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 *Трубки Дениса Андрійовича*

академічної групи

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему Політика безпеки в інформаційно-телекомунікаційній системі комунального підприемства ‘NewMed’

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	проф. Кагадій Т.С.			
розділів:				
спеціальний	ст. вик. Святошенко В.А			
економічний	доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. вик. Тимофєєв Д.С.			

Дніпро
2021

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Трубки Дениса Андрійовича* **академічної групи** *125-17-1*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*
спеціалізації _____
за освітньо-професійною програмою *Кібербезпека*

на тему Політика безпеки в інформаційно-телекомунікаційній системі комунального підприемства 'NewMed'

Затверджену наказом ректора НТУ «Дніпровська політехніка» від _07.06.2021_ № ___317-С___

Розділ	**Зміст**	**Термін виконання**
1. Стан питання. Постановка задачі	Проаналізувати проблеми захисту інформації в ІТС в сфері медичних послуг. Виконати аналіз нормативно-правових документів. Здійснити постановку задачі.	07.05.2021
2.Спеціальна частина	Виконати обстеження ОІД, категорювання об'єкту. Створити моделі загроз та порушника. Обрати профіль захисту. Розробити основні елементи політики безпеки.	22.05.2021
3. Економічний розділ	Розрахувати економічну доцільність створення політики безпеки.	09.06.2021

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)
Дата видачі завдання: _____10.02.2021_____
Дата подання до екзаменаційної комісії: ___11.06.2021_____
Прийнято до виконання _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: с., рис., табл., додаток, джерело.

Об`єкт дослідження: клініка “NewMed”

Предмет дослідження: політика безпеки інформації в інформаційно-телекомунікаційній системі підприємства

Мета роботи: розробка захищеної інформаційної системи для повноцінного функціювання підприємства.

В першому розділі кваліфікаційної роботи надано загальний аналіз проблем інформаційної безпеки світу та України, розглянуто стан інформаційної безпеки на підприємствах, які займаються наданням медичних послуг.

В другому розділі кваліфікаційної роботи розглянуто наведену загальну характеристику обстежуваного об’єкту інформаційної діяльності, розроблено модель загроз, виконано аналіз та оцінка ризиків інформаційної безпеки, сформовано загальні положення політики безпеки інформації.

Також, у другому розділі надані пояснення стосовно обраних рішень, так як розуміючи детально для чого було вибране саме таке рішення, співробітники будуть більш відповідально ставитися до виконання своєї ролі у ІБ.

В третьому розділі кваліфікаційної роботи розраховано доцільність використання системи безпеки та економічну ефективність впровадження її елементів в інформаційно-телекомунікаційній системі на об’єкті інформаційної діяльності.

ІНФОРМАЦІЙНА БЕЗПЕКА, ЗАГРОЗИ, ВРАЗЛИВОСТІ, ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, ПРОФІЛЬ ЗАХИЩЕНОСТІ, МОДЕЛЬ ЗАГРОЗ, ОЦІНКА РИЗИКУ

Реферат

Пояснительная записка с., Рис., Табл., Приложение, источник.

Объект исследования: клиника "NewMed"

Предмет исследования: политика безопасности информации в информационно-телекомуникационной системе предприятия

Цель работы: разработка защищенной информационной системы для полноценного функционирования предприятия.

В первом разделе квалификационной работы предоставлено общий анализ

проблем информационной безопасности мира и Украины, рассмотрено состояние информационной безопасности на предприятиях, занимающихся предоставлением медицинских услуг.

Во втором разделе квалификационной работы рассмотрены приведенную общую характеристику обстежуваного обьекта информационной деятельности, проработано модель угроз, сделано анализ и оценка рисков информационной безопасности, сформировано общие положения политики безопасности информации.

Также, во второй главе даны пояснения относительно избранных решений, так как понимая подробно для чего было выбрано именно такое решение, сотрудники будут более ответственно относиться к выполнению своей роли в ИБ.

В третьем разделе квалификационной работы рассчитана целесообразность использование системы безопасности и экономической эффективности внедрение ее элементов в информационно-телекоммуникационную систему на объекте информационной деятельности.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, УГРОЗЫ, УЯЗВИМОСТИ, ИНФОРМАЦИОННО-ТЕЛЕКОМУНИКАЦИОННАЯ СИСТЕМА, ПРОФИЛЬ ЗАЩЕЩЕННОСТИ, МОДЕЛЬ УГРОЗ, ОЦЕНКА РИСКОВ

Abstract

Explanatory note

Object of research: clinic "NewMed"

Subject of research: policy of information security in the information and telecommunication system of the enterprise

Purpose of work: development of a secure information system for the full functioning of the enterprise.

In the second section of the qualification work, the given general characteristics of the information activity object are considered, a model of threats has been worked out, an analysis and assessment of information security risks has been made, and general provisions of information security policy have been formulated.

Also, in the second chapter, explanations are given regarding the selected solutions, since understanding in detail why such a solution was chosen in detail, employees will be more responsible in fulfilling their role in information security.

In the third section of the qualification work, the expediency is calculated use of a safety and cost-effectiveness system introduction of its elements into the information and telecommunication system at the object of information activity.

INFORMATION SECURITY, THREATS, VULNERABILITIES, INFORMATION AND TELECOMMUNICATION SYSTEM, SECURITY PROFILE, THREAT MODEL, RISK ASSESSMENT

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС - автоматизована система;

ДСТУ – державний стандарт України;

ІТС – інформаційно-телекомунікаційна система;

КЗЗ — комплекс засобів захисту;

КС — комп'ютерна система;

КСЗІ — комплексна система захисту інформації;

НД - нормативний документ;

НД ТЗІ - нормативний документ системи технічного захисту інформації;

НСД — несанкціонований доступ;

ОІД – об’єкт інформаційної діяльності;

ОС — обчислювальна система;

ПЗ — програмне забезпечення.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

На сьогоднішній день ситуація з кіберзлочинами стає все більшою проблемою. Кіберзловмисники об'єднуються в злочинні угрупування та атакують приватну та державну системи. Різке підвищення кіберзлочинів в Україні почалося у 2014-2015 роках через геополітичні та соціально-економічні причини.

Однією із головних причин збільшення кількості атак у 2017 році було викриття вразливості MS17-010[30]. Є інформація, що во знайдення цієї вразливості пряме відношення мало Агентство Національної Безпеки Сполучених Штатів Америки.[31] Ця вразливість давала змогу виконувати системні команди із правами системи, тобто мала найвищі привілеї в системі. Атака проводилася на 445 порт, який відповідав за протокол SMBv1. Вразливості були знайдені у системах сімейства Windows, особливо це стосується версії Windows 7.Завдяки цієї вразливості стало можливо побудувати експлоіт EternalBlue та виготовити декілька вірусів, таких як Wannacry та Petya[29].

Принцип дії віруса Wannacry складався с декількох етапів. На першому етапі програма сканувала спилок IP-адрес у локальній мережі та намагалася виявити відкритий порт 445. Далі вона намагалася виконати експлуатацію вразливості MS17-010. Якщо їй вдавалося це зробили, то вона установлювало шкідливий код DoublePulsar і вже через нього встановлювала програму-вимагач, яка шифрувала всі несистемні файли на ПК, тим самим залишаючи комп'ютер в робочому стані, відправляла ключи на сервер в мережі Tor та вимагала оплату за розблокування даних в розмірі приблизно 300 доларів США[30].

Від цієї атаки більш за все постраждали Росія, Україна та Індія.[30] В Україні атака вразила і державну систему, в тому числі і медичну. Основною причиною стало застаріле ПЗ, так як ще в 2015 році була випущена Windows 10[32], яка не мала цієї вразливості. Це означає, що українські компанії, в тому числі медичні заклади, мали приблизно два роки на те, щоб виправити цю проблему просто встановивши нову версію. Особливо це дивно для медичного

сектору, так як в медичних закладах, особливо в ті роки, була невелика кількість комп'ютерів і ціна на ліцензійне ПЗ була невелика.

Сьогодні все більше інформації зберігається в електронному вигляді, причиною цього став масовий перехід на електронну систему обліку та відмову від застарілих паперових методів зберігання інформації.

Здебільшого, сучасні лікарні зберігають інформацію про стан пацієнтів, які зараз проходять лікування; зареєстрованих мешканців району, що можуть відвідувати лікарню та є закріпленими за певним лікарем; інформацію про електронні банківські картки пацієнтів або членів їх родини, якими були сплачені рахунки за надані медичні послуги; персональні данні людей, які користуються або користувалися послугами в певній лікарні; персональні та робочі данні працівників лікарні та інше.

Всі ці данні дуже корисні і бажані будь-якими злочинцями, так званими хакерами, оскільки вони дають змогу не тільки зібрати персональні дані, а ще і локалізувати їх власників. Це дуже корисно для шахрайства. Якщо зловмисник зможе отримати доступ по аналізів або діагнозів та змінити їх, це може призвести до великих проблем із здоров'ям пацієнтів або навіть вбити пацієнта, який, лікуючись вдома, почне приймати ліки, що завдасть йому шкоди.

Поширені загрози кібербезпеки, з якими стикаються медичні заклади є:

- крадіжка персональних даних та втрата конфіденційних даних. Ця інформація буде особливо цінною для кіберзловмисників, так як вони можуть використати цю інформацію для шахрайства або для завдання шкоди честі та гідності людини.
- автоматизовані загрози. До цього відносяться злам облікових записів пацієнтів, лікарів та інших робітників медичного закладу. Сканування вразливостей, спам та додавання серверу та комп'ютерів до ботнету, відмова від обслуговування – це все може швидко вивести інформаційну систему із ладу.
- порушення діяльності. Завдяки кібератаки може бути видалена комп'ютерна інфраструктура, персональні дані, шаблони, бланки, аналізи, пошта. Це може унеможливити

Основними проблемами захисту інформації для закладів, які займаються наданням медичних послуг є:

- проблема збереження цілісності даних
- проблема захисту ПК та серверів від комп'ютерних вірусів
- проблема фізичного несанкціонованого доступу до інформації

Згідно з Законом України 'Про захист персональних даних' № 2297-VI[2], усі персональні дані повинні зберігатися та оброблюватися згідно з ним, і кожен громадянин має право на 'захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи'. Саме це вимагає від компанії, а саме NewMed, впровадження політики безпеки, що буде дотримуватися усіх вимог, яких потребує законодавство та ділова репутація.

1.2 Аналіз нормативно-правової бази

Поняття «безпека інформації» визначено у ISO/IEC 27000 п. 3.28 (information security)[33] «Безпека інформації» - збереження конфіденційності, цілісності та доступності інформації.

Для кваліфікації безпеки в сфері інформації мають враховуватися і інші властивості, такі як справжність, звітність, неприйняття та надійність. В національному вимірі поняття безпека інформації передбачає захищеність інформації від несанкціонованих дій (випадкових чи навмисних), що призводять до модифікації, розкриття чи знищенням даних.

Забезпечення кібербезпеки в Україні ґрунтується на принципах:

- верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом;
- забезпечення національних інтересів України;
- відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі;

- державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері;
- пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід'ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі;
- пріоритетності запобіжних заходів;
- невідворотності покарання за вчинення кіберзлочинів;
- пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;
- забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки.

Більш за все виділяють такі проблеми в інформаційно-телекомунікаційних системах медичних закладів:

- Низький рівень інформатизації медичної сфери
- Несанкціонований доступ до інформаційно-телекомунікаційних систем
- Використання неліцензійного ПО, засобів та комплексів обробки інформації

Останнє є дуже поширеною проблемою через велику ціну ліцензійного ПО.

Також виконання роботи ґрунтується на дійсному та чинному законодавству України, пов'язаним із забезпеченням інформаційної безпеки, а також на інших офіційних рекомендаціях та нормативних документах:

- Закон України «Про інформацію» від 02.10.1992 No2657-XII [1]. У цьому законі визначається правила щодо одержання, збирання, зберігання, використання, поширення та захисту інформації.
- Конституція України[22]. Вона є основним законодавчим чинником та у неї входять інформація про права та свободи громадян, а також в неї входять норми, на яких будується забезпечення ІБ України.

- Закон України “Про захист персональних даних” від 01.06.2010 No 2297-VI.[2] Регулює відносини в правовому полі, що пов’язані із захистом персональних даних, їх обробкою, та його основною метою є прав та свобод громадянина, а саме право будь-якої на невтручання в особисте життя під час обробки інформації.
- Закон України “Про доступ до публічної інформації” від 13.01.2011 No2939-VI[3]
- Закон України “Про захист інформації в інформаційно- телекомунікаційних системах” від 05.07.1994 No80-VI.[4] Цей закон регулює відносини в інформаційно-телекомунікаційних системах.
- НД ТЗІ 1.4-001[9] - Типове положення про службу захисту інформації в автоматизованій системі.
- НД ТЗІ 1.6-005[12] - Захист інформації на об’єктах інформаційної діяльності. Положення про категорювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.
- Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека Пілова. Д.П [14]
- НД ТЗІ 1.1-002-99[25] - Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу цей нормативний документ технічного захисту інформації (НД ТЗІ) визначає методологічні основи (концепцію) вирішення завдань захисту інформації в комп'ютерних системах і створення нормативних і методологічних документів, регламентуючих питання:
- - визначення вимог щодо захисту комп'ютерних систем від несанкціонованого доступу;
- - створення захищених комп'ютерних систем і засобів їх захисту від несанкціонованого доступу;
- - оцінки захищеності комп'ютерних систем і їх придатності для вирішення завдань споживача.
- Документ призначено для постачальників (розробників), споживачів

(замовників, користувачів) комп'ютерних систем, які використовуються для обробки (в тому числі збирання, зберігання, передачі і т. д.) критичної інформації (інформації, що вимагає захисту), а також для державних органів, що здійснюють функції контролю за обробкою такої інформації.

- НД ТЗІ 1.1-005-07[26] - цей нормативний документ (НД) системи технічного захисту інформації (ТЗІ) визначає основи організації та етапи виконання робіт щодо створення комплексу на об’єкті інформаційної діяльності (ОІД) органу державної влади, місцевого самоврядування, військового формування, підприємства, установи та організації (далі – установа), який має забезпечувати захист від витоку інформації з обмеженим доступом (ІзОД) можливими технічними каналами (далі – комплекс ТЗІ).

Вимоги цього НД можуть використовуватися під час обґрунтування, організації розроблення, впровадження заходів захисту ІзОД від загроз, що можуть бути здійснені каналами спеціального впливу на технічні засоби інформаційних (автоматизованих), телекомунікаційних, інформаційно-телекомунікаційних систем (далі – ІТС) та на інші технічні засоби.

Захищеність об’єктів, комплексів та засобів спеціального зв'язку від витоку інформації технічними каналами визначається іншими НД.

- НД ТЗІ 1.6-005-2013[24] Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці, розроблено відповідно до Закону України “Про Державну службу спеціального зв’язку та захисту інформації України” та Положення про технічний захист інформації в Україні, затвердженого Указом Президента України від 27.09.1999 № 1229.
- НД ТЗІ 3.6-001-2000[23] Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. Цей нормативний документ 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 НД ТЗІ 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.

- НД ТЗІ 3.7-001-99[27] Цей нормативний документ 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 (далі — оброблення) інформації з обмеженим доступом або інформації, захист якої гарантується державою. Положення цього документа розповсюджуються на державні органи, Збройні Сили, інші військові формування, МВС, Раду Міністрів Автономної Республіки Крим і органи місцевого самоврядування, а також підприємства, установи і організації всіх форм власності, які володіють, користуються і розпоряджаються інформацією, яка належить до державних інформаційних ресурсів, або інформацією, вимога щодо захисту якої встановлена законом. Власники (користувачі) іншої інформації, положення цього документа застосовують на свій розсуд.
- НД ТЗІ 3.7-003-2005.[28] Цей документ 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.

1.3 Постановка задачі.

Для повноцінного функціонування та зменшення ризиків треба розробити політику безпеки інформації ПП "NewMed". Необхідно провести обстеження фізичного та інформаційного середовища підприємства. Обстеженню підлягають

обчислювальні системи та середовища користувачів. Також треба скласти модель порушника, виконати розробку основних елементів ІБ, класифікувати джерела загроз та вразливості, економічно обґрунтувати доцільність впровадження політики безпеки інформації.

Висновок до розділу 1

У даному розділі були розглянуті загрози, що несуть собою комп'ютерні віруси та хакерські атаки. Розглянуто типові проблеми в області інформаційної безпеки для компаній, що займаються наданням медичних послуг та зроблено аналіз нормативно-правової бази, що охоплює інформаційну безпеку в Україні та відноситься до медичної сфери надання послуг. Також було визначено завдання на спеціальну частину.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про ПП «NewMed»

Підприємство "NewMed" займається надання медичних послуг.

Форма власності: «NewMed» комерційна організація, що зареєстрована як приватне підприємство. Обслуговує фізичних осіб та юридичних осіб.

Для діяльності організації клієнти повинні надавати ксерокопії документів, для підтвердження особи. Також, через оплату послуг, клієнти надають свої банківські дані. Через це ПП «NewMed» має справу з комерційною таємницею і персональними даними. Вищий гриф секретності – строго конфіденційно.

Графік роботи підприємства 5 днів на тиждень, з 9:00 до 17:00 з перервою на обід з 12:00 до 13:00. В обідню перерву підприємство не займається основною діяльністю, служба охорони обідають на місці.

2.2 Обґрунтування створення КСЗІ

Згідно з нормами чинного законодавства України щодо захисту інформації доступ до певних видів інформації повинен бути обмеженим. Для додержання законодавства створюється КСЗІ, яка забезпечує цілісність та доступність інформації, перелік користувачів та їх права доступу, політика безпеки інформації, а відповідальність за збереження інформації та її захист покладається на власника системи.

2.3 Обстеження на об’єкті інформаційної діяльності

Обстеження фізичного середовища: Об’єкт знаходиться на 2 поверху двоповерхової прибудови, що є частиною різноповерхової будівлі у лівому крилі. Об’єкт розташований між житловими домами-багатоповерхівками. З північної сторони знаходиться інша чотириповерхова медична установа. З південної сторони знаходиться дорога, за якою розташовані житлові будинки, найближчий з яких знаходиться у 100 метрах. З західної сторони знаходиться перехрестя доріг. Із східної сторони знаходиться приватна медична установа, спеціалізована на аналізах. Північна та східна установа знаходяться у приміщеннях, які фактично є частиною однієї будівлі із об’єктом інформаційної діяльності. На першому

поверху знаходиться аптека, через яку клієнти заходять по сходах на другий поверх.

Характеристика складових ОІД:

- Висота стелі 350 мм
- Стіни залізобетонні з товщиною 500 мм з внутрішньої сторони. відремонтовані під евростандарт.
- Перекриття між кімнатами – 500 мм залізобетон із євроремонтом.
- Перекриття стеля\підлога залізобетон 500мм
- Вікна мають розмір 2000х1500 мм металоплатикові із зовнішніми віконними гратами.
- Двері в приміщення виготовленні з цільного сталевого листу, мають механічний врізний замок. Розміри 2200х1050 мм.

Максимальне навантаження 60 чоловік на годину.

Будівля обладнана системами електроживлення, опалення, водопостачання, каналізації.

Система електроживлення від трифазної мережі 220 В. Заземлення в наявності. Вентиляція витяжна локальна.

Протипожежною сигналізацією обладнанні всі приміщення окрім туалету. Два типи сповіщувачів: димовий і ручний. Ручні знаходяться в коридорі по шляху евакуації. Димові розташовані в коридорі та кожному кабінеті. Теплові розташовані у серверній та кабінеті директора. Електропровідна система виконана з вогнестійких матеріалів.

Система електропостачання та опалення працює завдяки міській комунальній мережі.

Системи наведені у таблиці:

Таблиця 2.1 Системи підключення

Система	Тип підключення
Заземлення	Комп'ютери, принтер та сервер заземлені спільним контуром, вихід якого знаходиться за межами КЗ
Електроенергія	Приміщення живиться від трансформаторної станції, до якої мають доступ інші споживачі. Станція знаходиться за межами КЗ
Вентиляція	Проточно-витяжна
Водопостачання	Підключення до комунального водоканалу міського водопостачання, що знаходиться за межами КЗ
Інтернет	Кабельне, виходить за межі ОІД
Опалення	Міська мережа опалення за межами КЗ
Каналізація	Міська мережа каналізації за межами КЗ

Структурні підрозділи, з яких складається підприємство:

- охорона. Виконує функції фізичної охорони підприємства. Функції інформаційної охорони підприємства полягають на системного адміністратора;
- лікарі. Основний структурний підрозділ підприємства, який виконую частину інформаційної діяльності підприємства;
- медичні співробітники. Асистенти лікарів, на яких полягають допоміжні функції, функції секретарів та прибиральників;
- реєстратура. Місце реєстрації клієнтів, сховище ключів від кабінетів, місце друкування та місцезнаходження принтера. Виконує адміністративну функцію;

- серверна. Місцезнаходження серверу та баз даних. Також на сервері розміщений сайт. Доступ до серверної мають директор та системний адміністратор. Ключ від серверної знаходиться у кабінеті директора, так що, фактично, отримати доступ до серверної можливо тільки через дозвіл директора та фізичну передачу ключа;

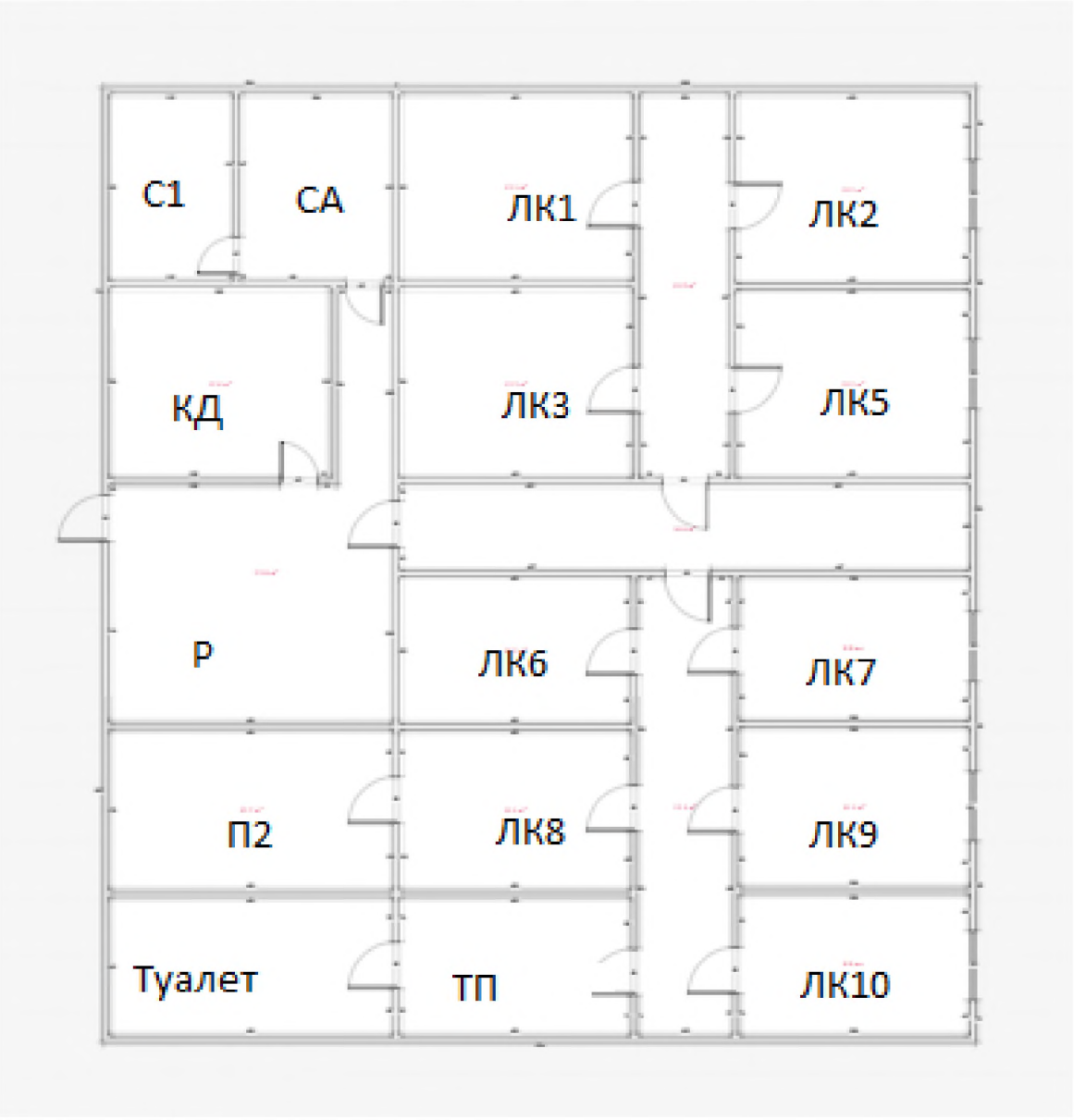

Рисунок 2.1 План приміщень

Умовні позначення:

- С1 – серверна кімната
- СА – системний адміністратор
- Р - регістратура
- КД – кабінет директора
- П1 – процедурна кімната 1
- П2 – процедурна кімната 2
- ЛК1 – кабінет лікаря
- ЛК2 – кабінет лікаря
- ЛК3 – кабінет лікаря
- ЛК4 – кабінет лікаря
- ЛК5 – кабінет лікаря
- ЛК6 – кабінет лікаря
- ЛК7 – кабінет лікаря
- ЛК8 – кабінет лікаря
- ЛК9 – кабінет лікаря
- ЛК10 – кабінет лікаря
- ТП – технічне приміщення для зберігання засобів для підтримання чистоти
- Туалет - туалет

Таблиця 2.2 Штат співробітників

Посада	Кількість
Співробітник реєстратури	6 (дві зміни по 2 + 1 адміністратор клініки
Лікар	10
Медичний співробітник	10
Системний адміністратор	1
Директор	1
Охоронець	4 (дві зміни по 2)

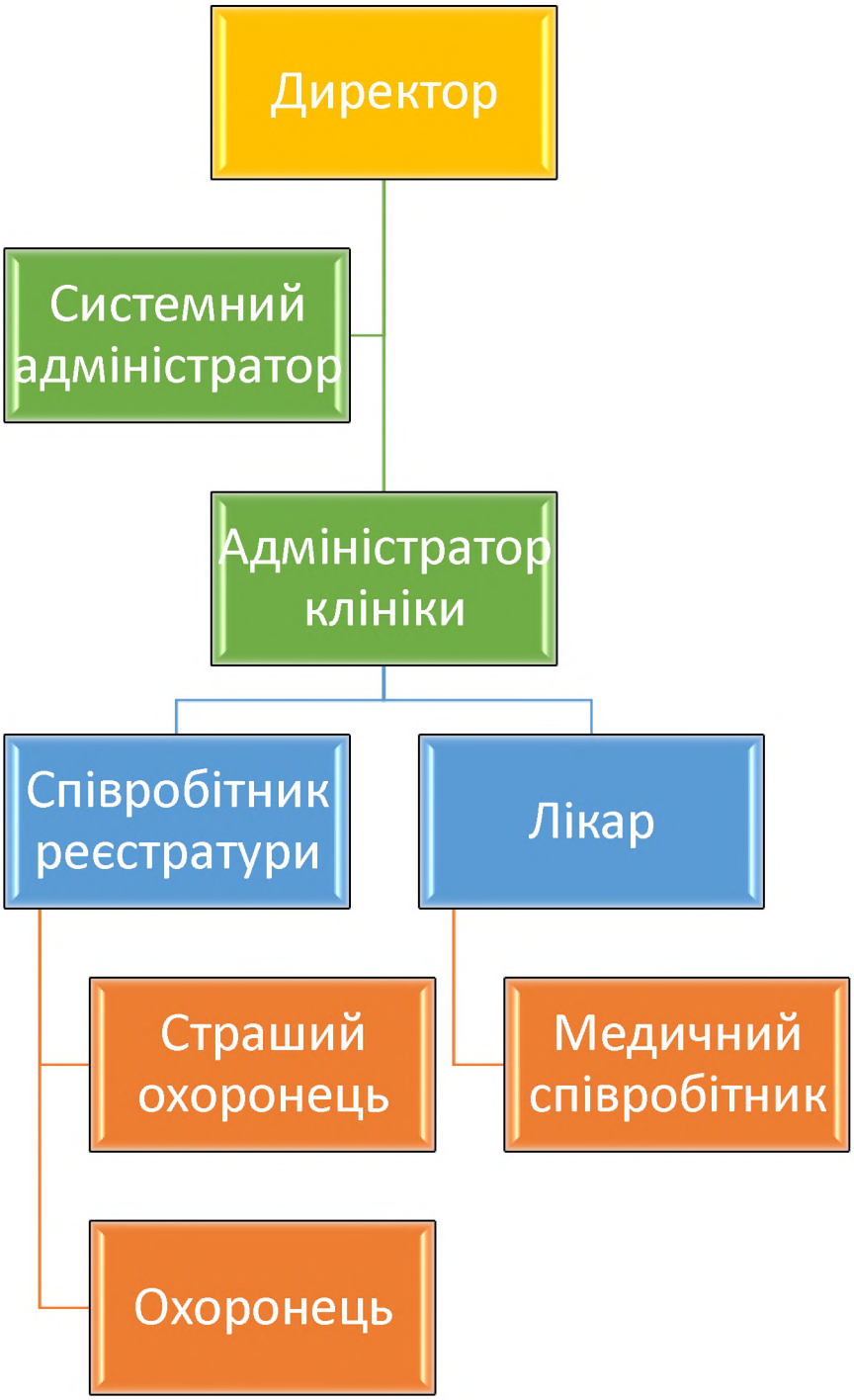

Рисунок 2.2Організаційна структура підприємства. Підпорядкування.

Обов'язки персоналу:

- Директор.

Керує юридичною, господарською та фінансовою діяльністю підприємства. Організовує роботу для ефективної взаємодії всіх структурних підрозділів. Забезпечує дотримання дійсного та чинного законодавства, впроваджує прогресивні форми управління та нововведення, слідкує за раціональною витратою фінансів та матеріальної складової підприємства. Розподіляє матеріальні ресурси підприємства та слідкує за балансом матеріальної забезпеченості підрозділів.

- Адміністратор клініки.

Виконує організаційно-розпорядчу для ефективного виконання роботи, слідкує за дотриманням санітарних норм всіми присутніми, як співробітниками, так і клієнтами. Вирішує конфліктні питання.

- Співробітник реєстратури.

Відповідає на телефонні дзвінки клієнтів, складає графік для лікарів. Складає базу даних нових клієнтів, виставляє рахунки, друкує документи, приймає оплату. Відповідає на запитання в онлайн-чаті. Заздалегідь нагадує клієнтам про їх час прийому через онлайн-месенджери або через смс. Відправляє медичні справки, діагнози та інше на пошту клієнта.

- Старший охоронець.

Керує роботою охорони, слідкує за дотриманням порядку та наглядає за пожежною безпекою.

- Охоронець.

Слідкує за дотриманням порядку, виконує вказівки старшого охоронця.

- Лікар.

Виконує обов'язки для своєї посади, призначає лікування, ставить діагнози та заносить їх у базу даних.

- Медичний співробітник.

Слідкує за чистотою кабінета, допомагає лікарю, виконує його прямі вказівки.

- Системний адміністратор.

Усунення технічних неполадок, адміністрування баз даних, надання прав доступу згідно з розпорядженням директора, редагування бази даних, забезпечення безпеки баз даних, слідкування та оновлення ПЗ, видалення інформації з баз даних, підтримка баз даних в актуальному стані. Слідкування за станом серверу та серверної кімнати.

Інформація, що оброблюється

Інформація, що оброблюється на підприємстві поділяють на три категорії:

- Публічна
- Конфіденційна
- Строго конфіденційна

До публічної інформації відноситься:

- Список лікарів
- Офіційні документи
- Ліцензія на надання медичних послуг
- Розклад прийомів лікарів
- Розклад роботи
- Інформація про надаванні послуги
- Ціни на послуги

До конфіденційної інформації відносять:

- Економічну складову підприємства
- Стратегія розвитку
- Внутрішні зміни
- Робоче листування працівників
- Скарги
- Внутрішня інформація компанії

До строго конфіденційної інформації відносять:

- Особисті дані клієнтів
- Інформація, що відноситься до системи охорони та інформаційної безпеки підприємства
- Класифікація інформації

Таблиця 2.3 Класифікація інформації

№	Назва	Тип	Режим доступу	Доступ мають
1	Публічні офіційні документи	Публічна	Відкрита	Всі
2	Внутрішні документи	Конфіденційна	ІзОД	Д, СА, АК, ЛК, Р
3	Інформація про послуги, ціни, графік роботи	Публічна	Відкрита	Всі
4	Документи обліку та реєстрації	Конфіденційна	ІзОД	Д, АК, Р, ЛК, СА, О
5	Персональні дані клієнтів	Конфіденційна	ІзОД	Д, АК, Р, ЛК, СА
6	Стратегія розвитку	Конфіденційна	ІзОД	Д, АК, СА
7	Система охорони і інформаційної безпеки	Конфіденційна	ІзОД	Д, АК, СА

Обчислювальна система є розподіленою, пристрої мають вихід до глобальної мережі. Локальна мережа використовується для внутрішніх потреб підприємства. Для взаємодії з зовнішніми ресурсами кожна робоча станція має вихід до глобальної мережі Інтернет, що забезпечується кабельним з'єднанням. Надання послуг по забезпеченню підключення до мережі Інтернет займається компанія «Фрегат».

Обладнання АС, завдяки якого оброблюється та зберігається інформація на ОІД:

- ПК директора
- ПК системного адміністратора
- ПК реєстратури
- ПК лікарів
- Сервер
- Мережеві принтери

ІТС ОІД представляє собою мережу типу «зірка», з окремо підключеним сервером. Використовується один комутатор.

Таблиця 2.4 Технічні характеристики ПК:

№	Тип	Найменування	Кількість
1	Процесор	Intel Core i5-11400 2.6GHz/12MB	12
2	Материнська плата	ASUS ROG Crosshair VII з Wi-Fi модулем	12
3	ОЗУ	DDR4-3600 16 Гб	12
4	Жорсткий диск	AMD R5 960 Гб	12
5	Відеоадаптер	MSI GT 710 2 Гб	12
6	Монітор	Dell E2420H Black	12
7	Корпус	MSI MAG Forge 100M	12

№	Тип	Найменування	Кількість
8	Комп’ютерна миша	Logitech M185 Wireless Grey	12
9	Клавіатура	Logitech K280e USB	12

Рисунок 2.3Схема розміщення обчислювальної техніки.

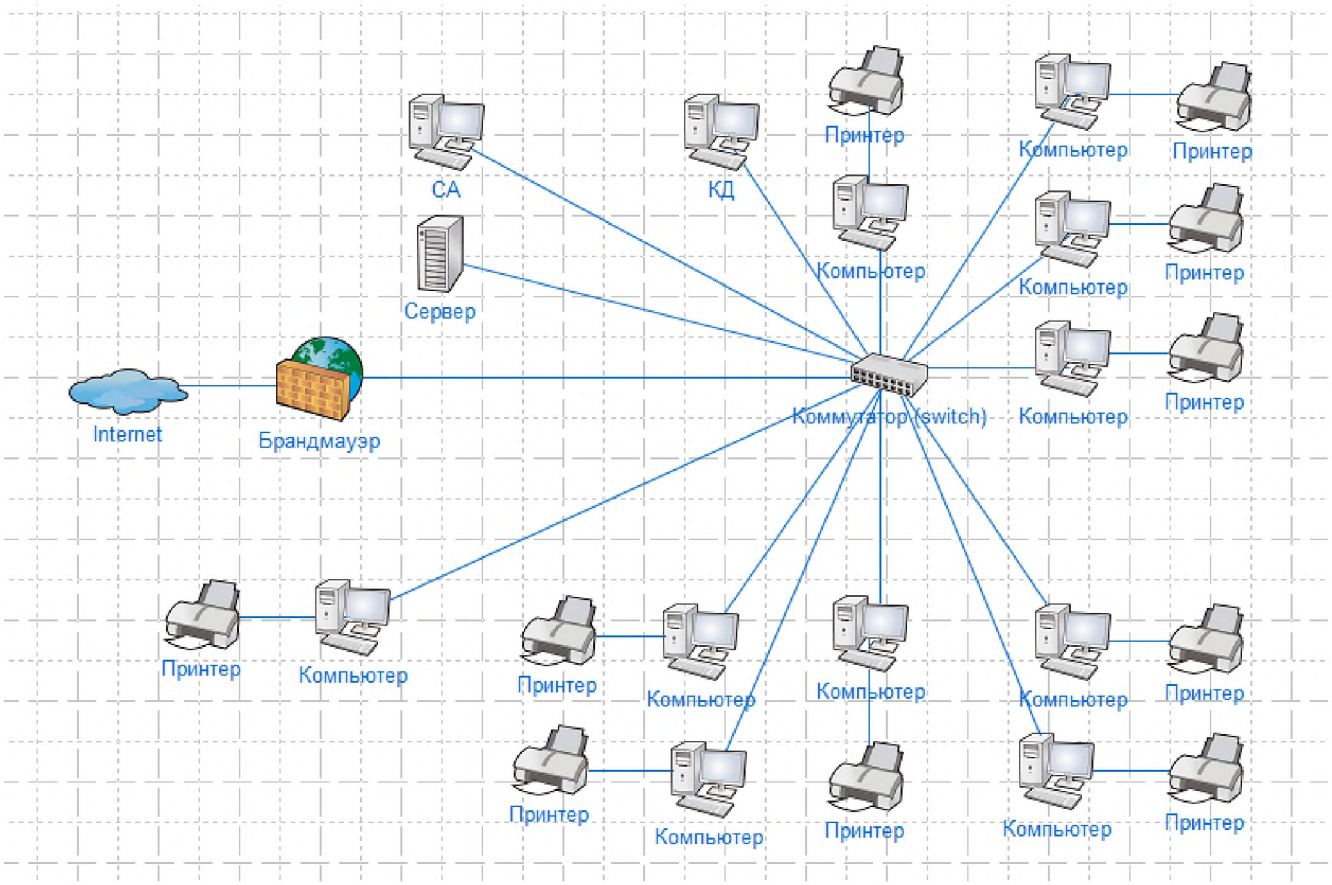

Рис 2.4 Схема ІТС

2.4 Аналіз інформаційних ризиків

2.4.1 Модель порушника

Модель порушника ІБ – це теоретичне описання можливої шкоди, що може завдати зловмисник на основі його рівня доступу та технічної кваліфікації. Порушником може бути співробітник або інший користувач системи, тоді це називається внутрішній порушник інформаційної безпеки. Також порушником може бути особа, що знаходиться за межами КЗ і тоді це буде зовнішнім порушником інформаційної безпеки.

Модель порушника визначає:

- Мету порушника, яку він намагається досягти, коли порушує інформаційну безпеку
- Технічну кваліфікацію порушника, яку він повинен мати щоб мати змогу порушити інформаційну безпеку
- Категорія осіб, що можуть бути порушниками інформаційної безпеки

- Загроза для АС, що базується на можливій шкоді, що порушник інформаційної безпеки може їй завдати

Мета порушника може полягати у:

- Отриманні конфіденційної інформації
- Видозміненні інформації
- Знищені конфіденційної інформації
- Втручанні в роботу АС для виведення її з експлуатації

Для аналізу порушника інформаційної безпеки треба розділити порушників на категорії, що будуть характеризувати їх обізнаність, технічні навички так розуміння систем інформаційної безпеки та їх недоліків.

Таблиця 2.5 Специфікація порушника за технічними навичками

Умовне позначення	Технічні навички, рівень обізнаності
К0	Не має технічних навичок, не розбирається в технологія, що використовує підприємство
К1	Має базові навички користування ПК, не розбирається в технологіях, що використовує підприємство
К2	Має поглибленні навички користування ПК, може зрозуміти як працює автоматизована система
К3	Має глибокі знання ПК та в області інформаційних технологій, мав справу зі схожою АС
К4	Має глибокі знання в області інформаційних технологій, розуміє як само працює ця конкретно АС на основі відомих йому технологій
К5	Знає недоліки автоматичної системи, помилки в програмному забезпеченні
К6	Знає вразливості, що можуть бути в АС, знає методи їх експлуатації, знає та розуміє недоліки в системі інформаційної безпеки підприємства

Таблиця 2.6 Специфікація порушника за часом дії

Умовне позначення	Час
Ч0	До впровадження АС або її компонентів
Ч1	Під час збоїв, бездіяльності або оновленні компонентів АС
Ч3	Під час функціонування АС

Таблиця 2.7 Специфікація порушників за місцем дій

Умовне позначення	Характеристика порушника за місцем дії
Д1	Без доступу на контрольовану зону
Д2	З доступом до КЗ, але без доступу до технічних засобів АС
Д3	З доступом до КЗ та технічних засобів АС
Д4	З доступом до засобів керування АС

Таблиця 2.8 Специфікація порушників за їх мотивом

Умовне позначення	Мотив
М1	Безвідповідальність
М2	Корисливий мотив

Класифікація порушників за мотивом, місцем дії, часом дії та категорією обізнаності

Таблиця 2.9 Аналіз порушників

Тип або посада	Категорія обізнаності	Час дії	Місце дії	Мотив
Директор	К2	Ч3,Ч1	Д3, Д4	М2
Системний адміністратор	К4,К6	Ч1,Ч2,Ч3	Д3, Д4	М1, М2
Адміністратор клініки	К1	Ч3	Д3	М1,М2
Співробітник реєстратури	К1	Ч3	Д2	М1, М2
Лікар	К1	Ч3	Д2	М1, М2
Медичний співробітник	К0, К1	Ч3	Д1	М2
Охоронець	К0	Ч3	Д1	М2, М1
Злочинець-хакер	К5,К6	Ч3	Д0	М2

Таблиця 2.10 Характеристики імовірності

Оцінка ймовірності	Характеристика
1	Виникнення інциденту практично неможливо
2	Виникнення інциденту малоймовірне (не частіше ніж 1 раз на 1 рік)
3	Виникнення інциденту ймовірне до 1 разу на 3 місяці
4	Виникнення інциденту ймовірне до 1 разу на тиждень
5	Виникнення інциденту ймовірне до 1 разу на добу

Таблиця 2.11 Рівень загроз

Рейтингова оцінка	Опис
1	незначний
2	низький
3	середній
4	високий
5	критичний

Таблиця аналізу загроз

№	Джерело	Причина вразливості	Тип Загрози	Імовірність	Рівень загрози
1	Внутріш не	Низький рівень кваліфікації	Неналежне розмежування прав доступу	2	4
2	Внутріш не	Порушення цілісності інформації, що зберігається	Копіювання ІзОД людиною, що не має права доступу до ІзОД	2	4
3	Внутріш не	Низький рівень кваліфікації працівників, відсутність або застарілість антивірусного ПЗ.	Завантаження вірусу через неналежне використання мережі Інтернет до ІТС підприємства	2	5

№	Джерело	Причина вразливості	Тип Загрози	Імовірність	Рівень загрози
4	Внутріш не	Низький рівень кваліфікації працівників	Крадіжка інформації через неналежне використання електронної пошти	3	3
5	Внутріш не	Відсутність або застарілість антивірусного ПЗ.	Вразливість у програмному забезпеченні, що надає змогу встановити вірусне програмне забезпечення для контролю частини ІТС	1	5
6	Внутріш не	Відсутність або застарілість антивірусного ПЗ, низький рівень кваліфікації працівників	Встановлення неліцензійного програмного забезпечення, що буде мати в собі вірус	2	4

№	Джерело	Причина вразливості	Тип Загрози	Імовірність	Рівень загрози
7	Внутріш не	Низький рівень кваліфікації працівників, політики безпеки або розділу у політиці безпеки про використання електронної пошти	Використання електронної пошти не в цілях підприємства	4	1
8	Внутріш не	Низький рівень кваліфікації працівників, відсутність або застарілість антивірусного ПЗ.	Навмисне пошкодження технологічного обладнання ІТС підприємства через фізичне або програмне пошкодження елементу ІТС	1	4

№	Джерело	Причина вразливості	Тип Загрози	Імовірність	Рівень загрози
9	Внутріш не	Відсутність контролю за електронною поштою працівників	Навмисне відсилання великої кількості електронних листів або файлів для порушення роботи ІТС через неможливість обробки такої кількості інформації, що призведе до неможливості ефективної роботи підприємства	3	2

№	Джерело	Причина вразливості	Тип Загрози	Імовірність	Рівень загрози
10	Внутріш не	Застаріле ПЗ та\або наявність вірусів; Некомпетентність працівника	Неправильна робота з програмами резервного копіювання, що призведе до пошкодження резервної копії	1	4
11	Внутріш не	Низький рівень кваліфікації працівників, відсутність контролю за використанням програмного забезпечення та за мережею Інтернет в ІТС підриємства	Використання встановленого програмного забезпечення в неналежних цілях	1	3
12	Внутріш не	Відсутність політики, яка регулює використання дозволених програмних засобів.	Неправомірна зміна інформації, в тому числі інформації з обмеженим доступом	1	3

№	Джерело	Причина вразливості	Тип Загрози	Імовірність	Рівень загрози
13	Внутрішне	Відсутність політики безпеки, яка регулює використання дозволених програмних засобів	Використання програмного забезпечення, що заборонено політикою безпеки	1	2
14	Внутрішне	Низький рівень кваліфікації працівників	Некомпетентність персоналу, що призведе до тимчасової відмови правильного функціонування мережі ІТС підприємства та\або окремих її елементів чи пошкодження обладнання підприємства	2	1

№	Джерело	Причина вразливості	Тип Загрози	Імовірність	Рівень загрози
15	Внутріш не	Низький рівень кваліфікації працівників, використання застарілого ПЗ для резервного копіювання, відсутність контролю за резервним копіюванням даних	Порушення цілісності інформації, яке зберігається після відновлення, що було проведено після програмного чи апаратного збою	1	4
16	Внутріш не	Низький рівень кваліфікації працівників	Помилкове введення невірних даних, що будуть збережені в ІТС підприємства	3	2
17	Внутріш не	Відсутність Антивірусних програмних засобів, наявність застарілого ПЗ	Атака на мережу ІТС підприємства, ціллю якою є відмова від обслуговування	1	4

№	Джерело	Причина вразливості	Тип Загрози	Імовірність	Рівень загрози
18	Внутрішне	Порушення правил встановлених політикою безпеки, низький рівень кваліфікації працівників	Системний чи апаратний збій, що тимчасово заблокує можливість доступу до ІзОД	2	1
19	Внутрішне	Порушення правил встановлених політикою безпеки, низький рівень кваліфікації працівників	Передача інформації до автентифікації через неналежне ставлення до зберігання інформації з обмеженим доступом	3	2
20	Внутрішне	Порушення правил встановлених політикою безпеки, низький рівень кваліфікації працівників	Пошкодження технічного обладнання через виливання рідини на неї через неналежне користування робочим місцем	1	3

№	Джерело	Причина вразливості	Тип Загрози	Імовірність	Рівень загрози
21	Внутріш не	Застарілі лінії електронного запезпечення, відсутність заземлення	Скачок напруги, що призведе до пошкодження технологічного обладнання	2	3
22	Внутріш не	Неналежна робота служба охорони	Пошкодження обладнання через третіх осіб(монтажник и, ремонтники) через їх некомпетентніст ь	2	4
23	Внутріш не	Порушення правил встановлених політикою безпеки, низький рівень кваліфікації працівників	Неналежне використання копіювального, що призведе до витоку ІзОД	3	2

№	Джерело	Причина вразливості	Тип Загрози	Імовірність	Рівень загрози
24	Зовнішне	Наявність легкозаймистих речовин, порушення правил встановлених політикою безпеки, низький рівень кваліфікації працівників	Пожежа	1	2
25	Зовнішне	Пошкодження фундаменту, затоплення приміщень, пошкоднення технологічного обладнання підприємства	Повінь	1	2
26	Зовнішне	Пошкодження фундаменту	Землетрус	1	3

Згідно з наведеними вище таблицями можна сказати, що найбільшу увагу варто приділити системному адміністратору та директору, так як вони мають найвищий рівень доступу та можуть порушити систему інформаційної безпеки у різний час. Системний адміністратор має достатньо високі технічні навички, має

великий рівень доступу, точно знає коли буде оновлення системи, що дає йому змогу обходити системи безпеки.

Найбільшою зовнішньою загрозою буде злочинець-хакер, так як йому не потрібен прямий доступ до КЗ і він має високу технічні навички.

2.4.2 Профіль захищеності системи

За результатами обстеження на об’єкті інформаційної діяльності був обраний профіль захищеності системи ЗКЦД1[34] = { КД-2, КО-1, КВ-1,ЦД-1, ЦО-1, ЦВ-1,ДР-1, ДВ-1,НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

КД-2 Базова довірча конфіденційність.

Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. 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. КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта.

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

Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту.

КО-1. Повторне використання об'єктів

Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС. 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, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.

КВ-1. Мінімальна конфіденційність при обміні

Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і 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.

ЦД-1. Мінімальна довірча цілісність

Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. 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.

КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.

ЦО- Обмежений відкат.

Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

ЦВ-1. Мінімальна цілісність при обміні

Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності. КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається.

ДР-1. Квоти

Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу. Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

ДВ-1. Ручне відновлення

Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС.

Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження. Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування.

НР-2. Захищений журнал

Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються. КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки. Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню

для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події.

КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

НИ-2. Одиночна ідентифікація і автентифікація

Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ.

Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму. КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

НК-1. Двонаправлений достовірний канал

Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ. Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен зініціюватись виключно користувачем.

НО-2. Розподіл обов'язків адміністраторів

Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції. Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі.

Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

НЦ-2. КЗЗ з гарантованою цілісністю

Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів. КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування.

Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

НТ-2. Самотестування при старті

Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ. КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ.

НВ-1: Автентифікація вузла

Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ. КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму. Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

2.5 Розробка політики безпеки

Оскільки ПП «NewMed» оброблює інформацію з обмеженим доступом, яка знаходиться у ІТС власника, треба впровадити інформаційний захист. Інформаційний захист повинен мати необхідний рівень захищеності та не потребувати великих затрат на його впровадження. Необхідно провести запобіжні заходи для зменшення ризику загроз, а саме:

- ввести антивірусний захист, що допоможе зменшити загрозу від вірусних атак;
- завадити розширенню повноважень користувачів ІТС завдяки різним атрибутам доступу до системи;
- завадити маскуванню під іншого користувача ІТС
- запобігти від отримання доступу до систему через неуважність або необережність;
- запобігти перехват інформації на паперових та електронних носіях;

Це найбільш серйозні загрози, так як вони можуть призвести до витоку інформації, а оскільки ПП «NewMed» має справу з особистими даними клієнтів, це має бути пріоритетом. Для цього повинні бути впровадженні такі політики інформаційної безпеки:

- політика антивірусного захисту, що знизить ризик зараження комп'ютерів в ІТС комп'ютерними вірусами;
- політика "чистого столу", що знизить ризик витоку інформації через паперовій та електронні носії інформації;
- політика контролю і моніторингу користувачів при їх користуванні мережею Інтернет для зниження ризику від випадкового зараження комп'ютерів різноманітними комп'ютерними вірусами;
- політика легального програмного забезпечення, щоб уникнути "піратського" ПЗ, що може бути заражене комп'ютерними вірусами;
- політика резервного копіювання, щоб зберегти в цілісності конфіденційну інформацію при будь-яких помилках або атаках на ІТС;
- політика утилізації, що вимагає знищення паперових та електронних носіїв інформації після їх виходу з користування;
- політика електронної пошти;

Розробка політики безпеки інформації

Політика антивірусного захисту

Метою політики є встановлення антивірусного захисту для запобігання, виявлення вірусної загрози та її ефективного знешкодження. Всі комп'ютери, що

підключенні до ІТС ПП «NewMed» мають мати антивірусний захист та дотримуватися цієї політики безпеки. Також, при додаванні будь-якого іншого персонального комп'ютеру, наприклад ноутбуку, до ІТС треба перевірити його на відповідність до політики безпеки.

Інструкція політики:

Усі персональні комп'ютери підприємства мають мати встановлене антивірусне програмне забезпечення. Антивірусне програмне забезпечення повинно бути налаштованим, та працювати через рівні проміжки часу.

Антивірусне програмне забезпечення та зразки вірусів повинні постійно оновлюватися. Комп'ютери, що були заражені вірусом повинні бути видалені з мережі, проведене повне сканування системи, відновлення пошкоджених файлів. Комп'ютери повинні знаходитися поза мережею ІТС до їх повного вичищення від вірусних загроз.

Системний адміністратор відповідає за створення та керування процедурами запуску антивірусного програмного забезпечення. Процедури повинні запускати антивірусне програмне забезпечення та підтверджувати комп'ютери як захищенні від вірусів. Будь-які дії з метою створення, встановлення, розповсюдження та маскування шкідливих програм, комп'ютерних вірусів та встановлення неліцензійного програмного забезпечення заборонено.

Рекомендовані процеси для запобігання потрапляння вірусів до персональних комп'ютерів, що знаходяться в ІТС:

- видалення всіх листів із папки "спам", що приходять на електронну пошту;
- ніколи не відкривати файли, що були прислані з невідомої адреси. Такі файли повинні бути негайно видалені, та треба повідомити про цей інцидент системного адміністратора;
- ніколи не відкривати файли, що надходять до електронної пошти без попереднього повідомлення щодо їх відправлення. Якщо буде підтверджено, що файл був відправлений без попередження, то цей файл повинен бути негайно видалений, та треба повідомити про цей інцидент системного адміністратора;

- завжди перевіряти адресу, з якої приходять прийшло електронний лист, так як хакер може встановити електронну адресу, з якої очікується електронний лист або електронну адресу, яка користується довірою, та підмінити адресу. Наприклад електронна адреса admin@company.com та адреса abmin@company.com виглядають схожими на перший погляд, але вони різні, чим і може скористуватись хакер для відправлення файлу з вірусом або для виманювання інформації під виглядом іншого користувача;
- ніколи не завантажуйте файли з невідомих або підозрілих джерел, при випадковому завантаженні в жодному разі неможна відкривати цей файл, його треба негайно видалити;
- треба уникати обміну файлами через диски та флеш-носії, якщо це не є необхідним через ділові вимоги. Якщо, через ділові вимоги, абсолютно необхідно провести обмін файлами через прямий обмін дисками та\або флеш-носіями, їх треба перевірити антивірусним програмним забезпеченням перед його використанням;
- потрібно регулярно створювати резервні копії критичних даних та системних конфігурацій та зберігати їх окремо від ІТС у сейфі. Таким чином при серйозній вірусній атаці або системній помилці, що призведе до пошкодженню або зміненню критичних даних, резервні копії не будуть пошкодженні та завжди буде можливість відновити всі дані.

Відповідальність за порушення політики безпеки

Працівник, що порушив цю політику безпеки, повинен зазнати дисциплінарного стягнення аж до звільнення. Під час розслідування інциденту працівник має бути відсторонений від роботи до завершення розслідування інциденту.

Політика “чистого столу”

Основною задачею введення цієї політики є гарантія, що конфіденційні дані, що знаходяться на паперових та електронних носіях інформації, а також на комп’ютері працівника, повинні вилучатися з робочої місця або

блокуватися, коли предмети, що мають відношення до роботи і ІТС та всі електронні та паперові носії інформації, якщо вони не використовуються або коли працівник покидає своє робоче місце. Ця політика поширюється на всіх працівників організації.

Інструкція політики:

1) Всі співробітники повинні гарантувати, що вся критична та конфіденційна інформація про працівників, клієнтів та будь-яка інша інформація підприємства, до якої працівник має доступ, та знаходиться на робочій станції, в електронному або паперовому вигляді на робочому місці працівника, буде захищена на робочому місці в кінці робочого дня та коли працівник буде відсутній тривалий час.
2) Комп'ютер працівника повинен бути заблокований, коли працівник відсутній.
3) Комп'ютер працівника повинен бути повністю вимкнений наприкінці робочого дня.
4) Конфіденційна або критична інформація має бути прибрана зі столу та закрита у ящику коли працівник відсутній тривалий час або наприкінці робочого дня.
5) Картотеки, що містять критичну та\або конфіденційну інформацію, за їх наявності, повинні зберігатися закритими коли вони не використовуються.
6) Ключі від конфіденційної та\або критичної інформації та серверної не повинні залищатися без нагляду або у дверях.
7) Паролі не мають бути записані у доступному місці або бути приклеєними до єкрану комп'ютера.
8) Завжди перевіряти принтер на наявність залишених у ньому роздруківок або документів на сканування. Якщо такі документи будуть знайдені їх повинно видалити негайно.
9) Зберігати пристрої зберігання даних, такі як флеш-носії та компакт-диски, у замкненому ящику.

Відповідальність

Працівник, що порушив цю політику безпеки, повинен зазнати дисциплінарного стягнення аж до звільнення. Під час розслідування інциденту

працівник має бути відсторонений від роботи до завершення розслідування інциденту.

Політика моніторингу та контролю мережі Інтернет

Метою політики є визначення системних стандартів, що обстежують та обмежують користувачам мережу Інтернет для кожного комп'ютеру у ІТС підприємства. Ця політики потрібна для того, щоб працівники користувались Інтернетом безпечно, та впровадження цієї політики допоможе при розслідуванні інцидентів.

Сфера застосування

Політика поширюється на всіх працівників, що працюють за комп'ютером, що знаходиться в ІТС організації. Ця політика стосується всіх комунікацій між ІТС підприємства та мережею Інтернет.

Інструкція політики

Системний адміністратор контролює використання мережі Інтернет з усіх робочих комп'ютерів працівників у мережі ІТС підприємства. Весь трафік до мережі Інтернет повинен документуватись. Також повинно бути задокументовано яким користувачем виконуються запити до мережі Інтернет. Задокументовані дані про використання мережі Інтернет повинні зберігатися протягом 180 діб.

Доступ до веб-сайтів в мережі Інтернет, що вважаються невідповідними для ІТС підприємства мають бути заблоковані.

Відповідальність

Працівник, що порушив цю політику безпеки, повинен зазнати дисциплінарного стягнення аж до звільнення. Під час розслідування інциденту працівник має бути відсторонений від роботи до завершення розслідування інциденту.

Політика резервного копіювання

Політика використовується для встановлення порядку резервного копіювання та зберігання копій, для наступного відновлення працездатності ІТС

при її частковому або повному пошкодженні, що може бути викликане збоями, чи пошкодженням апаратного або програмного забезпечення, при помилках користувачів та будь-якими надзвичайними обставинами. Відновлення має проводитись при необхідності.

Сфера застосування

Політика поширюється на всіх працівників, що мають доступ до комп'ютерів у ІТС підприємства.

Інструкція політики

Для будь-якої інформації, що оброблюється працівниками, періодично повинна створюватися резервна копія. Носії резервного копіювання повинні зберігатися з захистом їх несанкціонованого копіювання та пошкодження. Частота резервного копіювання повинні відповідати важливості інформації, визначеним власником інформації.

Процес резервного копіювання, ситуації, при яких потрібне повне або часткове відновлення повинен бути задокументований та періодично переглядатися. Носії інформації, на яких буде знаходитися резервні копії інформації, повинні бути захищені так, як і інформація з найвищим рівнем конфіденційності. Резервні копії операційних систем та програмного забезпечення повинні зберігатися в том місці, що і програмне забезпечення ІТС. Рівень зберігання має бути таким, як і найбільш критична інформація. Для підтвердження надійності носія та цілісності інформації на ньому, резервна копія та інформація повинні періодично перевірятися.

Резервні копії даних повинні бути легко ідентифіковані за мітками або системою штрихового кодування:

- назва системи;
- класифікація;
- дата створення;
- відповідальний за її створення;

Відповідальність

Працівник, що порушив цю політику безпеки, повинен зазнати дисциплінарного стягнення аж до звільнення. Під час розслідування інциденту працівник має бути відсторонений від роботи до завершення розслідування інциденту.

Політика електронної пошти

Політика вводиться для забезпечення належного використання електронної пошти, електронного листування та передачі файлів. Політика визначає мінімальні вимоги щодо використання працівниками електронної пошти.

Сфера застосування

Ця політика охоплює будь-яке листування за допомогою електронної пошти працівниками від імені організації.

Інструкція політики

Використання електронної пошти повинно відповідати політиці підприємства, правилам інформаційної безпеки та правилам ділового листування. Адресу підприємства можна використовувати тільки для ділового листування. Особисте спілкування повинно бути обмеженим темами, що частково або повністю стосуються задач підприємства.

Усі дані, що надсилаються через електронну пошту, в тому числі файли, повинні бути захищенні відповідно до стандартів захисту даних. Електронна пошта зберігається та може бути створена її резервна копія тільки у тому разі, якщо вона визначається як діловий запис організації. Електронна пошта не повинна використовуватись для надсилання образливих повідомлень та повідомлень, що порушують ділову етику листування. Якщо працівник отримує електронний лист, що містить образи чи загрози, то в такому разі працівник повинен негайно повідомити про це керівництво. Працівникам заборонена автоматична переадресація електронних листів на будь-яку іншу електронну адресу. Пересилання повідомлень на іншу електронну адресу дозволяється тільки в тому разі, якщо інформація не містить конфіденційної інформації. Працівникам забороняється користування іншими системами електронної пошти, такими як

Google та схожими, від імені компанії. Працівникам забороняється користування іншими системами електронної пошти, такими як Google та схожими, для збереження електронної пошти організації. Всі операції та комунікації такого типу повинні проводитись через канали, що дозволені підприємством. Такі канали зв'язку повинні відповідати вимогам інформаційної безпеки.

Відповідальність

Працівник, що порушив цю політику безпеки, повинен зазнати дисциплінарного стягнення аж до звільнення. Під час розслідування інциденту працівник має бути відсторонений від роботи до завершення розслідування інциденту.

Політика утилізації технологічного обладнання

Будь-яке технологічне обладнання, таке як жорсткі диски, флеш-носії, компакт-диски та інші носії інформації, яке було застосоване для обробки або зберігання інформації містить інформації підприємства. Деяка інформація є конфіденційною. Щоб захистити конфіденційність інформації, перед утилізацією повинні бути очищені. Видалення або навіть форматування даних не вважається достатнім. Під час видалення файлів або форматування носія інформації дані позначаються для видалення, але вони все одно залишаються доступними поки файл не буде замінений іншим. Тому для надійного стирання даних перед утилізацією повинні використовуватись спеціальні інструменти.

Сфера застосування

Політика поширюється на все комп'ютерне обладнання та будь-які інші технологічне обладнання або периферійні пристрої, що виходять з користування підприємством.

До основних видів таких пристроїв відносяться:

- комп'ютери;
- сервери;
- жорсткі диски;
- ноутбуки;

- принтери;
- сканери;
- флеш-носії;
- компакт-диски;
- зовнішні жорсткі диски;
- мобільні телефони, що видані підприємством;
- планшети;

Всі працівники повинні дотримуватися цієї політики безпеки.

Інструкція політики

Причини, що можуть викликати необхідність утилізації обладнання:

- закінчення терміну використання обладнання;
- часткове пошкодження, що має критичний характер;
- повне пошкодження технічного обладнання;
- планове оновлення технічного обладнання;

Якщо, з наведених вище причин, технічне обладнання потребує утилізації, його треба утилізувати згідно до сучасних найкращих практик у галузі.

Рекомендацією до знищення даних компанії перед утилізацією технічного обладнання будуть такі кроки:

1) визначення типу інформації, що зберігалась на даному технічному носії інформації;
2) класифікація інформації;
3) резервне копіювання інформації;
4) порівняння інформації на технічному носії та інформації, що була збережена;
5) видалення інформації з носія;
6) шифрування всього носія інформації ефективним шифруванням, наприклад AES-2048, та знищенням ключів його дешифрування;
7) форматування носія інформації;
8) запис кожного блоку пам’яті нульовими блоками;
9) Запис кожного блоку пам’яті випадковими блоками;
10) повторити пункт 8 та 9 декілька разів;

11) фізичне знищення носія інформації.

Під час утилізації фізичного носія інформації треба вдосконалитись, що:

- у фізичному носії інформації не залишилось інших носіїв інформації, наприклад компакт-дисків;
- після очищення носія інформації, переносний носій інформації, на якому було ПЗ, що використовувалось для очищення, також був вийнятий з технічного пристрою зберігання інформації;

Відповідальність

Працівник, що порушив цю політику безпеки, повинен зазнати дисциплінарного стягнення аж до звільнення. Під час розслідування інциденту працівник має бути відсторонений від роботи до завершення розслідування інциденту.

Політика легального програмного забезпечення

Однією із найбільш небезпечних вад інформаційної безпеки є неліцензійне(піратське) програмне забезпечення. Так як програмне забезпечення, що не є ліцензованим, було модифіковано якимось хакером, то в середині ПЗ можуть знаходитись віруси, що будуть встановлені у ІТС підприємства при встановленні неліцензійного ПЗ.

Типи вірусів, що можуть бути встановлені з неліцензійним ПЗ:

- Stiller, вірус що викрадає дані автентифікації та відсилає їх зловмиснику;
- RAT, вірус що надає змогу контролювати хост;
- Crypter, вірус що шифрує дані на комп'ютері і не дає змогу їми користуватись через неможливість розшифрування;
- Rootkit, вірус що використовує вразливості ОС для збільшення привілеїв та отримання найвищого рівня доступу и виконання команд від імені системи

Часто віруси можуть бути збірних типів, і таким чином їх загроза для системи комп'ютеру та ІТС підприємства зростає.

Сфера застосування

Ця політика безпеки стосується системного адміністратора особливо, оскільки він зобов'язаний займатися встановленням ПЗ на робочі комп'ютери працівників підприємства, та всіх працівників, що працюють в ІТС підприємства.

Інструкція політики

Будь-яке програмне забезпечення, що встановлюється на комп'ютери в ІТС підприємства, має бути ліцензійним. В жодному разі не можна встановлювати неліцензійне ПЗ, якщо було виявлене неліцензійне ПЗ то про це треба негайно доповісти керівництву.

При завантаженні та встановленні програмного забезпечення з відкритим кодом та розповсюджується безоплатне, наприклад ПЗ з GitHub, треба перевірити на наявність відомих проблем і періодично перевіряти на наявність відомих вразливостей. За можливості самостійно перевіряти код. Використання ПЗ з відкритим кодом дозволяється тільки у виключних випадках.

Висновок до розділу 2

У другому розділі було виконано обстеження ОІД, а саме:

- класифіковано інформацію, що оброблюється підприємством;
- побудовано та проаналізовано модель порушника;

Спираючись на аналіз загроз була розроблена політика безпеки:

- політика антивірусного захисту;
- політика "чистого столу";
- політика електронної пошти;
- політика утилізації технологічного обладнання;

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Економічне обґрунтування доцільності впровадження політики безпеки інформації

Для економічного обґрунтування доцільності розробки політики безпеки інформації потрібно провести розрахунки, щоб визначити економічну ефективність використання основних результатів, які будуть отримані після розрахунків.

Економічна доцільність визначається:

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

3.1.1 Розрахунок суми витрат на розробку політики безпеки інформації.

Спочатку розраховується трудомісткість розробки політики безпеки інформації, для цього потрібно скласти час, який знадобиться для кожної робочої операції:

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}, \text{ годин, де}$$

- $t_{тз}$ - тривалість складання ТЗ на розробку ПБІ = 82 години;
- $t_{в}$ - тривалість розробки концепції безпеки інформації у організації = 48 годин;
- $t_{а}$ - тривалість процесу аналізу ризиків = 72 годин;
- $t_{вз}$ - тривалість визначення вимог заходів, методів та засобів захисту = 36 годин;
- $t_{озб}$ - тривалість виробу основних рішень з забезпечення БІ = 72 годин;
- $t_{овр}$ - тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організацій = 96 годин;
- $t_{д}$ - тривалість документального оформлення політики безпеки = 12 годин.

$$t = 82 + 48 + 72 + 36 + 72 + 96 + 12 = 418 \text{ годин.}$$

3.1.2 Розрахунок суми витрат на реалізацію політики безпеки інформації.

Сума витрат на розробку політики безпеки (*Крп*) складається з витрат на: Заробітну плату спеціаліста з кібербезпеки — *Ззп* = 7047 грн;

Вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації — Змч.

$$Крп = Ззп + Змч = 18410.28+4709.78 = 23120.07 \text{ грн}$$

Заробітна плата спеціаліста складається з основної та додаткової заробітної плати, соціальних виплат та визначається за формулою:

$$Ззп = t \cdot Зіб = 418 \cdot 44{,}04 = 18410.28 \text{ грн}$$

де t – загальна тривалість розробки політики безпеки інформації = 418 годин;

Зіб – середньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями = 7047 / 160 = 44,04 грн/годину.

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

$$Змч = t \cdot Смч = 418 * 2{,}6 = 4709.78 \text{ грн}$$

де t – трудомісткість підготовки документації на ПК, годин;

Смч – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = Р \cdot tнал \cdot Се + Ф_{зал} \cdot На / Fр + Клпз \cdot Напз / Fр = 11{,}26$$

де $Р$ – встановлена потужність ПК = 0,065 кВт;

$Се$ – тариф на електричну енергію = 1,68 грн/кВт·година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік = 63984 грн;

$Н_а$ – річна норма амортизації на ПК = 20% частки одиниці;

$Н_{апх}$ – річна норма амортизації на ліцензійне програмне забезпечення = 0,1 частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення = 79 980 грн;

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

Сума амортизації:

$$А = \frac{Ф_п - Ф_{лікв}}{Т}$$

де $Ф_п$ - первісна вартість = 79 980 грн

$Ф_{ліквід}$ - ліквідаційна = 0 грн

Т - термін корисної дії = 5 років

$$А = (79\ 980-0)/5=15996$$

Норма амортизації:

$$H_a = \frac{Ф_п - Ф_{ліквід}}{Ф_п \cdot T} \cdot 100\%$$

$$На = 20\%$$

$$Ф_{зал} = Ф_п - А = 63984грн$$

Програмний засіб	**Вартість, грн**
1С для 2 ПК	13 380
Windows 10 Enterprise для 12 ПК	51 600
Avast Business Pro для 12 ПК	15000
Загально	79 980

Відповідно до розроблених рекомендацій, планується використання ліцензійних програмних засобів, як вже встановлених, так і нових.

Розрахована вартість розробки політики безпеки інформації ***Крп*** є складовою одноразових капітальних витрат разом з витратами на придбання програмних засобів, які рекомендовані для використання.

Отже фіксована сума капітальних витрат на розробку політики безпеки інформації складає:

$$К = Крп + Кзпз + Кпз + Каз + Кнавч + Кн = 110700 \text{ грн.}$$

де *Кзпз* – вартість закупівель ліцензійного основного і додаткового програмного забезпечення (ПЗ), 79,98 тис. грн;

Крп – вартість розробки політики безпеки інформації, 23,12 тис. грн;

Каз – вартість закупівли апаратного забезпечення та допоміжних матеріалів, 0 тис. грн;

Кнавч – вартість витрати на навчання технічних фахівців і обслуговуючого персоналу = 7,6 тис. грн;

Кн – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, 0 тис. грн.

3.2.2 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$C = Св + Ск + Сак \text{ , грн.}$$

де Св - вартість відновлення й модернізації системи Св = 0;

Ск - витрати на керування системою в цілому;

Сак - витрати, викликані активністю користувачів системи інформаційної безпеки = Сак = 0 грн.

Витрати на керування системою інформаційної безпеки (Ск) складають:

$$Ск = Сн + Са + Сз + Сел + Со + Стос = 33510 \text{ грн}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються = Сн = 7600 грн.

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

$$Сз = Зосн + Здод, \text{ грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового. Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 7047 грн. Отже,

$$Сз = (7047 * 12) = 8597,34 \text{ грн.}$$

З 01.01.2019 р. Ставка ЄСВ для всіх категорій платників складає 22%.

$$Сєв = 8597,34*0,22 = 1891,41 \text{ грн}$$

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

$$Сел = Р \cdot Fр \cdot Це = 209,66 \text{ грн.},$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=0,065 кВт);

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

Це – тариф на електроенергію[20], (Це = 1,68 грн./кВт за годину).

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1%

$$Стос = К \cdot 1\% = 110700 * 0,01 = 1107 \text{ грн}$$

Річний фонд амортизаційних відрахувань: Са = К * 0,25

$$Са = 110700 * 0,25 = 27675,01 \text{ грн.}$$

Витрати на керування системою інформаційної безпеки визначаються:

$$Ск = Сн + Са + Сз + Сел + Со + Стос = 45189,02$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 45189,02 грн.

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.2.1 Оцінка величини збитку

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

Необхідні вихідні дані для розрахунку:

tп – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 5 годин;

tв – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 3 годин;

tви – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі 4 годин;

Зо – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 9500 грн./міс.;

Зс – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 10450 грн./міс.;

Чо – чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особа;

Чс – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 28 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 3,78 млн грн. у рік;

Пзч – вартість заміни устаткування або запасних частин, грн = 0;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 7.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U=Пп+Пв+V = 33607,12,$$

де Пп – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, 4987.5 грн;

Пв – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), 6811,93 грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, 21807,69 грн.

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

$$П_П = \frac{\sum Зс}{F} \cdot t_П \ ,$$

$$П_п = 4987.5 \text{ грн},$$

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

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

$$Пв = Пви + Ппв + Пзч,$$

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

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

Пзч – вартість заміни устаткування або запасних частин, грн.

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

$$Пви=\Sigma Зс/F* tви$$

$$Пви = 6650 \text{ грн.}$$

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

$$Пвп=\Sigma Зо/F* tв$$

$$Пвп = 161,93 \text{ грн.}$$

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

$$Пв = 6811,93 \text{ грн.}$$

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

$$V = \frac{O}{Fг} \cdot (t_П + t_В + t_{ВИ})$$

$$V = 21807,69 \text{ грн.}$$

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

$U = Пп + Пв + V = 33607,12$ грн.

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

$$B = \sum_i \sum_n U$$

B = 235250 грн.

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B * R - C$$

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

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці = 57%;

C – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

E = 88903,40

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

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

ROSI = E / K, частки одиниці

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

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

Коефіцієнт повернення інвестицій ROSI:

ROSI = 0.80

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

ROSI > (Nдеп – Nінф)/100,

де Nдеп – річна депозитна ставка, (23%);

Nінф – річний рівень інфляції, (14%).

Розрахункове значення коефіцієнта повернення інвестицій:

0,80 > (23 – 14)/100 = 0,80 > 0,09

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI}, \text{ років}$$

$T_o = 1/0,8 = 1,24$ роки.

Висновки до розділу 3

Розробка політики інформаційної безпеки для ПП «NewMed» є економічно доцільною, оскільки коефіцієнт повернення інвестицій ROSI складає 0,8, що означає отримання 0,8 грн. економічного ефекту на кожну гривню капітальних вкладень на розробку політики інформаційної безпеки підприємства. Отримане значення коефіцієнту повернення інвестицій значно вище дохідності альтернативного вкладення коштів. Термін окупності при цьому складатиме 1,24 роки (близько 15 місяців). Капітальні витрати складають 110700 грн.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було:

- проаналізовано сучасні загрози інформаційної безпеки, зокрема в сфері надання медичних послуг;
- обстежено ОІД;
- класифіковано інформацію, що оброблюється в ІТС підприємства;
- побудовано модель порушника;
- проаналізовано загрози інформаційної безпеки;;
- проведено розрахунки та доведено економічну доцільність впровадження політики інформаційної безпеки;

Отримані дані говорять про те, що впровадження політики безпеки інформації є доцільними.

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

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України «Про інформацію» від 02.10.1992 No 2657-XII // Відомості Верховної Ради України. - 1992. - No 48. [Електронний ресурс]. - Режим доступу https://zakon.rada.gov.ua/laws/show/2657-12 Класифікація “інформації в законодавстві України”.
2. Закон України “Про захист персональних даних” від 01.06.2010 No 2297-VI // Відомості Верховної Ради України. - 2010. - No 5. [Електронний ресурс]. - Режим доступу https://zakon.rada.gov.ua/laws/show/2297-17.
3. Закон України “Про доступ до публічної інформації” від 13.01.2011 No 2939-VI // Відомості Верховної Ради України. - 2011. - No 32. [Електронний ресурс]. - Режим доступу https://zakon.rada.gov.ua/laws/show/2939-17.
4. Закон України “Про захист інформації в інформаційно- телекомунікаційних системах” від 05.07.1994 No80-VI // Відомості Верховної Ради України. -
5. 1994. - No 80. [Електронний ресурс]. - Режим доступу http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
6. ДСТУ ISO/IEC 27002:2015 [Електронний ресурс] // ДСТУ. - 2015. - Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66911.
7. ДСТУ ISO/IEC 27005:2017 [Електронний ресурс] // ДСТУ. - 2017. - Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66912.
8. НД ТЗІ 3.7-003 - Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно - телекомунікаційній системі. - [Чинний від 08.11.2005] - К. : ДССЗЗІ, 2005. - No125 - (Нормативний документ системи технічного захисту інформації).
9. НД ТЗІ 1.4-001 - Типове положення про службу захисту інформації в автоматизованій системі. - [Чинний від 04.12.2000] - К. : ДСТСЗІ СБУ, 2000. - No53 - (Нормативний документ системи технічного захисту інформації).
10. НД ТЗІ 2.5-004 - Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. - [Чинний від 28.04.1999] - К. :

ДСТСЗІ СБУ, 1999. - No22 - (Нормативний документ системи технічного захисту інформації).

11. НД ТЗІ 2.5-005 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. - [Чинний від 28.04.2000] - К. : ДСТСЗІ СБУ, 2000. - No22- (Нормативний документ системи технічного захисту інформації).
12. НД ТЗІ 1.6-005 - Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. - [Чинний від 15.04.2013] - К. : ДССЗЗІ, 2013. - No125 - (Нормативний документ системи технічного захисту інформації).
13. Етапи створення КСЗІ [Електронний ресурс] - Режим доступу до ресурсу:http://www.vaas.gov.ua/news/zaxist-informacijnix-sistem-vazhlive-zavdannya-sogodennya/.
14. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека/Упоряд. Д. П. Пілова. – Дніпро: Національний технічний університет «Дніпровська політехніка», 2019.
15. Методичні рекомендації до виконання дипломних робіт (проектів) бакалаврів та магістрів спеціальностей 125 Кібербезпека / О.В. Герасіна, Д.С.Тимофєєв, О.В. Кручинін, Ю.А.Мілінчук – Дніпро: НТУ "ДП", 2020. – 47 с.
16. НД ТЗІ 2.5-004 - Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. - [Чинний від 28.04.1999] - К. : ДСТСЗІ СБУ, 1999. - No22 - (Нормативний документ системи технічного захисту інформації).
17. НД ТЗІ 2.5-005 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. - [Чинний від 28.04.2000] - К. : ДСТСЗІ СБУ, 2000. - No22- (Нормативний документ системи технічного захисту інформації).

18. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.2–004–99. – Київ: ДСТСЗІ СБ України, 1999. – 55 с.
19. Інформація щодо середньої заробітної плати спеціаліста з кібербезпеки. [Електронний ресурс]. - Режим доступу https://ua.trud.com/salary/2/67683.html
20. Актуальні ціни на електроенергію [Електронний ресурс]. - Режим доступу https://yasno.com.ua/b2c-tariffs
21. Ціна ліцензійної копії 1С [Електронний ресурс] https://www.softcom.ua/ru/1c/prices/
22. Конституція України [Електронний ресурс] – Режим доступу https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text
23. НД ТЗІ 3.6-001-2000 [Електронний ресурс]https://tzi.ua/ru/nd_tz_3.6-001-2000.html
24. НД ТЗІ 1.6-005-2013 [Електронний ресурс] https://tzi.com.ua/nd-tz-1.6-005-2013.html
25. НД ТЗІ 1.1-002-99 [Електронний ресурс] https://tzi.com.ua/downloads/1.1-002-99.pdf
26. НД ТЗІ 1.1-005-07 [Електронний ресурс] https://tzi.com.ua/nd-tz-1.1-005-07.html
27. НД ТЗІ 3.7-001-99 [Електронний ресурс] https://tzi.ua/ua/nd_tz_3.7-001-99.html
28. НД ТЗІ 3.7-003-2005 [Електронний ресурс] https://tzi.com.ua/downloads/3.7-003-2005.pdf
29. Кібератака WannaCry. [Електронний ресурс] https://ru.wikipedia.org/wiki/WannaCry
30. MS17-010 Eternalblue Описання вразливості [Електронний ресурс] https://ru.wikipedia.org/wiki/EternalBlue
31. Відношення АНБ США до розробки Eternalblue [Електронний ресурс] https://www.avast.com/c-eternalblue та [Електронний ресурс] https://en.wikipedia.org/wiki/EternalBlue
32. Windows 10 [Електронний ресурс] https://ru.wikipedia.org/wiki/Windows_10

33. Стандарт ISO/IEC 27000 [Електронний ресурс] https://www.iso.org/ru/standard/73906.html
34. НД ТЗІ 2.5-005-99 [Електронний ресурс] https://tzi.ua/ua/nd_tz_2.5-005-99.html

Додаток А. Матеріали на електронному носії

Кваліфікаційна робота – Трубка Д.А. 125-17-1.docx

Презентація-Трубка Д.А.pptx

ДОДАТОК Б Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-17-1

Трубки Дениса Андрійовича

на тему: «Політика безпеки в інформаційно- телекомунікаційній системі комунального підприемства ‘NewMed’»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на_____сторінках.

Метою кваліфікаційної роботи є забезпечення деталізованої та актуалізованої ідентифікації інформаційних активів об`єктів захисту.

Тема кваліфікаційної роботи безпосередньо пов’язана з об’єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз нормативно-правової бази у сфері забезпечення кібербезпеки; аналіз організаційно-документаційного забезпечення ідентифікації інформаційних активів; аналіз автоматизованих засобів збору інформації; визначення основних характеристик для класифікації інформаційних активів. Розроблено рекомендації для проведення ідентифікації інформаційних активів.

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні ефективності процесу ідентифікації інформаційних активів, за рахунок розробки рекомендацій для проведення ідентифікації.

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

За час дипломування Трубка Д.А. 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

Керівник спец. розділу

Додаток В. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	1	
4	А4	1 Розділ	8	
5	А4	2 Розділ	38	
6	А4	3 Розділ	13	
7	А4	Висновки	1	
8	А4	Перелік посилань	2	
9	А4	Додаток А	1	
12	А4	Додаток Б	1	
13	А4	Додаток В	1	

Додаток Г Відгук керівника економічного розділу

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Підпис керівника економічного розділу _____