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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Тітова Дмитра Сергійовича*

академічної групи *125-16-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка політики безпеки інформації інформаційно-телекомунікаційної системи ТОВ "Кредит - Легко"*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	кт. н. доц. Галушко О.М.			
розділів:				
спеціальний	ст.в. Тимофєєв Д.С.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст.в. Тимофєєв Д.С.			

Дніпро
2020

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Тітову Дмитру Сергійовичу* **академічної групи** *125-16-1*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації _____

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка політики безпеки інформації інформаційно-телекомунікаційної системи ТОВ "Кредит - Легко"*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 26.05.20 № 275-С

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз нормативно-правової бази в сфері захисту інформації, актуальність проблеми захисту інформації в ІТС, задачі на розробку ПБ на ОІД.	06.04.2020
Розділ2	Обстеження на об'єкті інформаційної діяльності, аналіз середовища функціонування, аналіз ризиків, розробка основних положень політики безпеки	07.05.2020
Розділ 3	Визначення економічної доцільність впровадження політики безпеки, розрахунки витрат та ефекту від впровадження ПБ.	25.05.2020

Завдання видано _____ Тимофєєв Д. С.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: _____08.01.2020_____

Дата подання до екзаменаційної комісії: ___11.06.2020_____

Прийнято до виконання _____ Тітов Д. С.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 75 с., 5 рис., 14 табл., 4 додатків., 27 джерел.

Об’єкт розробки: інформаційно-телекомунікаційна система (ІТС) ТОВ "Кредит - Легко".

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

Мета кваліфікаційної роботи: підвищення рівня захищеності інформації в ІТС ТОВ "Кредит - Легко".

У першому розділі розглянуто питання захисту інформації взагалі, та в фінансовому секторі зокрема. Проведено аналіз нормативно-правової бази у сфері захисту інформації . Виконано постановку задачі.

У спеціальній частині проведено акт обстеження на об’єкті, описані середовища функціонування інформаційно-телекомунікаційної системи організації. Проведено класифікацію джерел загроз та вразливостей. Складено модель загроз та порушника. Обрано профіль захищеності системи. Розроблені політики безпеки для ТОВ "Кредит - Легко".

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

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ПОЛІТИКА БЕЗПЕКИ, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА.

ABSTRACT

Explanatory Note 75 p., 5 pictures., 14 tab., 4 applications., 27 sources.

Object of development: information and telecommunication system LLC "Credit - Easy."

Subject of research: information security policy of the information activity object.

The purpose of the qualification work: to increase information security level of information and telecommunication system of "Credit - Easy" LLC.

The first part of the study addresses information security issues in general, and in the financial sector in particular. The analysis of the regulatory framework in the field of information protection. The problem statement is completed.

The special part of the study considers the described functioning environment of the information and telecommunication system of the organization. The classification of sources of threats and vulnerabilities is carried out. A model of threats and an intruder has been compiled. The security profile of the system has been selected/ Developed security policies for LLC "Credit - Easy".

The third part defines the economic feasibility of implementing an information security policy. The calculations of capital costs, operating expenses, estimates of the amount of damage and the overall effect of the implementation of information security.

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

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ТОВ – товариство з обмеженою відповідальністю;

АС - автоматизована система;

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;

ПЗ – програмне забезпечення;

ТЗІ – технічні засоби інформації

СЗІ – системи захисту інформації

СУІБ – система управління інформаційною безпекою;

ЕЦП – електронний цифровий підпис;

ЗМІСТ

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Сучасний етап розвитку суспільства характеризується зростаючою роллю інформаційних технологій. Необхідність використання інформаційних технологій вже не викликає ніяких сумнівів, оскільки технологія — це одна з областей сучасного життя, що динамічно розвиваються.

Нажаль темпи якими розвивається сучасна кіберзлочинність випереджають глобальну індустрію кібербезпеки в цілому і українську зокрема, на декілька кроків вперед. Кількість кібератак, як і їх масштаби в світі та Україні, збільшуються з кожним роком. У засобах масової інформації, Інтернеті викладається великий обсяг інформації про вчинені кіберзлочини, збитки від них, про потерпілих, окремі аналізи кіберзлочинності в межах однієї країни або групи країн. Експертами компанії у сфері кібербезпеки [1] було подано відсоток кібератак у світі: США - 38%; Індія - 17%; Японія - 11%; Тайвань - 7%; Україна - 6%; Південна Корея - 6%; Бруней - 4%; Росія - 4%; В'єтнам - 4%; Пакистан - 3%. Згідно даних опублікованих на цьому ж сайті, спостерігається наступна тенденція росту зараженості шкідливим програмним забезпеченням у світі за останні 10 років (див. рисунок 1.1).

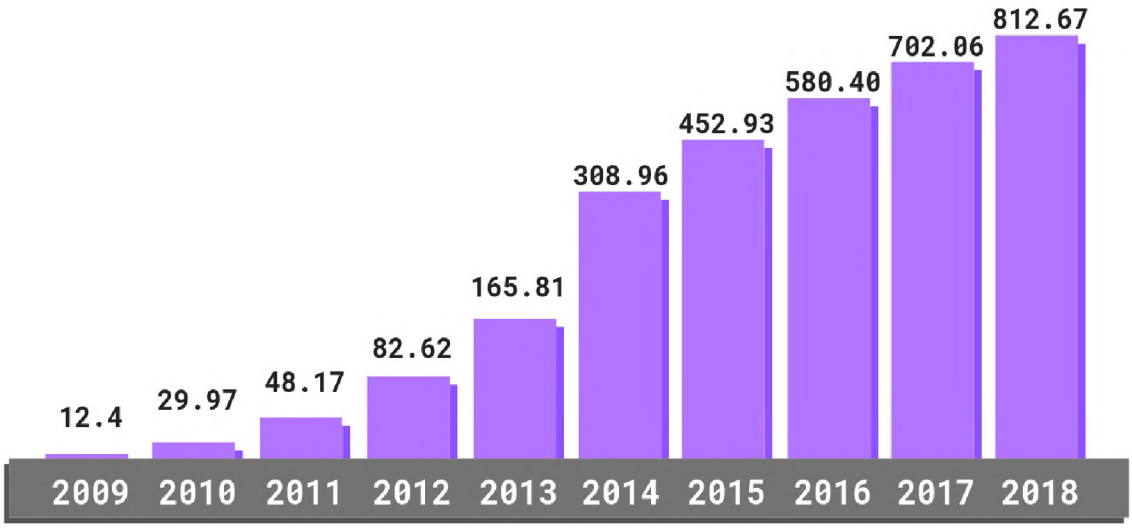

Рисунок 1.1 Графік темпів зростання зараження шкідливим ПЗ

Український сервіс OpenDataBot опублікував статистику кіберзлочинів в Україні за останні 5 років. Згідно з підрахунками, за ці роки кількість інформаційних злочинів зросла щонайменше у 2,5 рази. Стрибок кількості всіх кіберзлочинів відбувся у 2017 році. Значною міро він пов'язаний із вірусом "Petya". Однак відтоді кількість інформаційних злочинів не знижується.

Основний удар кіберзлочинців направлений на малий та середній бізнес, так як він має менш складну інфраструктуру і методи забезпечення безпеки, а також недостатню кількість навченого персоналу для управління загрозами та реагування на них.

Фінансовий сектор особливо вразливий для кібератак. Фінансові організації є привабливими об'єктами через їх важливу роль як посередників у русі грошових коштів. Успішна кібератака на одну організацію може швидко поширитися на інші через взаємопов'язану фінансову систему. Пряма кібератака може мати прямі суттєві наслідки у виді фінансових збитків, а також непрямих витрат, таких як втрата репутації. Аналізуючи світову статистику безпеки у фінансовому секторі було встановлено що: 67% фінансових установ повідомляють про збільшення кібератак за останній рік; 25% усіх атак зловмисних програм стосуються банків та інших фінансових галузей, це більше ніж будь-яка інша галузь; витоки облікових даних із фінансових установ збільшились на 129%, зараження шкідливими програмами зросло на 102% 31% фінансових установ повідомили про збільшення шахрайства з позиками власного капіталу, 79% фінансових установ зазначили, що кіберзлочинці стали більш досконалими, використовуючи соціальну інженерію; 69% фінансових установ планують збільшити виплати на кібербезпеку на 10% або більше.

Для підприємств, що займаються колекторською діяльністю, поверненням боргів юридичних осіб, купівлею боргів, що мають справу з персональними даними та комерційною таємницею є дуже важливим запобігати та боротися з загрозами кібербезпеки, з якими вони зіштовхуються. Ці загрози ростуть та розвиваються з великою швидкістю.

Від кібератак організації грошово-кредитної системи страждають в найбільшій мірі. В організаціях, що займаються фінансовою діяльністю, зосереджується найчастіше секретна інформація про фінансову і господарську діяльність багатьох людей, компаній та організацій. Ці підприємства зберігають та оброблюють цінну інформацію про своїх клієнтів, що розширює коло потенційних зловмисників, зацікавлених в крадіжці або псуванні такої інформації

Типи масових кібератак на компанії, що працюють в секторі по поверненню боргів мало відрізняться від атак на компанії, що працюють в інших секторах економіки. Поширені загрози кібербезпеки, з якими стикаються підприємства даної галузі це:

- крадіжка особистих даних і втрата конфіденційних даних. Ця інформація може бути особливо цінною для зловмисників, вони можуть використовувати добуту інформацію в якості інструменту для шахрайства, здирництва та інших фінансових злочинів.

- автоматизовані загрози. Злом облікових даних, сканування вразливостей, погані боти, заповнення облікових даних і відмова в обслуговуванні можуть потенційно швидко відключити системи компанії.

- порушення бізнесу. Кібератаки можуть серйозно підірвати бізнес, наприклад стерти комп'ютерну інфраструктуру включаючи телефонні довідники, електрону пошту, а також ділові записи, наприклад шаблони договорів. Така атака на компанію може на деякий час перервати її роботу. Проблеми захисту інформації для підприємств, що займаються фінансовою, в тому числі, колекторською діяльністю:

- проблема збереженості цілісності даних;

- проблема захисту від комп'ютерних вірусів;

- проблема фізичного несанкціонованого доступу до інформації.

1.2 Нормативно-правова база

Згідно Доктрини інформаційної безпеки України [3] визначено реальні та потенційні загрози інформаційній безпеці країни в економічній сфері:

- Недостатній рівень інформатизації економічної сфери, зокрема кредитно-фінансової системи;

- Несанкціонований доступ до інформаційних і телекомунікаційних мереж та систем, що може порушити діяльність стратегічно важливих для економіки підприємств;

- Використання неліцензійного програмного забезпечення, засобів і комплексів обробки інформації;

Під час розроблення політики безпеки інформації на підприємстві, що займається фінансовою діяльністю слід керуватися наступними нормативно-правовими документами та актами. Ці документи регламентують та визначають порядок захисту властивостей інформації (конфіденційності, цілісності та доступності), також регламентують порядок ефективного знешкодження загроз шляхом побудови комплексної системи захисту інформації; визначають права, обов'язки й відповідальність персоналу роботи яких пов'язані з інформаційною безпекою:

- Конституція України — основний закон України, прийнятий Верховною Радою України 28 червня 1996 року. В ній зокрема, є норми , що стосуються забезпечення інформаційної безпеки України та які є визначальними для побудов національної системи інформаційної безпеки.

- Закон України “ Про інформацію ” [4] - цей Закон регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації. Дія цього Закону поширюється на інформаційні відносини, які виникають у всіх сферах життя і діяльності суспільства і держави під час одержання, використання, поширення та зберігання інформації.

- Закон України “ Про захист інформації в інформаційно-телекомунікаційних системах ” [5] - цей Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Зокрема, об'єктами захисту в таких системах відповідно до Закону є інформація, що обробляється та програмне забезпечення, яке призначене для обробки цієї інформації. Суб'єктами відносин, пов'язаних із захистом інформації в системах Закон визначає: власників інформації та інформаційно-

телекомунікаційних систем, користувачів інформації та систем, а також уповноважений орган у сфері захисту інформації в інформаційно-телекомунікаційних системах.

- Закон України “ Про захист персональних даних ” [6] - цей Закон регулює правові відносини, пов'язані із захистом, обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя у зв'язку з обробкою персональних даних.

- Постанова Кабінету міністрів України “ Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. ” Від 29.03.2006. №373 поточна редакція від 13.10.2011 [7] — ці Правила визначають загальні вимоги та організаційні засади забезпечення захисту державних інформаційних ресурсів або інформації , вимога щодо захисту якої встановлення законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

- НД ТЗІ 1.1-002-99 [8] Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу — визначає методологічні основи вирішення завдань захисту інформації в комп'ютерних системах і створення документів що визначають вимоги щодо захисту комп'ютерних систем від несанкціонованого доступу, створення захищених комп'ютерних систем і засобів їх захисту від несанкціонованого доступу та оцінки захищеності комп'ютерних систем і їх придатності для вирішення завдань споживача. Документ призначено для постачальників, споживачів комп'ютерних систем, які використовуються для обробки (в тому числі збирання, зберігання, передачі) критичної інформації (інформації що вимагає захисту)

- НД ТЗІ 1.1-005-07 [9] Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення. - 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 можна використовувати під час

обґрунтування, організації розроблення, впровадження заходів захисту ІзОД від загроз.

- НД ТЗІ 1.4-001-2000 [10] Положення про службу захисту інформації. — встановлює вимоги до структури та змісту нормативного документу, що регламентує діяльність служби захисту в автоматизованій системі. Нормативний документ призначений для суб'єктів відносин, діяльність яких пов'язана з обробкою інформації в автоматизованих системах інформації, що підлягає захисту згідно з нормативно-правовими актами, а також для розробників комплексних систем захисту інформації в автоматизованих системах.

- НД ТЗІ 1.6-005-2013 [11] Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці - 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] Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи. - 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] Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації. - визначає порядок проведення робіт

на об’єкті інформаційної діяльності підприємства на етапі розроблення та впровадження заходів із захисту від витоку інформації з обмеженим доступом технічними каналами під час створення комплексу ТЗІ.

- НД ТЗІ 3.6-001-2000 [14] Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. — встановлює єдині вимоги до порядку створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу в комп'ютерних системах та захищених від несанкціонованого доступу компонентів обчислювальних систем. Дія нормативного документу поширюється на апаратні, програмні та програмно-апаратні засоби ТЗІ, призначені для використання в комп'ютерних системах, де обробляється, накопичується, зберігається та передається інформація, що підлягає технічному захисту. Документ призначений для виробників та розробників (впроваджувальних організацій), споживачів (замовників, користувачів) засобів ТЗІ, а також для органів, що здійснюють функції оцінювання засобів ТЗІ на відповідність вимогам НД ТЗІ.

- НД ТЗІ 3.7-001-99 [15] Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. — встановлює вимоги до порядку розробки, складу і змісту технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі призначеній для оброблення,зберігання і передачі інформації з обмеженим доступом або інформації захист якої гарантується державою. Положення цього документа розповсюджуються на підприємства, установи і організації всіх форм власності, які володіють, користуються та розпоряджаються інформацією вимога щодо захисту якої встановлена законом. Власники(користувачі) іншої інформації, положення цього документа застосовують на свій розсуд.

- НД ТЗІ 3.7-003-2005 [16] Порядок проведення робіт і створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. - 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. Дія документу поширюється тільки на ІТС, в яких здійснюється обробка інформації автоматизованим способом. 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 [17] Захист інформації. Технічний захист інформації. Порядок проведення робіт. - установлює вимоги до порядку проведення робіт з технічного захисту інформації, що є обов`язковими для підприємств та установ усіх форм власності й підпорядкування.

- ДСТУ ISO/IEC 27001:2015 [18] - Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT)- На заміну ДСТУ ISO/IEC 27001:2010 – цей стандарт створений для визначення вимог для розроблення,впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення системи управління інформаційною безпекою (СУІБ).

- ДСТУ ISO/IEC 27002:2015 [19] - Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor1:2014,

IDT) – цей міжнародний стандарт розроблено для організацій для використання як довідкової інформації щодо вибору заходів безпеки під час впровадження СУІБ на базі ISO/IEC 27001 або як настанову для організацій, які впроваджують загальноприйняті заходи інформаційної безпеки. Цей стандарт також призначено для використання в розробленні настановних документів з управління інформаційною безпекою, специфічних для промисловості та організацій, з урахуванням специфічних ризиків інформаційної безпеки їх середовища.

1.3 Постановка задачі

Для того щоб зменшити ризики для бізнесу та забезпечити безперервність діяльності всіх підрозділів підприємства треба забезпечити захист інформації, для цього розробити політику безпеки інформації ІТС ТОВ "Кредит — Легко". Необхідно провести обстеження фізичного та інформаційного середовища підприємства, обстеження обчислювальної системи, середовища користувачів, провести класифікацію джерел загроз та вразливостей, скласти модель загроз та модель порушника, виконати розробку основних елементів безпеки інформації та економічно обґрунтувати доцільність впровадження політики безпеки підприємства.

Висновок до розділу 1

У даному розділі були розглянуті темпи росту кіберзлочинності в світі та Україні, зокрема наведена статистика порушень інформаційної безпеки у фінансовому секторі і розглянуті проблеми захисту інформації для об'єктів, що займаються фінансовою діяльністю, в тому числі колекторською, поверненням боргів юридичних осіб, купівлею боргів та зроблено аналіз нормативно-правових документів в сфері захисту інформації, які використовуються на даних підприємствах та організаціях. Визначено завдання на спеціальну частину.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про ТОВ “Кредит — Легко”

Організація ТОВ «Кредит -Легко» веде - колекторську діяльність на передсудовому і судовому етапах. Займається поверненням боргів юридичних осіб в не судовому порядку, стягненням боргів в арбітражному суді, купівлею боргів.

Форма власності: «Кредит -Легко» комерційна організація, зареєстрована як товариство з обмеженою відповідальністю, на основі приватної власності статутний капітал 50000 грн.

Діяльність організації пов'язана з взаємодією з юридичними і фізичними особами на основі договору надання послуг, пов'язаних з колекторською діяльністю. Клієнти організації надають відомості про своїх боржників, і дебіторів. ТОВ «Кредит -Легко» має справу з комерційною таємницею і персональними даними. Вищий гриф конфіденційності визначений як - строго конфіденційно.

Підприємство функціонує 5 днів на тиждень. Графік роботи з 8:00 до 18:00, з перервою на обід з 12.00 до 13.00. У період обідньої перерви організація не займається основною діяльністю, служба охорони і зокрема співробітник бюро перепусток відповідно до інструкції з охорони і пропускного режиму обідають на місці.

2.2 Обґрунтування необхідності створення КСЗІ

Згідно норм чинного законодавства України щодо захисту інформації доступ до деяких видів інформації має бути обмеженим. Для цього створюється КСЗІ в якій рішення про забезпечення цілісності та доступності інформації в тому числі порядок доступу до інформації, перелік користувачів і їх права відносно цієї інформації визначається власником інформації, а відповідальність за забезпечення захисту інформації покладається на власника системи. Згідно з наказом (див. додаток А) було проведено обстеження і категоріювання об'єкта інформаційної діяльності ТОВ "Кредит - Легко", після чого йому була присвоєна

четверта категорія. Генеральним директором було прийнято рішення та видано наказ про створення КСЗІ на підприємстві (див. додаток Б).

2.3 Обстеження на об'єкті інформаційної діяльності

Обстеження фізичного середовища: Об'єкт знаходиться за адресою м.Кам'янське, проспект Незалежності 48, на 7 поверсі дванадцятиповерхової офісної будівлі, в правому крилі. Об'єкт розташований в діловій частині міста. З трьох боків оточений різними будівлями, четверта сторона виходить на автомобільну дорогу. Із заходу, на відстані 25 метрів, розташоване висотна офісна будівля з паркувальним майданчиком. З південного боку, на відстані 40 метрів, розташована багатоповерхова житлова будівля. Зі сходу, на відстані 25 метрів, розташовано адміністративну будівлю. З півночі розташована автомобільна дорога.

Характеристика складових ОІД:

– висота стель – 350 мм;

– перекриття(стеля, підлога) — залізобетонні, товщина 500 мм;

– стінні перегородки – залізобетон, товщина 500 мм;

– стіни зовнішні залізобетонні – товщина 700 мм з внутрішньої сторони стіни оброблені під євростандарт.

Вікна: розмір отвору 2000*1500 мм, тип вікна: металопластикові з подвійним потовщеним склом(ОРС 18 - 15В).

Двері в приміщення виготовлені із двох сталевих листів. Товщина дверей 70 мм. Розміри(ширина*висота) 950*2100 мм. Замок механічний врізний.

Територія підприємства обладнана одним КПП для персоналу. Максимальне навантаження 120 чол/год. Співробітники підприємства проходять КПП, підносячи постійний пропуск до зчитувача карт на турнікеті.

КПП виконано у вигляді турнікету з пристроєм для читання карт. На КПП є ручний металодетектор. Протоколюється пропуск відвідувачів через прохідну.

Присутня система відеоспостереження. Відвідувачі підприємства отримують тимчасові пропуски при пред'явлені посвідчення особи. Процедура видачі пропуску фіксується в електронному журналі обліку виданих перепусток. Після видачі пропуску, відвідувач може прийти на територію підприємства. При виході, відвідувач зобов'язаний здати тимчасовий пропуск на КПП. У журналі робиться відмітка про вибуття відвідувача і здачі пропуску.

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

Система електроживлення - Мережа 220В/50Гц. Використовуються LED лампи 12Вт. 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: пожежною сигналізацією обладнані усі приміщення за винятком туалетів. Застосовується три типи сповіщувачів: димовий, тепловий і ручний. Ручні сповіщувачі встановлені на шляхах евакуації. Димові сповіщувачі встановлені в коридорі та інших приміщеннях. Кабінет директора і приміщення для конфіденційних переговорів додатково обладнані тепловими сповіщувачами. Електропроводка пожежної сигналізації виконується кабелем, який не розповсюджує горіння, що прокладається в монтажних коробках.

- охоронна: датчики руху, акустичні датчики розбиття скла, магніто-контактні сповіщувачі на відкриття дверей.

Живлення систем освітлення, електропостачання та опалення здійснюється через підключення до міських комунальних мереж.

Таблиця 2.1 - Системи комунікації

Система комунікації	Тип підключення
Електропостачання	Підключено до трансформаторної підстанції №8, яка має сторонніх споживачів і знаходиться за межами КЗ

Продовження таблиці 2.1

Система комунікації	Тип підключення
Заземлення	Всі прилади, комп'ютери заземлені на спільний контур заземлення, який є замкнутий і виходить за межі КЗ
Система вентиляції	Припливно-витяжна
Internet	Кабельне підключення, що виходить за межі ОІД
Система водопостачання	Підключена до міського водоканалу, яка знаходиться за межами КЗ
Система опалення	Підключена до міської мережі опалення, знаходиться за межами КЗ
Система каналізації	Підключена до міської мережі, яка знаходиться за межами КЗ

Підприємство складається з наступних структурних підрозділів:

• Служба безпеки - служба, яка виконує функції допоміжних процесів організації, вона виконує функції з інформаційної безпеки організації, пропускного режиму, організації фізичної охорони активів. Служба інформаційної безпеки розташована в службовому приміщенні;

• Юридичний відділ - відділ основних бізнес-процесів підприємства, він займається роботою зі справами клієнтів, організовує діяльність представників організації в арбітражних судах і досліджує фінансову активність боржників. Також юридичний відділ відповідає за правове забезпечення діяльності організації як господарюючого суб'єкта, включаючи правове забезпечення інформаційної безпеки. Юридичний відділ знаходиться в службовому приміщенні;

• Бухгалтерія - служба, яка займається веденням бухгалтерської та податкової звітності, за сумісництвом виконує функції фінансового відділу, тим самим, розподіляючи фінансові потоки внутрішнього і зовнішнього середовища організації, в тому числі, бухгалтерія фінансує діяльність служби безпеки підприємства;

• Служба охорони - частина служби безпеки, що відповідає за організацію та ведення пропускного режиму на підприємстві та охоронної діяльності. Служба розташована в окремому приміщенні;

• Клієнтський відділ - відділ, який організовує взаємодію організації з клієнтами. У клієнтському відділі полягають бізнес-контракти організації, надаються звіти про виконану роботу клієнтам. Клієнтський відділ веде касові операції з розрахунку з клієнтами;

• Відділ кадрів - виконує функції по забезпеченню вакансій на підприємстві, управління людськими ресурсами, ведення особистих справ співробітників і організацією розвитку корпоративної культури, спортивних та інших заходів;

• Серверна - сховище основних баз даних, включаючи персональні дані 2 категорії, і іншу інформацію з грифом строго конфіденційно. Доступ до серверної мають тільки співробітники відділу безпеки.

Рисунок 2.1 – План приміщення

Штат співробітників підприємства складається з 16 осіб. На рисунку 2.2 зображена організаційна структура робітників підприємства.

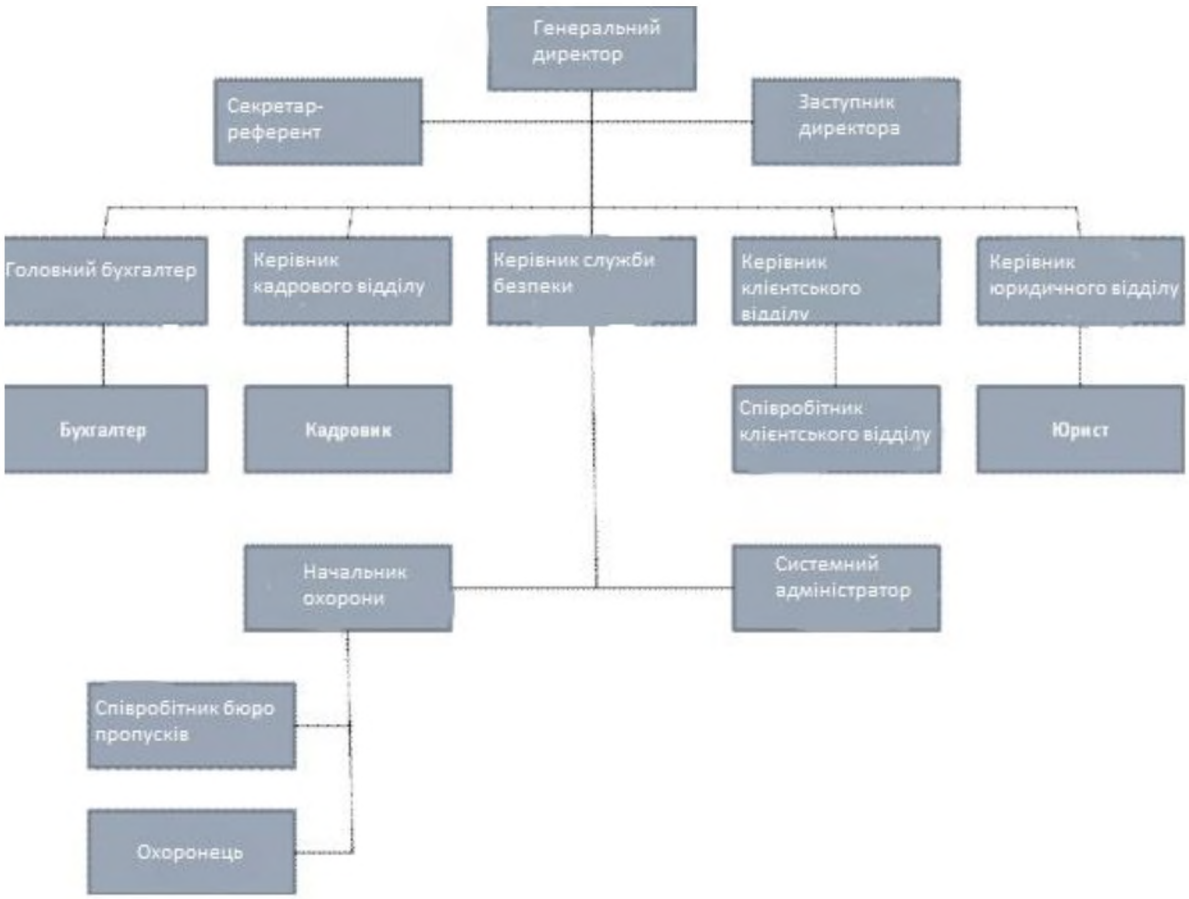

Рисунок 2.2 - Організаційна структура ТОВ «Кредит — Легко»

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

Обов'язки генерального директора. Генеральний директор керує господарською та фінансово-економічною діяльністю організації згідно з діючим законодавством України. Організовує роботу і ефективну взаємодію всіх структурних підрозділів організації. Забезпечує дотримання законності діяльності підприємства, організовує розробку і впровадження прогресивних форм управління і організації праці, раціонального використання виробничих резервів і економічного витрачання всіх видів ресурсів.

Обов'язки заступника директора. Заступник директора підпорядковується безпосередньо директору. Безпосередньо при відсутності генерального директора або за його дорученням веде перемовини з замовниками, потенційними партнерами та іншими організаціями. Контролює дотримання працівниками трудової та виробничої дисципліни, правил і норм охорони праці. Забезпечує

доведення до відомості робітників і виконання ними розпоряджень і наказів генерального директора.

Обов'язки секретаря-референта. Секретар-референт здійснює роботу по організаційно-технічному забезпеченню адміністративно-розпорядчої діяльності генерального директора, приймає кореспонденцію, що надходить на розгляд генерального директора і передає її згідно з прийнятим рішенням в структурні підрозділи ТОВ. Веде діловодство, виконує операції з використанням комп'ютерної техніки, призначеної для збору та обробки інформації при підготовці та прийнятті рішень.

Обов'язки системного адміністратора. Підготовка і збереження резервних копій даних, їх періодична перевірка і знищення. Встановлення і конфігурування оновлень ОС і прикладного ПЗ. Створення і підтримка в актуальному стані файлу облікових записів користувачів. Підтримання інформаційної безпеки в організації. Усунення неполадок в комп'ютерній системі.

Інформація що обробляється: Власником інформації виступає генеральний директор. В автоматизованій системі відсутня інформація, що є власністю держави або відомості, які становлять державну таємницю. 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. В організації циркулює велика кількість персональних даних, як клієнтів так і співробітників організації, всього 50000 об'єктів ПД. В організації ТОВ «Кредит — Легко» вся інформація, що захищається за режимом доступу розділяється на два рівня:

1. Конфіденційно — до такої інформації належить вся інформація, що захищається, яка не має гриф строго конфіденційно.

2. Строго конфіденційно — така інформація включає:

- персональні дані клієнтів і співробітників організації 2 категорії;
- відомості про концепцію розвитку підприємства, стратегічні плани розвитку, функціональні, маркетингові, фінансові та логістичні моделі ведення бізнесу;
- тактичні плани розвитку, інформація про поточні та планові контракти;

- відомості, що розкривають засоби захисту інформації, порядок обробки і передачі інформаційних активів.

Таблиця 2.2 Класифікація інформації

№	Опис	Правовий режим	Режим доступу	Вимоги до захисту	Доступ мають
1	Організаційно-розпорядча документація	Конфіденційна	ІзОД	К, Ц , Д	ГД, ЗД, СР, ГБ, ККадВ, КСБ, ККлВ, КЮВ, НО, СА
2	Облік внутрішніх документів	Конфіденційна	ІзОД	К, Ц , Д	ГД, ЗД, СР, ГБ, ККадВ, КСБ, ККлВ, КЮВ, НО, СА
3	Інформація про надання послуг, тарифна, контактна інформація підприємства	-	Відкрита, потребує захисту	Ц , Д	ГД, ЗД, СР, ГБ, Б, ККаД, К, КСБ, ККлВ, СКлВ, КЮВ, Ю, НО, СБП, СА
4	Інформація про робітників	Конфіденційна	ІзОД	К, Ц , Д	ГД, ЗД, СР, ГБ, ККадВ, КСБ, ККлВ, КЮВ, НО, СА
5	Статутні документи підприємства	-	Відкрита, потребує захисту	Ц , Д	Всі працівники
6	Персональні дані клієнтів	Конфіденційна	ІзОД	К, Ц , Д	ГД, ЗД, КСБ, ККлВ, СА

Продовження таблиці 2.2

№	Опис	Правовий режим	Режим доступу	Вимоги до захисту	Доступ мають
7	Концепції розвитку підприємства, стратегічні плани розвитку, функціональні, маркетингові, фінансові та логістичні моделі ведення бізнес	Конфіденційна	ІзОД	К, Ц , Д	ГД, ЗД, СР, ГБ, КЮВ
8	Поточні та планові контракти	Конфіденційна	ІзОД	К, Ц , Д	ГД, ЗД, СР, ККлВ, СКлВ, КЮВ, Ю
9	Конфігураційні файли СЗІ, паролі, ЕЦП	Конфіденційна	ІзОД	К, Ц , Д	ГД, ЗД, КСБ, СА
10	Документи обліку та реєстрації	Конфіденційна	ІзОД	К, Ц , Д	ГД, ЗД, СР, ГБ, ККадВ, КСБ, ККлВ, КЮВ, НО, СА

Скорочення в таблиці: генеральний директор-ГД; заступник директора-ЗД; секретар-референт-СР; головний бухгалтер-ГБ; бухгалтер-Б; керівник кадрового відділу-ККадВ; кадровик-К; керівник служби безпеки-КСБ; керівник клієнтського відділ-ККлВ; співробітник клієнтського відділу-СКлВ; керівник юридичного відділу-КЮВ; юрист-Ю; начальник охорони-НО; системний адміністратор-СА; співробітник бюро пропусків-СБП; охоронець-О.

Обстеження обчислювальної системи:

Обчислювальна система є розподіленою – пристрої мають вихід до глобальної мережі. Структурна схема зображена на рисунку 2.4, а також в таблиці наведені відомості про компоненти ІТС. Локальна мережа створена для забезпечення внутрішніх потреб підприємства. Для забезпечення взаємодії з зовнішніми організаціями всі робочі станції мають доступ до мережі Internet кабельним підключенням; роутер Wi-Fi забезпечує підключення до мережі Internet. Підключення до мережі забезпечує провайдер "Київстар".

Обладнання АС, за допомогою якого обробляється інформація на ОІД: робочі станції генерального директора; робоча станція секретаря-референта; робоча станція системного адміністратора; робоча станція бухгалтерії; робочі станції відділу роботи з клієнтами, робоча станція юридичного відділу, робоча станція відділу кадрів, робоча станція у приміщенні проведення конфіденційних перемовин, БФП, що підключений до робочої станції директора; мережевий принтер.

ІТС ОІД представляє собою мережу типу «зірка», з окремо підключеним сервером та з використанням одного комутатору. Структурна схема та схема розміщення обчислювальної техніки представлені на рисунку 2.3 і 2.4, та в таблиці 2.3 наведені відомості про компоненти ІТС.

Таблиця 2.3 Технічні характеристики клієнтських ПК

№	Тип	Найменування	кількість
1	Процесор	CPU AMD Sempron 2800 + Socket AM 2	11
2	Системна плата	MB MSI <MS-7260-010> K9N Neo-F (S AM2, nForce 550, ATX, PCI-E x16, 2DDRII ,SB,1GbitLAN, RAID, SATA, U2.0, U 133)	11
3	Жорсткий диск	HDD Seagate 500Gb <ST380811AS>, 7200rpm, SATA-II, 8mb cache	11
4	ОЗУ	DDR 4 DIMM 4Gb PC6400, 800Mhz, Elixir	11

Продовження таблиці 2.3

№	Тип	Найменування	кількість
5	Відеоадаптер	PCI-E 16x ASUS EAX300SE-X/TD <ATI Radeon X300SE> 128MB DDR (TV-Out, DVI) <RTL>	11
6	Корпус	Inwin ATX <J508> 350W, P4, USB,w/fan	11
7	Монітор	Monitor 17" BENQ <FP73G> LCD	11
8	Миша	Microsoft BasicBlack PS/2	11
9	Клавіатура	Keyboard Colors-it KB-1906 PS/2, White (біла)	11
10	Мережевий адаптер	10/100/1000Mbps PCI Adapter, 32 bit, WOL, Jumbo, Retail	11

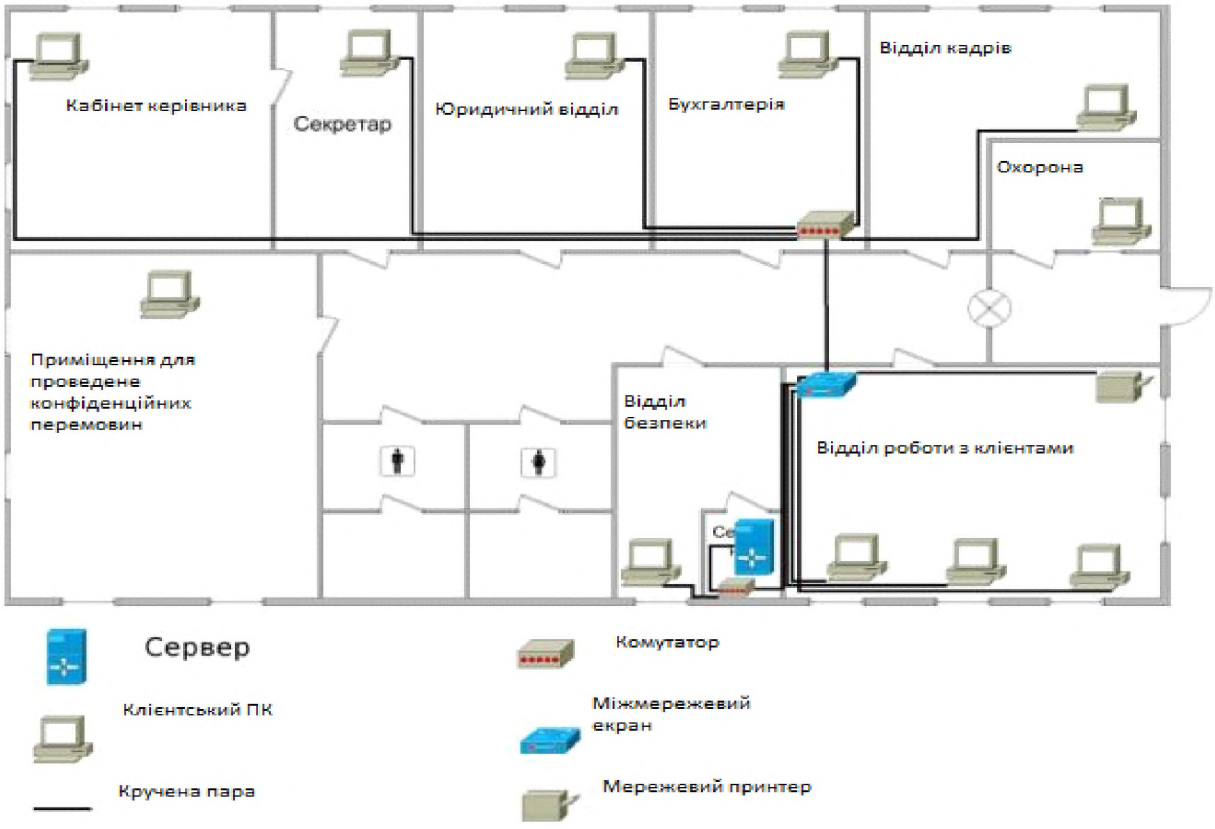

Рисунок2.3 - Схема розміщення обчислювальної техніки

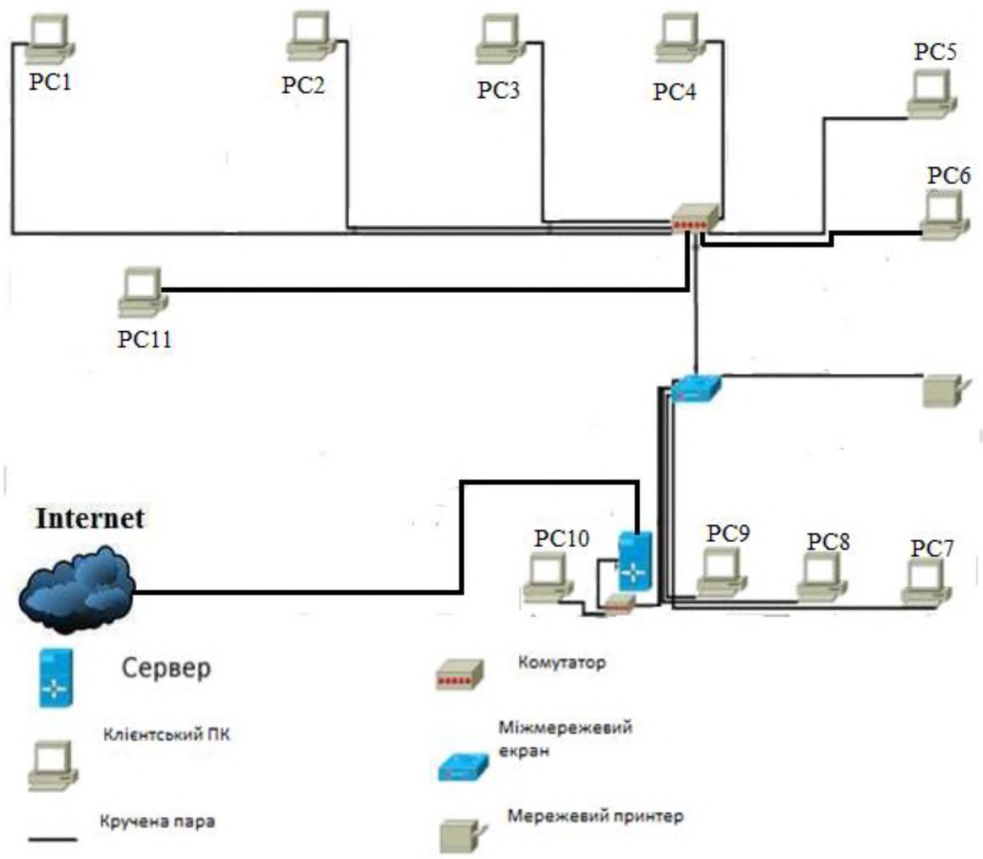

Рисунок 2.4 Схема ІТС "Кредит - Легко"

2.4 Аналіз та оцінка інформаційних ризиків

Аналіз ризиків інформаційної безпеки розроблений на основі документу ДСТУ ISO/IEC 27005:2015 - Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT) з урахуванням особливостей діяльності підприємства.

Визначення інформаційних ресурсів на ТОВ "Кредит - Легко", що потребують захисту

Таблиця 2.4 – Визначення рівня конфіденційності, цілісності та доступності інформації

№	Інформація	Рівень конфіденційності	Рівень цілісності	Рівень доступності
1	Організаційно-розпорядча документація	К3	Ц2	Д3

Продовження таблиці 2.4

№	Інформація	Рівень конфіденційності	Рівень цілісності	Рівень доступності
2	Облік внутрішніх документів(накази, службові записки, інструкції	К4	Ц2	Д2
3	Інформація про надання послуг, тарифи, контактна інформація	К1	Ц2	Д2
4	Інформація про робітників	К3	Ц2	Д2
5	Статутні документи підприємства(документи, що дозволяють займатись підприємницькою діяльністю)	К4	Ц3	Д3
6	Документи обліку та реєстрації	К1	Ц1	Д1
7	Трудові договори робітників	К3	Ц2	Д2
8	Персональні дані клієнтів	К4	Ц4	Д4
9	Концепції розвитку підприємства, стратегічні плани розвитку, функціональні, маркетингові, фінансові та логістичні моделі ведення бізнес	К4	Ц3	Д3
10	Поточні та планові контракти	К2	Ц4	Д3
11	Конфігураційні файли СЗІ, паролі, ЕЦП	К4	Ц4	Д4

Рівні конфіденційності:

К1– принести малозначний збиток в рідкісних випадках.

К2 – Приносить незначний матеріальний збиток в певних випадках;

К3 - Приносить відчутний матеріальний збиток в певних випадках;

К4 – розголошення призводить до значних матеріальних втрат, якщо не буде вжито заходів;

К5 – розголошення інформації призводить до краху роботи суб'єкта або дуже великих матеріальних втрат;

Рівні цілісності:

Ц1– несанкціоновані зміни не відображатимуться на роботі системи.

Ц2 – несанкціоновані зміни не приведуть до збою в роботі суб'єкта,наслідки оборотні;

Ц3 – несанкціоновані зміни призведуть до неправильної роботи суб'єктів через деякий час, якщо не буде вжито заходів, наслідки оборотні;

Ц4 – несанкціоновані зміни призведуть до неправильної роботи суб'єктів через деякий час, якщо не буде вжито заходів, наслідки незворотні;

Ц5 – призводить до неправильної роботи суб'єкта в цілому або значної його частини і наслідки зміни незворотні;

Рівні доступності:

Д1– у разі порушення доступності інформації даного типу підприємство не понесе матеріального збитку, робота підприємства не буде порушена, бажано впровадження, зміни в існуючих технологічних процесах;

Д2 – у разі порушення доступності інформації даного типу підприємство понесе мінімальний збиток матеріального прибутку, робота підприємства не буде порушена, загальний дохід залишиться без зміни;

Д3 – 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 підприємстві;

Д4 – у разі порушення доступності інформації даного типу підприємство понесе збиток матеріального прибутку, робота підприємства буде ускладнена, загальний дохід може знизиться до половини існуючого;

Д5 – 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.

Виконаємо оцінку інформаційних ризиків (див. табл 2.5) за формулою: ALE=ARO*SLE, де ALE– очікуваний річний збиток; ARO – річна частота подій; SLE – очікуваний одиничний збиток та розраховується за формулою: SLE=AV*EF, де; AV – вартість ресурсу; EF – ефект впливу.

AV - ранжується за 5 рівнями:

1 рівень - до 100 грн.;

2 рівень - 100-1000 грн.;

3 рівень - 1000-10000 грн.;

4 рівень - 10000-100000 грн.;

5 рівень - >100000 грн.

EF - ранжується за 5 рівнями:

1 рівень - 0 - 10% об'єкта пошкоджено;

2 рівень - 10 -25% об'єкта пошкоджено;

3 рівень - 25-50% об'єкта пошкоджено;

4 рівень - 50-75% об'єкта пошкоджено;

5 рівень - 75-100% об'єкта пошкоджено.

ARO - ранжується за 5 рівнями:

1 рівень - 0-50 випадків у рік;

2 рівень - 10-30 випадків у рік;

3 рівень - 30-60 випадків у рік;

4 рівень - 60-100 випадків у рік;

5 рівень - >100 випадків у рік.

Рівні ризику:

0-21 -малий рівень ризику

22-43 - припустимий рівень

44-75 - критичний рівень

Таблиця 2.5 Оцінка інформаційних ризиків

Інформація	Загроза	AV	EF	ARO	SLE	ALE
Організаційно-розпорядча документація	Знищення інформації	3	3	3	9	27
	Помилки персоналу	3	3	2	9	18
	Несанкціоноване копіювання інформації	3	2	3	6	18
	Витік інфомації	3	2	3	6	18
Облік внутрішніх документів(накази, службові записки, інструкції	Знищення інформації	2	3	3	6	18
	Помилки персоналу	2	2	2	4	8
	Несанкціоноване копіювання інформації	2	3	3	6	18
	Витік інфомації	2	3	3	6	18
Інформація про надання послуг, тарифи, контактна інформація	Знищення інформації	1	2	2	2	4
	Помилки персоналу	1	2	3	2	6
	Несанкціоноване копіювання інформації	1	2	1	2	2
	Модифікація інфомації	1	1	3	1	3

Продовження таблиці 2.5

Інформація	Загроза	AV	EF	ARO	SLE	ALE
Інформація про робітників	Знищення інформації	2	2	2	4	8
	Помилки персоналу	2	1	1	2	2
	Несанкціоноване копіювання інформації	2	3	2	6	12
	Витік інфомації	2	3	3	6	18
Статутні документи підприємства(документи, що дозволяють займатись підприємницькою діяльністю)	Знищення інформації	4	5	2	20	40
	Помилки персоналу	4	3	2	12	24
	Несанкціоноване копіювання інформації	4	4	3	16	48
	Модифікація інфомації	4	4	2	16	32
Документи обліку та реєстрації	Знищення інформації	2	2	2	4	8
	Помилки персоналу	2	2	2	4	8
	Несанкціоноване копіювання інформації	2	2	2	4	8
	Витік інфомації	2	2	3	4	12

Продовження таблиці 2.5

Інформація	Загроза	AV	EF	ARO	SLE	ALE
Персональні дані клієнтів	Знищення інформації	5	5	3	25	75
	Помилки персоналу	5	3	2	15	30
	Несанкціоноване копіювання інформації	5	4	3	20	60
	Витік інфомації	5	5	2	25	50
Концепції розвитку підприємства, стратегічні плани розвитку, функціональні, маркетингові, фінансові та логістичні моделі ведення бізнес	Знищення інформації	4	3	3	12	36
	Помилки персоналу	4	2	2	8	16
	Несанкціоноване копіювання інформації	4	4	3	12	36
	Витік інфомації	4	4	3	12	36
Поточні та планові контракти	Знищення інформації	4	4	3	16	48
	Помилки персоналу	4	2	2	8	16
	Несанкціоноване копіювання інформації	4	3	3	12	36
	Витік інфомації	4	4	3	16	48

Продовження таблиці 2.5

Інформація	Загроза	AV	EF	ARO	SLE	ALE
Конфігураційні файли СЗІ, паролі, ЕЦП	Знищення інформації	5	4	3	20	60
	Помилки персоналу	5	5	2	25	50
	Несанкціоноване копіювання інформації	5	5	3	25	75
	Витік інфомації	5	5	3	25	75
Трудові договори робітників	Знищення інформації	2	3	2	6	12
	Помилки персоналу	2	2	3	4	12
	Несанкціоноване копіювання інформації	2	3	2	6	12
	Витік інфомації	2	3	3	6	18

Отже найбільші ризики це: знищення та витік персональних даних клієнтів, знищення, несанкціоноване копіювання та витік інформації про конфігураційні файли СЗІ, паролі та ЕЦП.

2.4.1 Модель порушника

Модель порушника інформаційної безпеки [20] - абстрактний опис можливих дій порушника на основі його повноважень, знань, теоретичних і практичних можливостей. Порушників поділяють на внутрішніх (співробітники, користувачі системи) і зовнішніх(сторонні особи або особи, що знаходяться за межами КЗ).

Модель порушника визначає:

- можливу мету порушника та її градацію за ступенями небезпечності для АС;
- категорії осіб, з числа яких може бути порушник;
- припущення про кваліфікацію порушника;
- припущення про характер його дій.

Метою порушника є отримання необхідної інформації, отримання можливості вносити зміни в інформаційні потоки та нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

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 тощо).
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	Корисливий інтерес
М3	Відсутній

Таблиця2.10 – Модель внутрішнього порушника

Посада	Категорія обізнаності	Можливий час дії	Можливе місце дії	Можливий мотив
Генеральний директор	К1	Ч4	Д6	М3
Заступник директора	К1	Ч4	Д6	М2

Продовження таблиці 2.10

Посада	Категорія обізнаності	Можливий час дії	Можливе місце дії	Можливий мотив
Секретар-референт	К1	Ч3	Д4	М1,М2
Головний бухгалтер	К1	Ч3	Д4	М2
Бухгалтер	К1	Ч3	Д4	М1,М2
Керівник кадрового відділу	К1	Ч3	Д4	М2
Кадровик	К1	Ч3	Д4	М1,М2
Керівник клієнтського відділу	К1	Ч3	Д4	М2
Співробітник клієнтського відділу	К1	Ч3	Д4	М1,М2
Керівник юридичного відділу	К1	Ч3	Д4	М2
Юрист	К1	Ч3	Д4	М1,М2
Керівник служби безпеки	К1	Ч3	Д4	М2
Начальник охорони	К1	Ч3	Д4	М2
Співробітник бюро пропусків	К1	Ч3	Д4	М1,М2
Охоронець	К0	Ч3	Д3	М1,М2
Системний адміністратор	К5	Ч4	Д6	М2

Таблиця 2.11 – Модель зовнішнього порушника

Посада	Категорія обізнаності	Можливий час дії	Можливе місце дії	Можливий мотив
Злочинці (хакери)	К3	Ч4	Д1	М2
Представники організацій, що взаємодіють з питань ПЗ	К3	Ч1	Д3	М2
Представники організацій, що взаємодіють з питань технічного забезпечення і обслуговування внутрішньодомових систем	К0, К2	Ч2	Д3	М1, М2

Згідно інформації викладеної в таблиці 2.9 і таблиці 2.10 найбільшу увагу варто приділити системному адміністратору та заступнику генерального директора, так як вони мають високий рівень обізнаності щодо ІТС (системний адміністратор) та мають доступ у зону керування засобами забезпечення безпеки АС, володіють необмеженим доступом до інформації на підприємстві (генеральний директор, заступник генерального директора). Найбільш ймовірним зовнішнім порушником є злочинець(хакер) так як він має високий рівень кваліфікації та для реалізації загрози йому не потрібен прямий доступ до об'єкту.

2.4.2 Модель загроз

Результатом аналізу можливих загроз є модель загроз [20] - абстрактний формалізований опис методів і засобів здійснення загроз із зазначенням рівнів гранично припустимих втрат. Найбільш широко загрози інформаційним ресурсам можна розглядати як потенційно можливі випадки технічного,

антропогенного або стихійного характеру, які можуть спричинити небажаний вплив на інформаційну систему, а також на інформацію що зберігається в ній.

Шкала оцінки загроз:

К1 – визначає ступінь доступності до об'єкта

1 – в іншій країні (для техногенних загроз) / немає доступу до об'єкта (для антропогенних загроз);

2 – в тій самій країні (для техногенних загроз) / віддалений доступ до об'єкта (для антропогенних загроз);

3 – поблизу будівлі, де знаходиться ОІД, або в тій самій будівлі (для техногенних загроз) / фізичний несанкціонований доступ до об'єкта, несанкціоноване проникнення в приміщення (для антропогенних загроз);

4 – в тому ж приміщенні (для техногенних загроз) / доступ у приміщення, де знаходиться об'єкт (для антропогенних загроз);

5– сам об'єкт (для техногенних загроз) / фізичний дозволенний доступ до об'єкта (для антропогенних загроз).

К2 – присутність необхідних умов, ступінь кваліфікації виконавця та ступінь його бажання реалізувати загрозу

1 – виконавець постраждає при реалізації загрози; він не має ніяких відповідних можливостей; техніка та ПЗ постійно оновлюються, встановлюється належним чином та постачається надійним виробником;

2 – виконавець не постраждає через загрозу, але її виконання не є вигідним для виконавця; він має недостатній рівень знань для реалізації загрози; ПЗ та техніка оновлюється не постійно;

3 – виконавцю вигідна реалізація загрози; він може навчитися методам, що реалізують загрози; ПЗ та техніка вразливі для деяких атак;

4 – виконавцю дуже вигідна реалізація загрози; він володіє методами, що реалізують загрози; відсутність оновлень ПЗ або застарілі елементи техніки, ненадійні їх виробники, неякісна техніка;

5 – мета виконавця; виконавець є експертом у методах, що реалізують загрозу

(наприклад, він працює у відповідній сфері); стара або зламана техніка; піратське ПЗ, тощо.

К3 – фатальність наслідків

1 – ОІД нічого не втратить, або наслідки будуть позитивними;

2 – Наслідками можна знехтувати;

3– Наслідки відчутні, але несуттєві;

4– Наслідки можуть призвести до проблем, вирішення яких потребуватиме значну кількість матеріальних витрат та значну кількість часу; 5– Наслідки можуть призвести до втрати репутації компанії, недовіри клієнтів та збитків, що можуть призвести до закриття організації.

К загальне для загроз розраховується за формулою:

$$(К_{оп})_i=(К1*К2*К3)/125$$

Таблиця 2.12 Результати аналізу загроз та вразливостей інформації в ІТС

№	Загрози	Вразливості що приведуть до реалізації	Джерело	К1	К2	К3	$К_{оп}$
1	Здійснення атак на ОС	відсутність або неякісне антивірусне ПЗ	Зовнішнє, внутрішнє	4	3	4	0.38
2	Читання залишкової інформації з оперативної та зовнішньої пам'яті ЕОМ	не реалізованість заборони повторного використання інформації	Внутрішнє	5	3	3	0.36
3	Порушенні цілісності інформації, що зберігається внаслідок апаратного або програмного збою	відсутність резервного обладнання	Внутрішнє	4	3	4	0.38

Продовження таблиці 2.12

№	Загрози	Вразливості що приведуть до реалізації	Джерело	К1	К2	К3	$К_{оп}$
4	Впливи природних завад і стихійні лиха (грозові розряди,блискавка, землетруси, тощо)	Відсутність захисту від стихійного лиха Відсутність резервних каналів електроживлення	Зовнішнє	3	3	4	0.29
5	Зміна умов фізичного середовища(пожежі, аварії)	Наявність легкозаймистих матеріалів Недотримання норм пожежної безпеки персоналом підприємства Використання несправного обладнання в процесі роботи на підприємстві	Зовнішнє, внутрішнє	3	3	4	0.29
6	НСД до даних з порушенням встановлених правил розмежування внаслідок використання порушником відомих вразливостей системного та прикладного ПЗ	Недосконале ПЗ Помилки при розмежуванні доступу до системи	Зовнішнє внутрішнє	4	3	4	0.38
7	Порушення конфіденційності та цілісності інформації внаслідок навмисних дій авторизованого користувача	Відсутність резервних копій Неправильний підбір персоналу Неефективне розмежування доступу до системи	Внутрішнє	4	4	3	0.38

Продовження таблиці 2.12

№	Загрози	Вразливості що приведуть до реалізації	Джерело	К 1	К 2	К 3	$К_{оп}$
8	Розповсюдження і використання компютерних вірусів для порушення безпеки даних	відсутність або неефективність антивірусного ПЗ	Зовнішнє, Внутрішнє	5	3	4	0.48
9	Одержання та використання атрибутів доступу системи іншим користувачем ІТС для розширення своїх повноважень або маскування під іншого зареєстрованого	відсутність/неефективність ідентифікації та автентифікації користувача	Внутрішнє	5	4	3	0.48
10	Неправомірне впровадження і забороненого політикою безпеки ПЗ	недбалість персоналу	Внутрішнє	5	3	3	0.36
11	Несанкціонований доступ до інформації через Wi-Fi	нерегулярна зміна паролів на Wi-Fi	Зовнішнє	4	3	4	0.4
12	Ненавмисне пошкодження інформації або її носіїв	- недосвідченість персоналу	Внутрішнє	5	2	3	0.24
13	Соціальна інженерія(шантаж, підкуп тощо)	- неправильний підбір персоналу	Внутрішнє	4	3	4	0.4
14	Проникнення в приміщення	неефективна система охорони; - неякісний контроль за приміщенням	Зовнішнє	3	1	4	0.1

Продовження таблиці 2.12

№	Загрози	Вразливості що приведуть до реалізації	Джерело	К1	К2	К3	$К_{оп}$
15	Несанкціоноване копіювання інформації	- відсутність журналу подій.	Внутрішнє	2	3	4	0.2
16	Одержання та використання атрибутів доступу системи сторонніми особами, внаслідок необережного поводження користувачів	- передавання паролів у відкритому вигляді. - недосвідченість персоналу	Зовнішнє	5	3	4	0.48
17	Випадкове зараження програмних засобів комп'ютерними вірусами	- недосвідченість персоналу; - відсутність або неякісне антивірусне ПЗ.	Внутрішнє	5	2	3	0.24
18	Несанкціонований перехват інформації на паперових або електронних носіях	неналежне зберігання документів та пристроїв з інформацією	Внутрішнє	5	3	4	0.48

Згідно даних викладених в таблиці 2.11 найбільший рівень критичності (0.48) мають наступні загрози: розповсюдження і використання комп'ютерних вірусів для порушення безпеки даних, одержання та використання атрибутів доступу системи іншим користувачем ІТС для розширення своїх повноважень або маскування під іншого зареєстрованого, одержання та використання атрибутів доступу системи сторонніми особами, внаслідок необережного поводження користувачів та одержання, використання атрибутів доступу системи сторонніми особами, внаслідок необережного поводження користувачів та несанкціонований перехват інформації на паперових або електронних носіях. Тому що організація є

найбільш вразливою до цих загроз і їх реалізація може привести до серйозних негативних наслідків.

2.4.3 Профіль захищеності системи.

За результатами попереднього аналізу ризикв та загроз в ІТС організації, був обраний профіль захищеності системи ЗКЦД1 ={ 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 }

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 на об’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.

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 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 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 тощо), 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 не задекларованих функцій), іншими непередбачуваними ситуаціями.

Політикою відновлення після збоїв повинна бути визначена й задокументована множина типів відмов і переривань обслуговування обчислювальної системи 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.0

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

Виходячи з того, що на ТОВ "Кредит - Легко" є ІзОД, 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. Необхідно ввести заходи для зниження ризиків загроз, що мають рівень критичності 0,48. До цієї категорії відносяться: розповсюдження і використання комп'ютерних вірусів для порушення безпеки даних,одержання та використання атрибутів доступу системи іншим користувачем ІТС для розширення своїх повноважень або маскування під іншого зареєстрованого, одержання та використання атрибутів доступу системи сторонніми особами, внаслідок необережного поводження користувачів, та несанкціонований перехват інформації на паперових або електронних носіях. Необхідно зосередитися на організаційних методах захисту. Для цього розробляються наступні політики безпеки інформації:

- політика антивірусного захисту, націлена на зниження ризику зараження комп'ютерними вірусами;
- політика "чистого столу", націлена на зниження ризику від несанкціонованого перехвату інформації на паперових та електронних носіях;
- політика моніторингу та контролю мережі Інтернет користувачами системи та політика електронної пошти, націлені зниження ризику від випадкового зараження компютерними вірусами користувачами системи;
- політика резервного копіювання даних націлена збереження цілісності конфіденційної інформації;
- політика утилізації технологічного оладнання націлена на зниження ризику перехвату інформації на електронних носіях.

Політика антивірусного захисту

Метою політики є встановити вимоги, яким повинні відповідати всі комп'ютери. підключені до мережі ТОВ "Кредит - Легко", щоб забезпечити ефективне виявлення та запобігання вірусам.

Ця політика поширюється на всі персональні комп'ютери або комп'ютери, що використовують спільний доступ до ПК-файлів. Наприклад: настільні

(стаціонарні комп'ютери), портативні комп'ютери (ноутбуки), файлові/ftp/tftp/проксі-сервери та будь-яке обладнання на базі ПК(генератори трафіку).

Інструкція політики:

Усі комп'ютери на базі ПК організації повинні мати встановлене стандартне підтримуване антивірусне програмне забезпечення, встановлене і заплановане працювати через рівні проміжки часу. Крім того, антивірусне програмне забезпечення та файли зразків вірусів повинні постійно оновлюватися. Комп'ютери заражені вірусом повинні бут видалені з мережі, поки вони не будуть підтвердженні як захищені від вірусів Адміністратори/менеджери відповідають за створення процедур, які забезпечують запуск антивірусного програмного забезпечення через регулярні проміжки часу, а комп'ютери підтверджуються як захищені від вірусів. Будь які

дії з метою створення та/або розповсюдження шкідливих програм у мережах організації(віруси, хробаки, троянські коні, поштові бомби тощо) заборонені.

Рекомендовані процеси для запобігання проблемам з вірусами:

- Ніколи не відкривайте файли чи макроси, приєднані до електронного листа з невідомого, підозрілого чи недостовірного джерела. Видаліть ці файл негайно, а потім "подвійно видаліть", очистивши Кошик.
- Видаліть спам та інші непотрібні електронні листи без переадресації, відповідно до політики допустимого використання.
- Ніколи не завантажуйте файли з невідомих або підозрілих джерел.
- Уникайте прямого обміну дисками з доступом до читання/запису, якщо для цього не існує абсолютно ділових вимог.
- Завжди скануйте дискету з невідомого джерела на наявність вірусів перед її використанням.
- Регулярно створюйте резервні копії критичних даних та конфігурацій системи та зберігайте їх у безпечному місці.

Відповідальність

Працівник, який порушив цю політику, може зазнати дисциплінарного стягнення аж до припинення роботи, звільнення

Будь-який виняток із політики повинен бути затверджений.

Політика "чистого столу"

Політика чистого столу повинна гарантувати, що всі конфіденційні матеріали вилучаються з робочої області кінцевого користувача та блокуються, коли предмети не використовуються або працівник покидає своє робоче місце.

Метою політики є встановлення мінімальних вимог щодо підтримки "чистого столу" - де конфіденційна/критична інформація про співробітників, інтелектуальну власність, клієнтів та постачальників захищена. Ця політика поширюється на всіх працівників організації.

Інструкція політики:

1. Співробітники зобов'язані гарантувати, що вся конфіденційна/критична інформація (на паперовому носії) або в електронній формі буде захищена на робочому місці в кінці робочого дня, і коли вони будуть відсутні тривалий час.

2. Робочі станції комп'ютера повинні бути заблоковані, коли робоче місце незайняте.

3. Робочі станції комп'ютера повинні бути повністю вимкнені наприкінці робочого дня.

4. Будь-яку конфіденційну або критичну інформацію необхідно прибрати з письмового столу та закрити у ящику, коли стіл незайнятий та наприкінці робочого дня.

5. Картотеки, що містять конфіденційну та критичну інформацію повинні зберігатись закритими, коли вони не використовуються.

6. Ключі що використовуються для доступу до конфіденційної або критичної інформації не повинні залишатися без нагляду.

7.Ноутбуки повинні бути заблоковані замикаючим кабелем або закриті у ящику.

8. Паролі не мають залишатися на наклеєних нотатках, розміщених на комп'ютері або під ним, а також не можуть бути записані у доступному місці.

9. Роздруківки, що містять конфіденційну або критичну інформацію, слід негайно видалити з принтера.

10.Після утилізації конфіденційні або критичні документи повинні бути подрібнені та поміщенні в конфіденційні контейнери для сміття.

11. Конфіденційну або критичну інформацію, що написана на дошці повинна бути стерта.

12.Портативні обчислювальні пристрої(ноутбуки, планшети) повинні бути заблоковані.

13. Зберігати пристрої масового зберігання даних(CDROM, DVD, USB накопичувачі) у замкненому ящику.

14. Усі принтери та факси повинні бути очищені від паперів після друкування, це допомагає гарантувати, що конфіденційні документи не залишаться в лотках принтерів.

Відповідальність

Працівник, який порушив цю політику, може зазнати дисциплінарного стягнення аж до відлучення від роботи, звільнення

Політика моніторингу та контролю мережі Інтернет
користувачами системи

Метою цієї політики є визначення стандартів для систем, які обстежують та обмежують користування Інтернету від будь-якого хоста в мережі організації. Ця політика розроблена для того, щоб співробітники користувались Інтернетом безпечно та відповідально, а також гарантувати що веб службовці будуть контролюватися під час інциденту.

Сфера застосування.

Ця політика поширюється на всіх службовців організації, підрядників та агентів з компютером або робочою станцією, що належить організації, або особистою власністю підключеною до мереж іорганізації.

Ця політика стосується усіх кінцевих користувачів комунікацій між мережею організації та Інтернетом, включаючи веб-перегляд, миттєві повідомлення, передачу та обмін файлами, тощо.

Інструкція політики

Системний адміністратор повинен контролювати використання Інтернету з усіх компютерів та пристроїв підключених до корпоративні мережі. Для всього трафіку система повинна записувати вихідну IP-адресу, дату, час, протокол та місце призначення або сервер. Там де це можливо система повинна записувати ідентифікатор користувача(особи або облікового запису, що ініціює трафік). Записи про використання Інтернету повинні зберігатися протягом 180 днів. Доступ до веб-сайтів та протоколів Інтернету, яків важаються невідповідними для корпоративного середовища організації мають бути заблоковані.

Відповідальність

Працівник, який порушив цю політику, може зазнати дисциплінарного стягнення аж до відлучення від роботи, звільнення

Політика резервного копіювання

Метою політики є встановлення порядку резервного копіювання для наступного відновлення працездатності АС при повній або частковій втраті інформації, викликаної збоями чи відказами апаратного або програмного забезпечення, помилками користувачів, надзвичайними обставинами(пожежі, стихійні лиха, тощо). Встановлення порядку відновлення інформації у разі необхідності. Забезпечення міри захисту від помилок людини або ненавмисного видалення файлів.

Сфера застосування

Ця політика поширюється на всіх службовців, підрядників та сторонніх працівників, які мають доступ до IT-активів організації та можуть бути зв'язані договірними умовами. Ця політика поширюється на всю IT-інфраструктуру організації

Інструкція політики.

Для інформації рівня користувача та рівня системи, що обробляється організацією, періодично повинна створюватися резервна копія. Носії резервного копіювання повинні зберігатися з достатнім захистом та належними умовами навколишнього середовища. Частота та ступінь резервного копіювання повинні

відповідати важливості інформації та прийнятому ризику, визначеному власником даних. Процес резервного копіювання та відновлення інформаційних ресурсів повинен бути задокументований та періодично переглядатися. Будь які системи, що надають резервне копіювання за межами сайтів, повинні бути очищенні від обробки найвищого рівня (конфіденційності) інформації що зберігається. Фізичні засоби управління доступом у місцях зберігання резервних копій, повинні відповідати або перевищувати фізичні засоби контролю вхідних систем. Крім того, носії резервного копіювання повинні бути захищені відповідно до найвищого рівня конфіденційності інформації, що зберігається. Необхідно здійснити процес підтвердження успішності резервного копіювання електронної інформації. Резервні копії операційних систем та іншого інформаційно важливого ПЗ не повинні зберігатися в тому самому місці. що і операційне програмне забезпечення. Інформація про резервну копію системи повинна забезпечуватися захистом від несанкціонованих змін та умов навколишнього середовища. Резервні копії повинні періодично перевірятися, щоб переконатися, що вони підлягають відновленню. Для підтвердження надійності носія та цілісності інформації, резервна інформація повинна перевірятися з певною частотою. Резервні копії даних повинні мати наступні критерії і , які можна легко ідентифікувати за мітками та/або системою штрихового кодування:

- назва системи;
- дата створення;
- класифікація;
- контактна інформація

Відповідальність

Працівник, який порушив цю політику, може зазнати дисциплінарного стягнення аж до відлучення від роботи, звільнення.

Політика електронної пошти

Метою цієї політики є забезпечення належного використання системи електронної пошти організації та інформування користувачів про те, що організація вважає прийнятим та неприйнятим для використання її системою

електронної пошти. Ця політика визначає мінімальні вимоги щодо використання електронної пошти в мережі організації.

Сфера застосування

Ця політика охоплює належне використання будь-якого електронного листа, надісланого з електронної адреси організації та стосується всіх співробітників, продавців та агентів, що працюють від імені організації.

Інструкція політики .

Будь-яке використання електронної пошти повинно відповідати політиці організації та процедурам етичної поведінки, безпеки, дотримання чинного законодавства та належної ділової практики. Адресу електронної пошти організації слід використовувати насамперед для цілей організації, пов'язаних з бізнесом. Особисте спілкування дозволено обмежено, але комерційне використання, яке не стосується організації заборонено. Усі дані організації, що містяться в електронному повідомленні або вкладеному файлі, повинні бути захищені відповідно до стандарту захисту даних. Електронну пошту слід зберігати лише в тому випадку, якщо вона визначається як діловий запис організації. Система електронної пошти організації не повинна використовуватися для створення або розповсюдження руйнівних або образливих повідомлень. Співробітники, які отримують такі повідомлення від будь-якого співробітника організації повинні негайно повідомити про це своєму керівнику. Користувачам забороняється автоматично пересилати електронну пошту організації сторонній системі електронної пошти. Окремі повідомлення, які пересилаються користувачем не повинні містити конфіденційну інформацію організації. Користувачам забороняється користуватися сторонніми системами електронної пошти та серверами зберігання даних, такими як Google, Yahoo тощо, для ведення бізнесу організації, створення або запам'ятовування будь-яких зобов'язальних операцій, а також зберігання електронної пошти від імені організації. Такі комунікації та транзакції повинні проводитись через належні канали, використовуючи підтверджену документацію організації. Працівники не повинні сподіватися на конфіденційність будь-чого, що вони зберігають,

надсилають або отримують у системі електронної пошти організації. Організація може контролювати повідомлення без попереднього попередження. Організація не забов'язана контролювати електронні повідомлення.

Відповідальність

Працівник, який порушив цю політику, може зазнати дисциплінарного стягнення аж до відлучення від роботи, звільнення.

Політика утилізації технологічного обладнання

Технологічне обладнання, таке як жорсткі диски, USB- накопичувачі, компакт-диски та інші носії інформації містять різні дані організації, деякі з яких є конфіденційними. Щоб захистити дані, перед утилізацією усі засоби зберігання мають бути очищеними. Однак просто видалення або навіть форматування даних не вважається достатнім. Під час видалення файлів або форматування пристрою дані позначаються для видалення, але вони все ще доступні , поки їх не замінить новий файл. Тому для надійного стирання даних перед утилізацією обладнання необхідно використовувати спеціальні інструменти. Метою політики є визначення вказівок щодо утилізації технологічного обладнання та компонентів, що належать компанії.

Ця політика поширюється на будь-яке комп'ютерне/технологічне обладнання або периферійні пристрої, які більше не потрібні організації, включаючи: персональні комп'ютери, сервери, жорсткі диски, портативні комп'ютери, принтери, сканери, портативні пристрої зберігання даних тощо. Всі співробітники організації мають дотримуватися цієї політики.

Інструкція політики

Коли закінчується термін експлуатації технологічного обладнання, його слід направити в офіс команди з вивезення обладнання, яка надійно утилізує всі носії інформації відповідно до сучасних найкращих практик галузі. Усі дані, включаючи всі файли та ліцензійне ПЗ, повинні бути вилучені з обладнання, використовуючи ПЗ, що очищає носій, переписуючи кожен сектор диска машини нульовими блоками. Жодне обладнання не може бути продане будь-якій особі. Всі електронні диски мають бути розмагнічені або перезаписані програмою

очищення диска. Жорсткі диски також можуть бути вилучені і зроблені нечитабельними (буріння, дроблення чи інші способи знесення). У технологічного обладнання зберігання буде видалена пам'ять або пристрій зберігання і фізично знищений. Перед виїздом із приміщення організації все обладнання повинно бути вилучено із системи інвентарізації інформаційних технологій.

Відповідальність

Працівник, який порушив цю політику, може зазнати дисциплінарного стягнення аж до відлучення від, звільнення.

Висновки до розділу 2

У другому розділі було виконано обстеження ОІД, а саме:

- 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 моніторингу та контролю мережі Інтернет користувачами системи;
- політика "чистого столу";
- політика антивірусного захисту;
- політика розмежування даних;
- політика електронної пошти;
- політика утилізації технологічного обладнання.

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.

Капітальні витрати

Запропонована політика безпеки передбачає необхідність витрат на реалізацію. До заходів, що потребують витрат відноситься:

- політика моніторингу та контролю мережі Інтернет користувачами системи;
- політика "чистого столу";
- політика антивірусного захисту;
- політика розмежування даних;
- політика електронної пошти;
- політика утилізації технологічного обладнання.

3.2 Визначення трудомісткості розробки політики безпеки інформації

Розрахунок витрат на розробку політику безпеки підприємства.

Тривалість створення політики безпеки визначається за формулою:

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

де $t_{тз}$ – тривалість складання технічного завдання на розробку політики безпеки інформації, становить 7 год.;

$t_{в}$– тривалість розробки концепції безпеки інформації у організації, становить 8 год.;

$t_{а}$– тривалість процесу аналізу ризиків, становить 5 год.;

$t_{вз}$ – тривалість визначення вимог до заходів, методів та засобів захисту становить 4 год.;

$t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації становить 6 год.;

$t_{овр}$ – тривалість організації виконання відновлювальних робі і забезпечення неперервного функціонування організації становить 7 год.;

$t_{д}$ – тривалість документального оформлення політики безпеки становить 4 год.

t=7 год+8 год+5 год+4год+6год+7год+4год=41 год (3.1)

Розрахунок витрат на створення політики безпеки інформації

Витрати на розробку політики безпеки інформації $К_{рп}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації $З_{мч}$ за формулою 3.2:

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

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 3.3:

$$Ззп = t \cdot Зіб, \text{ грн} \qquad (3.3)$$

де t – загальна тривалість розробки політики безпеки, годин;

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

$$З_{ЗП} = 41 \cdot 105 = 4305 \text{ грн.}$$

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою 3.4:

$$З_{мч} = t \cdot С_{мч}, \text{ грн,} \qquad (3.4)$$

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

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

Вартість 1 години машинного часу ПК визначається за формулою 3.5:

$$С_{мч} = Р \cdot t_{нал} \cdot С_{е} + (Ф_{зал} \cdot Н_{а}/F_{р}) + (К_{лпз} \cdot Н_{а}/F_{р}), \text{ грн} \qquad (3.5)$$

де Р – встановлена потужність ПК, кВт;

$t_{нал}$ - кількість задіяних робочих станцій при написані політики безпеки

C_e – тариф на електричну енергію, грн/кВт·година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$– річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_р$ = 1920).

Оскільки на даному підприємстві встановлена потужність $P=0,4$, а тариф на електричну енергію становить 1.91 грн/кВт·година то:

$$С_{мч}= 0.4·1.91·11+(10400·0.5/1920)+(5141·0.5/1920)=12.44 \text{ грн}$$

$$З_{мч}= t·С_{мч} = 41·12.44=510.04 \text{грн}$$

3.3 Розрахунок капітальних (фінансових) витрат

Капітальні витрати розраховуються наступним чином:

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

де $К_{пр}$ - вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів тис. грн. Стороння організація не наймалась, тому даний коефіцієнт не враховується при розрахунках;

$К_{зпз}$ - вартість закупівель ліцензійного основного й додаткового ПЗ, складає 56551 грн;

Таблиця 3.1 Перелік придбаного ліцензованого ПЗ.

Назва	Кількість	Вартість(грн.)
Windows 10	11	28512
Malwarebytes	11	13431
DeviceLock	11	14608
Всього		56551

$К_{рп}$ - вартість розробки політики інформаційної безпеки складає 4815.86 грн.;

$К_{аз}$ - вартість закупівлі апаратного забезпечення та допоміжних матеріалів;

$К_{навч}$ - витрати на навчання технічних фахівців і обслуговуючого персоналу, тис грн. Витртати на навчання системного адміністратора становлять 1600 грн.

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

Оскільки підприємство не закуповую апаратне забезпечення, для забезпечення інформаційної безпеки $К_{аз}$ та $К_{н}$ не враховуються.

$$К_{зпз}=5141 \cdot 11=56551 \text{ грн.}$$

$$К_{рп}=З_{зп}+З_{мч}=4305+510.04=4815.04 \text{ грн.}$$

$$К=56551+4815.04+1600=62966 \text{ грн.}$$

3.4 Розрахунок поточних(експлуатаційних) витрат

Річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в}+С_{к}+С_{ак}, \text{ тис. грн} \qquad (3.7)$$

де $С_{в}$ - це витрати на оновлення системи;

$С_{ак}$ - це витрати викликані активністю користувачів системи, що складають 110 грн. - пряма допомога, 120грн - неформальне навчання, 140 грн. - розробка додатків, 150 грн - робота з даними, 180 грн - формальне навчання, 300 грн - futz-фактор. Всього 1000 грн.

$С_{к}$ -це витрати на керування інформаційною безпекою, розрахунок відбувається за наступною формулою 3.8:

$$С_{к}=С_{н}+С_{а}+С_{з}+С_{єв}+С_{ел}+С_{о}+С_{тос} \qquad (3.8)$$

де $С_{н}$ - це витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації, що становить 2000 грн;

$С_{а}$ - це річний фонд амортизаційних відрахувань, що визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ). На підприємстві експлуатується 11 комп'ютерів, загальною вартістю 148000 грн. Вартість ПЗ для 11 комп'ютерів 56551 грн.

Загалом - 204551 грн. Мінімальний термін амортизації 2 роки. Ліквідаційна вартість 11 комп'ютерів - 5500грн., ліквідаційна вартість програмного забезпечення для 11 комп'ютерів - 1100грн.

$$С_а=(204551-6600)/2=98975 \text{ грн.}$$

$С_з$ - це річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки, складає:

$$С_з=З_{осн}+З_{дод}, \text{ грн.} \qquad (3.9)$$

де $З_{осн}$ - основна заробітна плата, складає 10000 грн. на місяць, відповідно 120000 грн на рік;

$З_{дод}$ - додаткова заробітна плата, складає 1000 грн на місяць, відповідно 12000 грн. на рік. В 2020 році розмір ЄСВ складає 22% від фонду заробітної плати і становить

$$С_{єв}=132000 \cdot 22\%=29040 \text{ грн.}$$

$$С_з= 120000+12000+29040=161040, \text{ грн.}$$

$С_{ел}$ - це вартість електроенергії, що споживається апаратурою системи інформаційної безпеки протягом року:

$$С_{ел}=Р \cdot F_р \cdot Ц_е, \text{ грн.} \qquad (3.10)$$

де Р - встановлена потужність апаратури інформаційної безпеки 0.4 ВТ для одного ПК, для всього комплексу враховується повна кількість ПК яка складає 11, тобто 4.4 кВт;

$F_р$ - річний фонд робочого часу системи інформаційної безпеки складає 12 місяців*20 робочих діб/міс*8 робочих годин*11 комп'ютерів = 22.176;

$Ц_е$ - тариф на електроенергію, 1.91 грн/кВт годин.

$$С_{ел}=4.4 \cdot 22176 \cdot 1.91=186367 \text{ грн.}$$

$С_о$ - це витрати на залучення сторонніх організацій для виконання деяких видів обслуговування та сертифікацію обслуговування персоналу (залучення сторонніх організацій не відбувається).

$С_{тос}$ - це витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються за даними організації або у відсотках від

вартості капітальних витрат, що складає 1% від суми капітальних інвестицій у вигляді 630 грн.

$$С_к= 2000+98975+161040+186367+630=449012 \text{ грн.}$$

Маючи всі необхідні дані можемо розрахувати річні експлуатаційні витрати:

$$С=449012+1000=450012 \text{ грн.}$$

Оцінка величини збиту

Таблиця 3.2 – Заробітна плата робітників за місяць

Посада	Розмір заробітної плати, грн.
Ген директор	28000
Заступник директора	25000
Секретар-референт	6800
Головний бухгалтер	13000
Бухгалтер	7500
Керівник кадровогу відділу	12500
Співробітник кадрового відділу	6200
Керівник клієнтського відділу	12500
Співробітник клієнтського відділу	7500
Керівник юридичного відділу	12500
Юрист	7500
Керівник служби безпеки	12500
Системний адміністратор	11000
Начальник охорони	12000
Співробітник бюро пропусків	6200
Охоронець	6800
Всього	187500

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

Упущена вигода від простою атакованого вузла або сегмента становить:

$$U = П_п + П_в + V \qquad (3.11)$$

де $П_п$ - оплачувані витрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн.;

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

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

Місячний фонд робочого часу складає 176 годин. Час простою внаслідок атаки 6 годин:

$$П_{п=(}(З_с/F) \cdot t_a, \text{ грн.} \qquad (3.12)$$

де $З_с$ - загальна кількість витрат на заробітну плату співробітників за місяць, F - місячний фонд робочого часу, t_a - час простою внаслідок атак.

Отже:

$$П_п=(187500/176) \cdot 6=6392 \text{ грн.},$$

Витрати на відновлення працездатності($П_в$) включають декілька 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:

$$П_{ви}=(З_с/F) \cdot t_{ви} \text{ грн}_{.,} \qquad (3.13)$$

де $З_с$ - загальна кількість витрат на заробітну плату співробітників за місяць; F - місячний фонд робочого часу; $t_{ви}$ - час повторного введення загубленої інформації співробітниками унаслідок атаки.

$$П_{ви}=(187500/176) \cdot 9=9588 \text{ грн.}$$

Витрати на відновлення $П_{пв}$ визначаються:

$$П_{пв}=(З_о/F) \cdot t_в \text{ грн.}, \qquad (3.14)$$

де $З_о$ - заробітна плата системного адміністратора; F - місячний фонд робочого часу; $t_в$ - час відновлення після атаки персоналом , що обслуговує корпоративну мережу.

$П_{пв}$=(11000/176) ·8=500 грн.

$П_{зч}$ - вартість витрат на заміну устаткування або запасних частин складає 1800грн.

$$П_в = П_{ви} + П_{пв} + П_{зч} \text{ грн.} \qquad (3.15)$$

$$П_в = 9588+500+1800=11888 \text{ грн.}$$

Витрати від зниження працездатності атакованої системи:

$$V=(O/F_г)(t_п+t_в+t_{ви}) , \qquad (3.16)$$

де О - обсяг продажів атакованого вузла або сегмента корпоративної мережі, 6000000 грн за рік;

$F_г$ - річний фонд часу роботи організації становить 2080 год.;

$t_п$ - 6 годин простою внаслідок атак;

$t_в$ - 8 годин відновлення після атаки;

$t_{ви}$ - 9 годин повторного введення загубленої інформації.

V=(6000000/2080) · 23=66346 грн.

Маючи всі потрібні дані, можна розрахувати упущену вигоду від атаки на ІТС організації:

$$U= 6392+500+66346=73238 \text{ грн.}$$

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

$$B=\sum_i\sum_n U \qquad (3.17)$$

$$B= 4\cdot11\cdot73238=3222479 \text{ грн.}$$

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

$$E=B\cdot R-C. \qquad (3.18)$$

де В - загальний збиток від атаки на вузол або сегмент корпоративної мережі, складає 3222479 грн.;

R - очікувана імовірність атаки на вузол або сегмент корпоративної мережі, становить 0.25(якщо реалізація загроз найймовірніша 1 раз на 3 місяці, тобто 4 рази на рік);

С - щорічні витрати на експлуатацію системи інформаційної безпеки, складає 450012 грн.

$$E=(3222479\cdot0.25)-450012=355608.$$

3.5 Аналіз показників економічної ефективності

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки. Щодо інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на вузол або сегмент корпоративної мережі., а отже:

$$ROSI= E/K, \qquad (3.19)$$

де Е - це загальний ефект від впровадження системи інформаційної безпеки, якай становить 355608 грн.;

К - це капітальні затрати, які становлять 62966.

$$ROSI= 355608/62966=5.64$$

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

$$T_o=K/E=1/ ROSI, \text{ років.} \qquad (3.20)$$

$$T_o = 1/5.64= 0.17 \text{ року(2 місяці)}$$

Висновок до розділу 3

Під час виконання економічної частини був проведений розрахунок та проаналізована доцільність впровадження політики безпеки інформації. Визначено економічну ефективність використання основних результатів. Капітальні витрати на впровадження інформаційної політики безпеки становлять 62966 грн., експлуатаційні витрати складають 450012 грн., а загальний збиток від атаки 3222479., ефект від впровадження системи інформаційної безпеки становить 355608 грн. Термін окупності капітальних інвестицій складає

приблизно два місяці. Отримані дані говорять про те що впровадження створених елементів політик безпеки інформації є доцільними.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було:

- проаналізовано темпи росту кіберзлочинності в світі та Україні, зокрема наведена статистика порушень інформаційної безпеки у фінансовому секторі і розглянуті проблеми захисту інформації для об'єктів, що займаються фінансовою діяльністю;

- проаналізовано нормативно правову базу у сфері захисту інформації;

- виконано обстеження об'єкта інформаційної діяльності;

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

- побудовано модель загроз та порушника в ІТС, за результатами яких було обрано профіль захищеності з урахуванням найбільш актуальних загроз, виконано аналіз інформаційних ризиків та для запобігання їх реалізації розроблені політики безпеки інформації, що стосуються організації відповідних методів захисту;

- був проведений розрахунок та проаналізована доцільність впровадження політики безпеки інформації.

Отримані дані говорять про те, що впровадження створених елементів політик безпеки інформації є доцільними.

На вимогу керівника підприємства з метою збереження конфіденційності деяка інформація про ІТС підприємства була змінена. Внесені зміни в цілому не впливають на результати розробки.

Перелік посилань:

1. Purplesec.us. Електронний ресурс. -2019.- Режим доступу: https://purplesec.us/resources/cyber-security-statistics/?utm_source=newsletter&utm_medium=email&utm_campaign=did_you_know_98_of_cyber_attacks_rely_on_social_engineering_learn_how_to_protect_yourself&utm_term=2020-06-01;

2. Сайт OpenDataBot. Електронний ресурс. -2018.- Режим доступу: https://opendatabot.ua/blog/374-hackers;

3. Доктрина інформаційної безпеки України Електронний ресурс. -2014.- Режим доступу: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&cat_id=61025;

4. Закон України "Про інформацію" Електорнний ресурс.-1992.- Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12;

5. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" Електронний ресурс.-1994.- Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80;

6. Закон України "Про захист персональних даних" Електронний ресурс.-2010.- Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17;

7. Постанова Кабінету міністрів України " Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах." Від 29.03.2006. №373 поточна редакція від 13.10.2011 Електронний ресурс. -2006.- https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF;

8.НД ТЗІ 1.1-002-99 Електронний ресурс. -1999-. Режим доступу: https://tzi.com.ua/downloads/1.1-002-99.pdf;

9.НД ТЗІ 1.1-005-07 Електронний ресурс. -2007-. Режим доступу: https://tzi.com.ua/downloads/1.1-005-07.pdf;

10. НД ТЗІ 1.4-001-2000 Електронний ресурс. -2000-. Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=102122&showHidden=0;

11.НД ТЗІ 1.6-005-2013 Електронний ресурс. -2013-. Режим доступу: https://tzi.com.ua/downloads/1.6-005-2013.pdf;

12. НД ТЗІ 3.1-001-07 Електронний ресурс. -2007-. Режим доступу: https://tzi.com.ua/downloads/3.1-001-07.pdf;

13. НД ТЗІ 3.3-001-07 Електронний ресурс. -2007-. Режим доступу: https://tzi.com.ua/downloads/3.3-001-07.pdf;

14. НД ТЗІ 3.6-001-2000 Електронний ресурс. -2000.- Режим доступу: https://tzi.com.ua/downloads/3.6-001-2000.pdf;

15. НД ТЗІ 3.7-001-99 Електронний ресурс. -1999.- Режим доступу: https://tzi.com.ua/downloads/3.7-001-99.pdf;

16. НД ТЗІ 3.7-003-2005 Електронний ресурс. -2005.- Режим доступу: https://tzi.com.ua/downloads/3.7-003-2005.pdf;

17. ДСТУ 3396.1-96 Електронний ресурс. -1996.- Режим доступу: https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf;

18. ДСТУ ISO/IEC 27001:2015 Електронний ресурс. -2015.- Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66910;

19. ДСТУ ISO/IEC 27002:2015 Електронний ресурс. -2015.- Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66911;

20. НД ТЗІ 1.1-003-99 Електронний ресурс. -1999.- Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102106&cat_id=46556&ctime=1344502446343

21. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядн.: Д. П. Пілова - Дніпро: Національний технічний університет "Дніпровська політехніка", 2019;

22. Методичні рекомедації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека / Упорядн.: О. В. Герасіна, Д. С. Тимофєєв, О. В. Кручинін, Ю. А. Мілінчук - Дніпро, НТУ "ДП", 2020;

23. Державний стандарт України. ДСТУ 3008-2015 «Інформація та документація. Звіти у сфері науки і техніки. Структура та правила

оформлювання») / [На заміну ДСТУ 3008-95; чинний від 2017-07-01].- Київ: ДП «УкрНДНЦ», 2016. 31 с. URL: http://www.knmu.kharkov.ua /attachments/3659_3008-2015.PDF;

24. Державний стандарт України. ДСТУ 8302:2015 "Інформація та документація. Бібліографічне посилання. Загальні вимоги та правила складання" URL: http://lib.npu.edu.ua/files/dstu-8302-2015.pdf (дата звернення 10. 04. 2017).

25. Стандарти з інформації, бібліотечної і видавничої справи. URL: http://wwvv.library.univ.kiev.ua/ukr/about/dstu.html (дата звернення 3. 04. 2017).

26. ДСТУ ISO 5807:2016 Обробляння інформації. Символи та угоди щодо документації стосовно даних, програм та системних блок-схем, схем мережевих програм та схем системних ресурсів (ISO 5807:1985, IDT);

27. Положення про систему запобігання та виявлення плагіату в Національному технічному університеті «Дніпровська політехніка», затвердженого Вченою радою 13.06.2018, протокол №8.

ДОДАТОК А Перелік матеріалів на електронному носіїв

1. Кваліфікаційна робота - Тітов Дмитро 125-16-1.docx

2. Презентація - Тітов Дмитро 125-16-1.pptx

ДОДАТОК Б. Наказ на проведення обстеження ОІД

Товариство з обмеженою відповідальністю

«Кредит-Легко»

НАКАЗ

«___»_____ Кам'янське №_____

Про обстеження та категоріювання
об’єктів інформаційної
діяльності ТОВ "Кредит - Легко"

Відповідно до Положення про технічний захист інформації в Україні, затвердженого Указом Президента України від 27.09.1999 № 1229, Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29.03.2006 № 373, вимог нормативного документа системи технічного захисту інформації № 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”, для проведення обстеження та категоріювання об’єктів наказую:

1. Створити комісію з обстеження та категоріювання об’єктів інформаційної діяльності ТОВ "Кредит - Легко", де циркулює інформація з обмеженим доступом, що не становить державної таємниці (далі – комісія) у складі:

Сидоренко В. М. - заступник генерального директора.

Петренко В.В. - керівник служби безпеки.

Іванов І.І. - системний адміністратор .

2. Комісії провести обстеження та категоріювання об’єктів інформаційної діяльності ТОВ "Кредит - легко", де циркулює інформація з обмеженим доступом, що не становить державної таємниці в терміни, які встановлені законодавством.

3. Контроль за виконанням даного розпорядження залишаю за собою.

Генеральний директор Власов М. К.

ДОДАТОК В . НАКАЗ НА СТВОРЕННЯ КСЗІ

Товариство з обмеженою відповідальністю

«Кредит-Легко»

НАКАЗ

«___»_____ Кам'янське №_____

Про створення КСЗІ

у товаристві з обмеженою

відповідальністю

«Кредит-Легко»

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 категоріювання і обстеження складових інформаційно-телекомунікаційної системи товариства з обмеженою відповідальністю «Кредит - Легко» (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 _____ Власов М. К.

ДОДАТОК Г.

Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-16-1

Тітова Дмитра Сергійовича

на тему: «Розробка політики безпеки інформаційно-телекомунікаційної системи ТОВ "Кредит - Легко"»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 75 сторінках.

Метою кваліфікаційної роботи є підвищення рівня захищеності інформації в ІТС ТОВ "Кредит - Легко".

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: проведення обстеження ТОВ "Кредит - Легко", проведення аналізу ризиків інформаційної безпеки з виявленням загроз; створення документів з політики безпеки..

Практичне значення результатів кваліфікаційної роботи полягає у підвищені рівня захисту інформації в ІТС організації, за рахунок розробки політик безпеки інформації.

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

За час дипломування Тітов Д.С. проявив себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека» .

Рівень запозичень у кваліфікаційній роботі не перевищує вимог "Положення про систему виявлення та запобігання плагіату".

Кваліфікаційна робота заслуговує оцінки «_____».

Керівник кваліфікаційної роботи **Галушко О.М.**

Керівник спец. розділу **Тимофєєв Д. С.**

Р Е Ц Е Н З І Я

на кваліфікаційну роботу студента групи 125-16-1

Тітова Дмитра Сергійовича

на тему: «Розробка політики безпеки інформаційно-телекомунікаційної системи ТОВ "Кредит - Легко"»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 75 сторінках.

Метою кваліфікаційної роботи є підвищення рівня захищеності інформації в ІТС ТОВ "Кредит - Легко".

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: проведення обстеження ТОВ "Кредит - Легко", проведення аналізу ризиків інформаційної безпеки з виявленням загроз; створення документів з політики безпеки..

Практичне значення результатів кваліфікаційної роботи полягає у підвищені рівня захисту інформації в ІТС організації, за рахунок розробки політик безпеки інформації.

Результати кваліфікаційної роботи можуть бути використані при розробці політики безпеки інформації підприємств подібногог профілю.

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

Кваліфікаційна робота заслуговує оцінки «_____».

ДОДАТОК Д. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	1	
4	А4	Стан питання. Постановка задачі	9	
5	А4	Спеціальна частина	46	
6	А4	Економічна частина	10	
7	А4	Висновки	1	
8	А4	Перелік посилань	3	
9	А4	Додаток А. Перелік матеріалів на електронному носії	1	
10	А4	Додаток Б. Наказ на проведення обстеження ОІД	1	
11	А4	Додаток В. Наказ на створення КСЗІ	1	
12	А4	Додаток Г. Відгук керівника кваліфікаційної роботи	1	
13	А4	Додаток Д. Відомість матеріалів кваліфікаційної роботи	1	

ДОДАТОК Е. ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

Керівник розділу _____ доц. Пілова Д.П.