «Оберіг-сервіс»"
студентки групи УБіт-15-1
Колєснік Марини Олександрівни

Мета кваліфікаційної роботи: розробка рекомендацій щодо захисту ресурсів в інформаційно-телекомунікаційній системі приватного підприємства «Оберіг-сервіс».

У зв’язку з постійним підвищенням вимог захисту інформації в інформаційно-телекомунікаційних системах (ІТС) приватних підприємства, що займаються охоронною діяльністю, надання рекомендацій щодо захисту інформаційних ресурсів приватного підприємства «Оберіг-сервіс» є актуальним.

Тема кваліфікаційної роботи безпосередньо пов’язана з об’єктом діяльності бакалавра фаху 6.170103 «Управління інформаційною безпекою», а зміст та структура проекту дозволяють розкрити поставлену задачу повністю.

У ході виконаня роботи були вирішені наступні завдання: проаналізовано умови функціонування інформаційно-телекомунікаційної системи, складені моделі загроз та порушника, за результатами аналізу яких, було детально розроблено елементи політики безпеки інформації:

– політика чистого столу;
– політика безпеки для системного адміністратора;
– політика антивірусного захисту.

Використання цих політик направлено на зниження ймовірності реалізації загроз та є економічно ефективними, що було підтверджено в економічному розділі кваліфікаційної роботи.

Практична значущість проекту полягає в можливості використання розроблених рекомендацій при розробці комплексної системи захисту інформації на реальному об’єкті інформаційної діяльності.

В ході виконання кваліфікаційної роботи студентка Колєснік М.О. проявила самостійність в роботі, працьовитість і володіння теоретичними і практичними знаннями. За час виконання кваліфікаційної роботи КолєснікМ.О. виявила себе фахівцем, здатним самостійно, на високому рівні вирішувати поставлені задачі.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

Загалом кваліфікаційна робота виконана у відповідності до вимог, що ставляться до кваліфікаційної роботи бакалавра та заслуговує оцінки *“добре”*, а Колєснік Марина Олександрівна присвоєння їй кваліфікації фахівця із організації інформаційної безпеки.

Керівник кваліфікаційної роботи,
доцент кафедри БІТ С.В. Флоров

Керівник спеціальної частини Ю.А Мілінчук
ас. каф. БІТ.