Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: «Розробка та впровадження комплексної системи захисту інформації в корпоративному середовищі».

Виконав: студент (ка)
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Заблоцький Віталій Валерійович
підпис (прізвище та ініціали)

Керівник Кульчицький Т.Р.
підпис (прізвище та ініціали)

Нормоконтроль Тимощук Д.І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент Шимчук Г.В.
підпис (прізвище та ініціали)

м. Тернопіль – 2023

АНОТАЦІЯ

«Розробка та впровадження комплексної системи захисту інформації в корпоративному середовищі» // Дипломна робота освітнього рівня «Бакалавр» //Заблоцький Віталій Валерійович// Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-42 // Тернопіль 2024 // С. 57 , рис. - 11, табл, - 2, додат. – , бібліогр. – 24.

Ключові слова: КСЗІ,ДСК, СЗІ, ІзОД, ПІДСИСТЕМА.

У роботі досліджено питання реалізації та встановлення комплексної системи захисту інформації на підприємстві, фактори впливу на таку підсистему та можливість здійснення заходів, щодо унеможливлення втручання у її роботу.

Оснащення і модернізація технологій на підприємствах створють постійний ризик втручання людського фактору в роботу системи захисту інформації

Основна увага у роботі присвячена використанню профілю безпеки, інженерно-технічних заходів, та також обраних стратегій розвитку систем захисту інформації. Проаналізовані функціональні можливості та засоби безпеки.

Результати даної роботи допоможуть підвищити розуміння процесів, котрі необхідні для створення систем захисту інформації, при обранні окремих стратегій, впровадження рекомендації щодо поліпшення систем захисту інформації, при автентифікації та авторизації.

Кваліфікаційна робота може бути корисною для організацій, які використовують або планують використовувати такі системи захисту інформації та допоможуть виявляти ризики безпеки профілю для користувачів.

ANNOTATION

"Development and Implementation of a Comprehensive Information Protection System in a Corporate Eenvironment" Thesis of the educational level "Bachelor" //Vitaliy Valeriyovych Zablotskyi// Ternopil National Technical University named after Ivan Pulyuy, Faculty of Computer Information Systems and Software Engineering, Cyber Security Department, SBs Group - 42 // Ternopil 2024 // P.57, fig. - 11, tabl – 2 add. – , bibliography - 24.

Keywords: KSZI, DSK, SZI, IzOD, SUBSYSTEM.

The study investigates the implementation and establishment of a comprehensive information protection system within an enterprise, the factors influencing such a subsystem, and the feasibility of measures to prevent interference with its operation.

The equipment and modernization of technologies in enterprises create a constant risk of human factor interference in the operation of the information protection system.

The primary focus of the study is on the use of security profiles, engineering and technical measures, and selected development strategies for information protection systems. The functional capabilities and security measures are analyzed.

The results of this work will help to enhance understanding of the processes necessary for creating information protection systems when choosing specific strategies and implementing recommendations for improving information protection systems during authentication and authorization.

This qualification work can be useful for organizations that use or plan to use such information protection systems and will help identify security risks for user profiles.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

БД – база даних;

ЕОМ – електронно-обчислювальна машина;

ІД – інформаційна діяльність;

ІзОД – інформація з обмеженим доступом;

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;

ОС – обчислювальна система;

ОТЗ – основні технічні засоби;

ПЗ – програмне забезпечення;

ДСК- для службового використання

ЗІ - засоби захисту інформації

ВСТУП

У сучасному світі інформаційних технологій розвиток комп'ютерних технологій швидкий і приносить значні зміни у наше повсякденне життя. Інформація стає товаром, з яким проводять операції обміну, продажу та покупки. Часто вартість інформації перевищує вартість самої комп'ютерної системи, де вона зберігається. Паперові документи поступово замінюються електронними. Для обробки цієї інформації потрібні системи, які забезпечують необхідний захист даних, оскільки їх вразливість може бути використана проти власників. Безпека комп'ютерних систем досягається через забезпечення конфіденційності, цілісності та доступності даних, а також доступності та цілісності інформаційних компонентів і ресурсів системи. Багато організацій не знають, як почати захист конфіденційної інформації.

Класифікування типів інформації за значенням та конфіденційністю допомагає компаніям визначити пріоритети та почати захист з найважливіших даних. Це може бути системна інформація про клієнтів або навчальні записи співробітників. Серед них можуть бути номери соціального страхування, номери рахунків, ідентифікаційні номери, номери кредитних карток та інші типи структурованої інформації, які потрібно захищати. Захист неструктурованої інформації, такої як контракти, фінансові звіти та переписка з клієнтами, є важливим наступним кроком, який виконується на рівні відділів.

Оскільки захист інформації є одним з найважливіших аспектів для будь-якого підприємства та є першочерговим у збереженні даних, наявна проблематика в розробці комплексних заходів для створення Комплексних Систем Захисту Інформації (КСЗІ). Це обумовлено необхідністю як організаційної, так і інженерно-технічної підготовки, що в свою чергу породжує нові проблеми у впровадженні комплексних та організаційних підходів до створення систем та методів організації захисту інформації. Необхідність формування комплексних систем захисту інформації чітко визначена у нормативно-правових актах України, оскільки саме комплексна система захисту інформації забезпечує виконання таких вимог, як доступ до публічної інформації та захист персональних даних. Тому впровадження нових комплексів заходів, як організаційно-правового, так і інженерно-технічного характеру, є необхідним для виконання встановлених законодавством вимог,

збереження персональних даних та відповідності конвенції "Про захист прав людини".

Метою даної роботи є висвітлення та аналіз методик впровадження комплексних заходів захисту інформації на підприємствах, а також у розгляді проблем, що виникають під час їх застосування.

Відповідно по поставленої мети нами були сформовані завдання:

– Дослідження стратегій впровадження КСЗІ;

– Оцінка та методика впровадження КСЗІ на підприємствах та установах.

Об’єктом дослідження виступає комплексна система захисту інформації в органі місцевого самоврядування та програмні засоби необхідні для її функціювання.

Практична цінність: аналіз використання комплексної системи захисту інформації дозволить виявити її вразливі сторони та впровадити нові методи для створення стійкого середовища захисту інформаційних ресурсів у Великоберезовицькій селищній раді. Представлення пропозицій для покращення роботи органу місцевого самоврядування дозволить підвищити ефективність його діяльності.

Методи дослідження: у даній роботі було використано такі методи дослідження, зокрема емпіричний аналіз, діалектичний метод та системний підхід також застосовувались структурний та порівняльний метод, для отримання глибшого розуміння сутності та функціювання комплексних систем захисту інформації.

Проблематика впровадження комплексних систем захисту інформації була предметом дослідження різних авторів: В.Борисов, О.Гарань, О.Горбань, Е.Сноуден, Г.Мінцберг.

Кваліфікаційна робота включає в себе вступ, чотири розділи , висновок та використанні джерела, де розглядаються основні принципи роботи комплексних систем захисту інформації, інформацію з обмеженим доступом, програмні забезпечення необхідні для їх впровадження.

РОЗДІЛ 1. ЗАГАЛЬНІ ПОЛОЖЕННЯ ПРО КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

1.1. Основні підходи до створення комплексної системи захисту інформації.

У сучасному світі існують подвійні стандарти стосовно аспектів та підходів до проблематики захисту інформації, що збирається та обробляється людиною, за допомогою автоматизованих систем чи електронно обчислювальних машин. Інколи ці твердження стосуються виключно комп’ютерних технологій та пристроїв, які займаються обробкою та систематизацією інформації. Враховуючи стрімкий розвиток технологій на сьогоднішній день існують великі ризики втрати цілісності, конфіденційності чи обмеження доступу до попередньо або слабо захищеної інформації. Розвиток технологій і розширення їх можливостей, призводить до зростання кількості загроз.

На сьогоднішній день інформація, яка зберігається в одному місці чи на одному джерелі, являє собою єдиний комплекс компонентів відомостей, пов'язаних спільним завданням у захисті персональних даних, інформації, дій та ін. потребує поглибленого погляду на захист.

На сучасних підприємствах стрімкий технологічний розвиток значно скоротив їхні можливості, необхідні для створення комплексу інформаційної безпеки, що передує зменшенню людських ресурсів, які використовуються для зберігання та захисту інформації на підприємстві.

Різноманітність інформації, що використовується в сучасну епоху, не може бути чітко оцінена в кількісних показниках, оскільки такі підсистеми є складними і тому не мають чітких критеріїв, а самі системи захисту можуть багатокомпонентними і досягати багатьох цілей в залежності від обсягу і потужності їх ресурсів.

Така система характеризується, по-перше, наявністю людини в кожній з її складових підсистем, адже основним носієм інформації в незалежності від епохи була людина як складова системи інформації, а саме створювача об’єктів інформації. Це пов’язано тим, що багато компонентів, з яких складається об'єкт інформатизації, можуть бути інтегровано представлена наступним набором з трьох різних системних груп, а саме біологічного чиннику людського, адже інформація не має формату

самовідтворення, створення та реалізації. Певні частини інформації являються додатковим ресурсом у діяльності людини і виконують функцію вторинного елементу, що забезпечує функціонування та створення окремих похідних необхідних для проведення людської діяльності.

З огляду на це слід звернути увагу на декілька періодів розвитку засобів захисту інформації, що наведенні на рисунку 1.1.

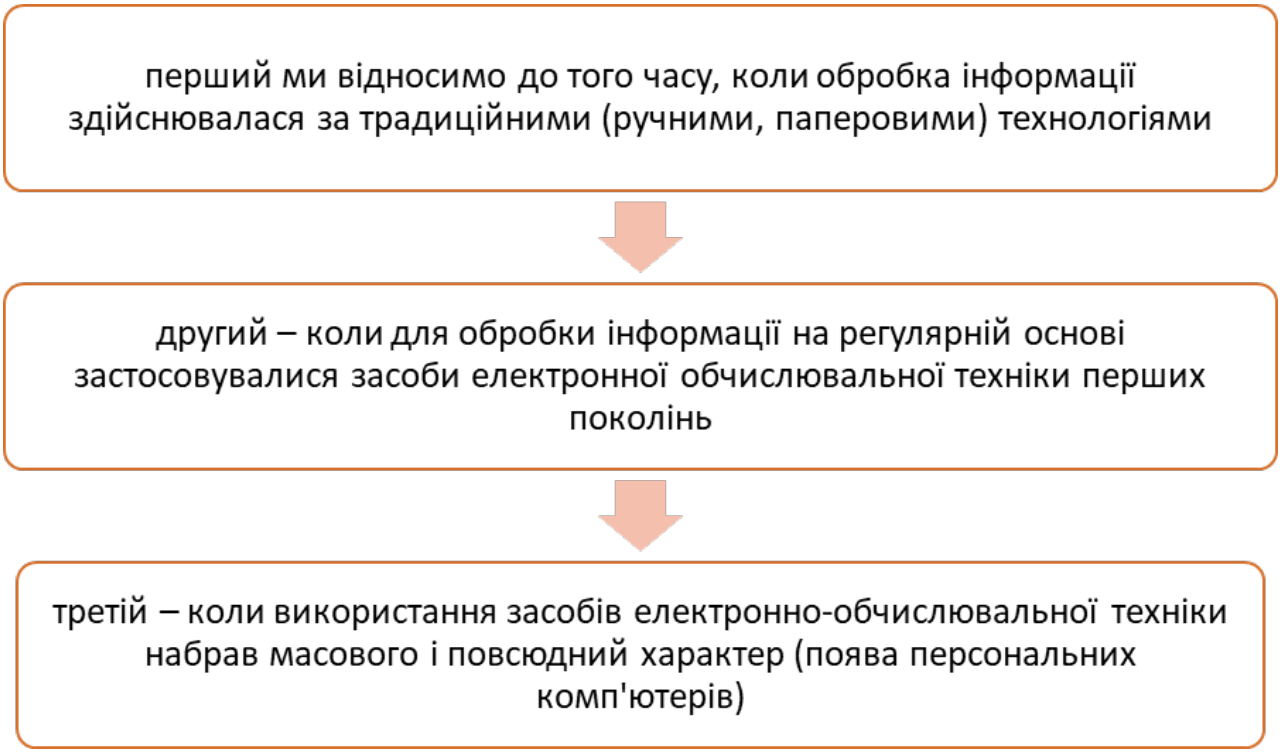

Рисунок 1.1 – періоди розвитку ЗІ

Поділ інформації, способи її аналітики, загострило ситуацію в людських відносинах адже на початку 60-тих, безпосередньо інформація, як із здебільшого в сучасному світі відігравала роль зброї, шляхом використання її як пропаганди, так і отримання інформації про інші цілі ворогуючої сторони, що в подальшому призвело до розвитку комплексних систем захисту такої інформації.

Базисні моделі сучасних суб’єктів господарювання та підприємництва вимушені використовувати складну модель захисту інформації системи, в рамках якої здійснюється ЗІ, адже складність структури підприємства створює необхідні вимоги щодо формування комплексних підсистем заходів організації збору обробки та поширення інформації в ресурсних розрахунках.

Слід розуміти сучасні особливості суб'єктів господарювання в момент використання інформації серед яких є основні та побічні, вони формують єдину базисну модель, яка відображення на рисунку 1.2

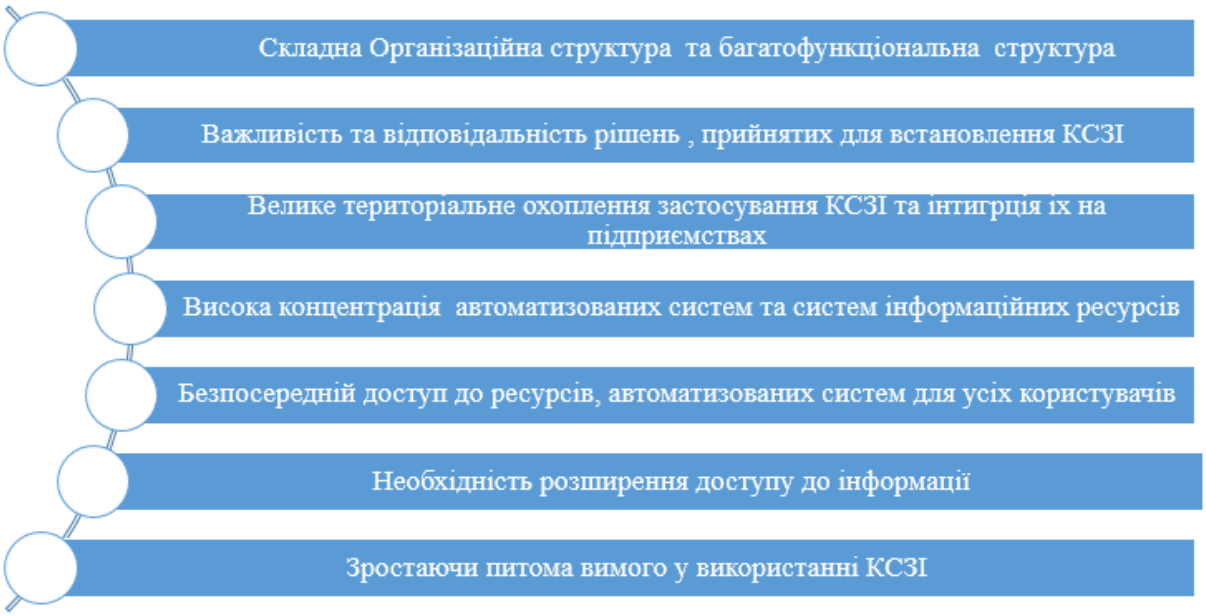

Рисунок 1.2 - Базисна модель використання інформації на підприємствах

Отже створення інформації та її обробка є прямою необхідністю для підприємства, адже інтенсивність циркуляції інформації в сучасних веб ресурсах та застосунках, потребує більш вагоміших внесків, як для захисту такої інформації від її спотворювачі в частинні зміни та перефразування, так і з метою встановлення дій спрямованих на збереження такої великої кількості інформації в автоматизованих системах, за умови придатності їх до використання великої кількості людей, а також формувань єдиних відкритих джерел баз даних, що в свою чергую не тільки запобігаю ризикам інформаційного впливу, а також і формує цілісну систему функціонування інформації задля розвитку суспільних інтересів. [6 с.7].

У зв'язку з вторгненням збройних сил російської федерації в Україну, комплексні системи захисту інформації на підприємствах критичної інфраструктури, обласних та міських радах, потребує особливої уваги. Спроби ворога здійснити отримання інформації із ресурсів, які йому не доступні, стало поштовхом для створення нових більш потужних комплексів підходів, як організаційних так і інженерно-технічних заходів, з метою недопущення поршень функцій держави через DOS–атаки.

Слід зазначити, що Україна є чи не однією із країн лідерів у системі захисту інформації, даний досвід отримано не тільки за допомогою іноземних партнерів, перейняттю досвіду та новітніх технологій, а за рахунок постійного досвіду у проведенні заходів, щодо боротьби із порушниками, які здійснюють постійні атаки з метою отримання інформації із систем, до яких є встановлення обмеженого доступу.

Основним напрямком на сьогодні являєтеся не тільки створення оновлених механізмі захисту інформації, а забезпечення надійного захисту інформації в основних кореневих системах, які надають можливість ідентифікувати осіб.

Такий вид заходів є першочерговий та формує основоположну модель вирішення проблеми необхідності виключення людини із ресурсу збереження інформації, мінімізуватиме вплив людського чинника, а також створює можливості мінімізації незручностей у пошуку, створенні та використанні інформації із відкритих джерел, що в подальшому, мінімізує можливість сукупність використання різних базисних модель засобів захисту інформації та приведе до використання відповідними суб'єктами більш складних форм індивідуального захисту інформації. [6].

Дані дії не можливі без розроблення загальної концепції складових, необхідних для створення комплексної системи захисту інформації, а найбільш оптимальним заходом, що має цьому передувати, являється саме вивчення предмету загроз які можуть порушувати функції систем організації засобів захисту інформації на основі теоретичних та інших прикладах.

Ці всі чинники слід аналізувати та усувати разом із первинними проблемами реалізації систем захисту інформації які наведенні в рисунку 1.3

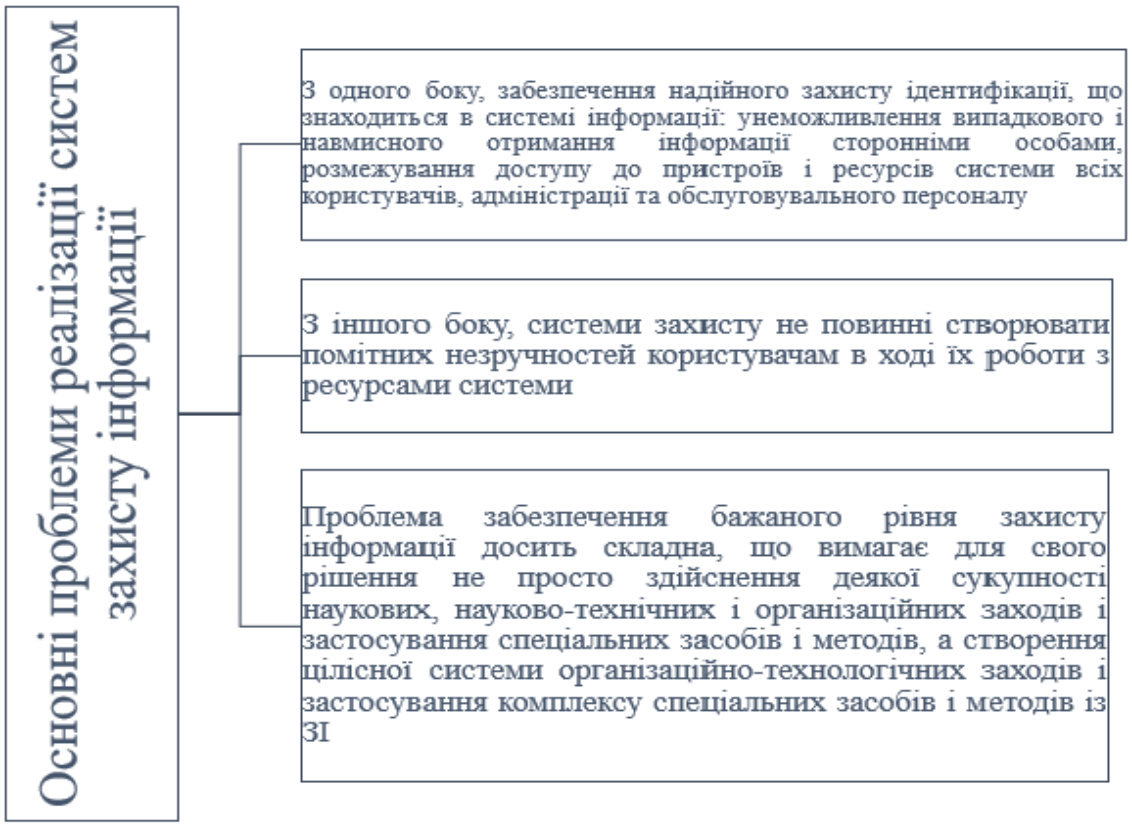

Рисунок 1.3 – Основні проблеми реалізації ЗІ

Проте слід зазначити що такі підходи в подальшому не повинні створювати незручності користувачеві при використанні джерел інформації.

Проблематикою формування систем захисту складає саме відсутність єдиної системи вимоги щодо захисту такої інформації у веб просторі, що в подальшому створює проблему у розвитку інженерно-технічних засобів захисту інформації.

За основу теоретичних і базисних моделей захисту інформації створили інші частини етапу формування захисту інформації.

Під системністю як основною частиною системно-концептуального походу розуміється:

– Цілеспрямована систематизація та інформаційна безпека визнані важливою частиною загальної концепції якості інформації;

– Просторові системи, які забезпечують взаємопов'язані рішення всіх проблем безпеки в усіх компонентах підприємства.;

– Тимчасова узгодженість. Тобто безперервність робіт, пов'язаних із ЗІЗ, що виконуються відповідно до плану.;

– Організаційна систематизація означає одноманітність в організації та управлінні всією діяльністю у сфері ІТ.

Концепція таких методів та дій здійснює подальший вплив на розробку єдиних телекомунікаційних системи, і створює новітні рішення в оптимізації організації діяльності робіт та послуг пов’язаних із розробкою систем захисту інформації, безпеки профілю та інших дій спрямованих на організації КСЗІ.

Комплексний (системний) підхід до створення системи включає в себе, перш за все, вивчення предмету системи, яка буде впроваджуватися, оцінку загроз безпеці предмету, аналіз засобів, які будуть використовуватися для створення системи, оцінку її економічної доцільності, вивчення самої системи, її характеристик, принципів функціонування та підвищення ефективності Це включає в себе саму систему, її характеристики, принципи функціонування та потенціал для підвищення її ефективності. [17].

Сюди входить взаємозалежність усіх внутрішніх і зовнішніх факторів, можливість подальших змін у процесі побудови системи та повна організація всього процесу від початку до кінця.

Інтегративний(системний) підхід- як принцип проведення експертиз проектів, базисного формування системи , який здійснює систематичний і повний аналіз рівня безпеки системи. Цей підхід є опційним оскільки здійснення покращення показників чи параметрів в одному вузлів захисту інформації, призводить до погіршення інших функцій системи, а намагання збалансування протиріччя вимог модулів захисту призводить до пониження рівня безпеки такого ЗІ та зменшує характеристики позитивних функцій системи.

Це також спричинено складністю структури підприємства оскільки різноманіття загроз може випливати від кількості потенційних учасників, підсистеми відповідальної за захист інформації на підприємстві.

1.2 Основні задачі комплексної системи захисту інформації

Щодо формування стратегії захисту інформації слід враховувати загальну спрямованість такої підсистеми, для вирахування потреба та інших об’єктивних чинників.

Серед усіх дослідників у сфер і стратегічного управління слід відзначити Генрі Мінцберга, який створив свою базисну модель (план) системи захисту «5-Р». він виражає її в наступних пунктах зображених на рисунку 1.4.

Рисунок 1.4 – Базисна модель Генрі Мінцберга

Серед однорідних завдань стратегії є саме фактично створення, найбільш сприятливих умов, задля зменшення нестабільності середовища підсистеми, а також задля вирівняння можливостей конкурентоспроможності, через етапність формувань таких стратегій випливають також чинники, з якими організація стикаєтеся щоденно, які відіграють роль у подальшому розвитку систем захисту інформації.

Основоположним значенням являєтеся те, що стратегія формується в незалежності від одного фактору, а від впливу чинників навколишнього та зовнішнього середовища.

На думку Б. Карлоффа, одного з провідних експертів у Європі та США, «Фактори мають специфічні властивості, які впливають на стратегію будь-якої організації» До таких факторів відображені у рисунку 1.5.

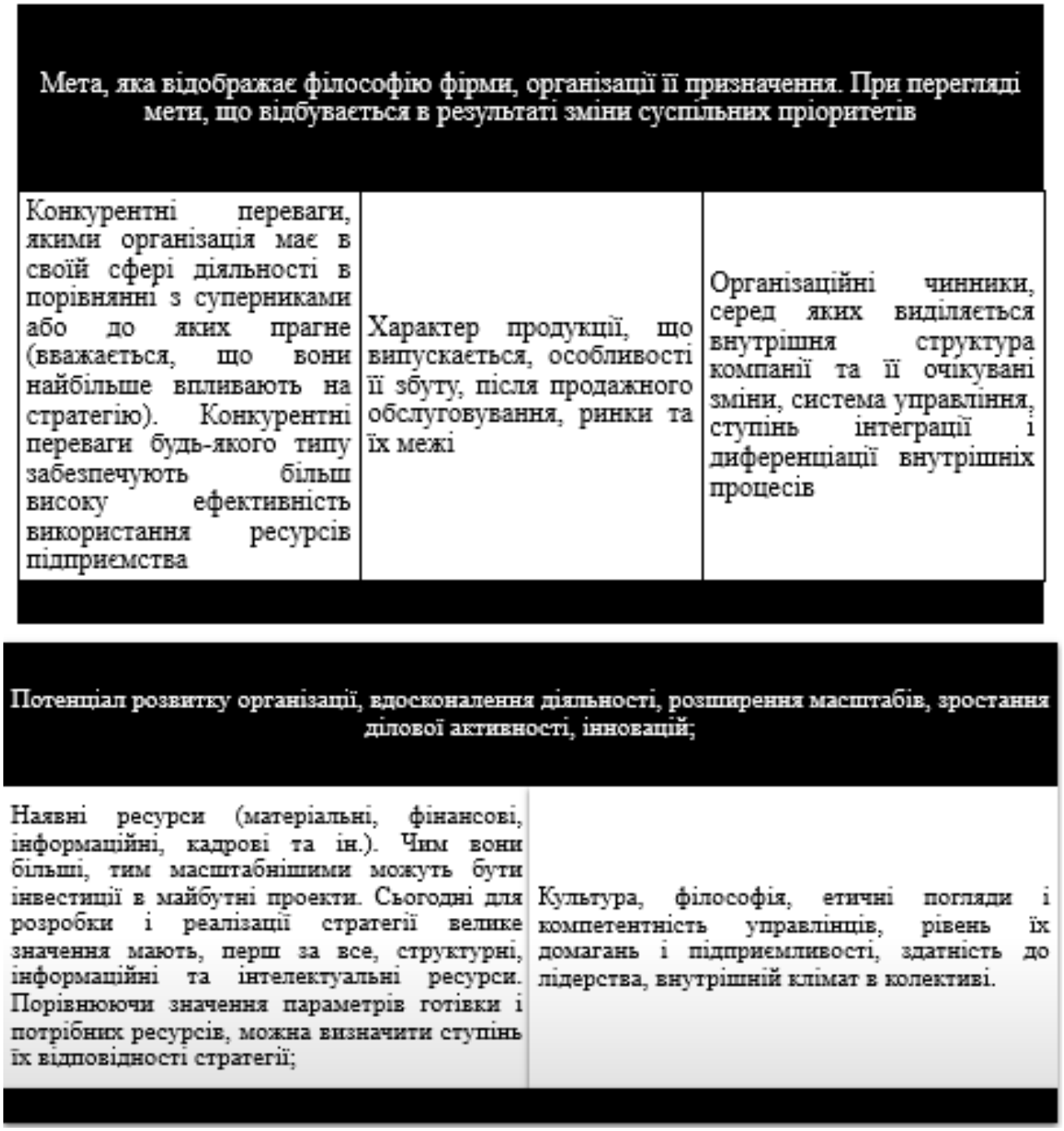

Рисунок 1.5 – Фактори та потенціал розвитку за Б. Карлоффа

Щодо стратегічного впливу то перш за все слід розібрати комплекси існуючих ризиків, серед яких слід включати інші аспекти, такі, як:

– ризик впливу людського фактору;

– ризик порушення регламенту;

– ризик зміну соціальної структури відповідального за КСЗІ структурного органу.

Слід врахувати деякі особливості стратегій рішень. Вони поділяються за фактом регламентованості і можуть належати до таких, що надають чи обмежують широкі можливості для виконавця стосовно тактики та свободи, або ж обмежуються директивами.

В частині поділу на функціональні призначення стратегічні рішення найчастіше являють собою організаційні або адміністративні методи виконання певної проблематики.

Із погляду визначення кращої практики, дані рішення повинні мати систематичний, математичний та програмний характер, і як правило вони формуються при вирішенні нестандартних обставинах.

З точки зору важливості та суттєвості ці рішення є фундаментальними і визначають основні шляхи вирішення головних проблем і напрямів діяльності компанії та розвитку компанії в цілому і окремих секторів і сфер діяльності в довгостроковій перспективі (не менше 5-10 років). [23].

Стратегічні рішення зумовлені здебільшого зовнішніми, а не внутрішніми умовами і повинні враховувати тенденції розвитку ситуації та інтереси багатьох зацікавлених сторін, вони практично незворотні і тому потребують ретельної та всебічної підготовки окрім того за своєю природою вони є складні тобто це, як правило, не одне рішення, а низка взаємопов'язаних рішень, об'єднаних спільними цілями і скоординованих за ототожненням та ресурсами. Такі рішення визначають пріоритети і напрямок розвитку компанії ,її майбутній потенціал, ринок і способи реагування на непередбачувані події. На практиці сформувалися такі вимоги до прийняття стратегічних рішень, які зображенні на рисунку 1.6.

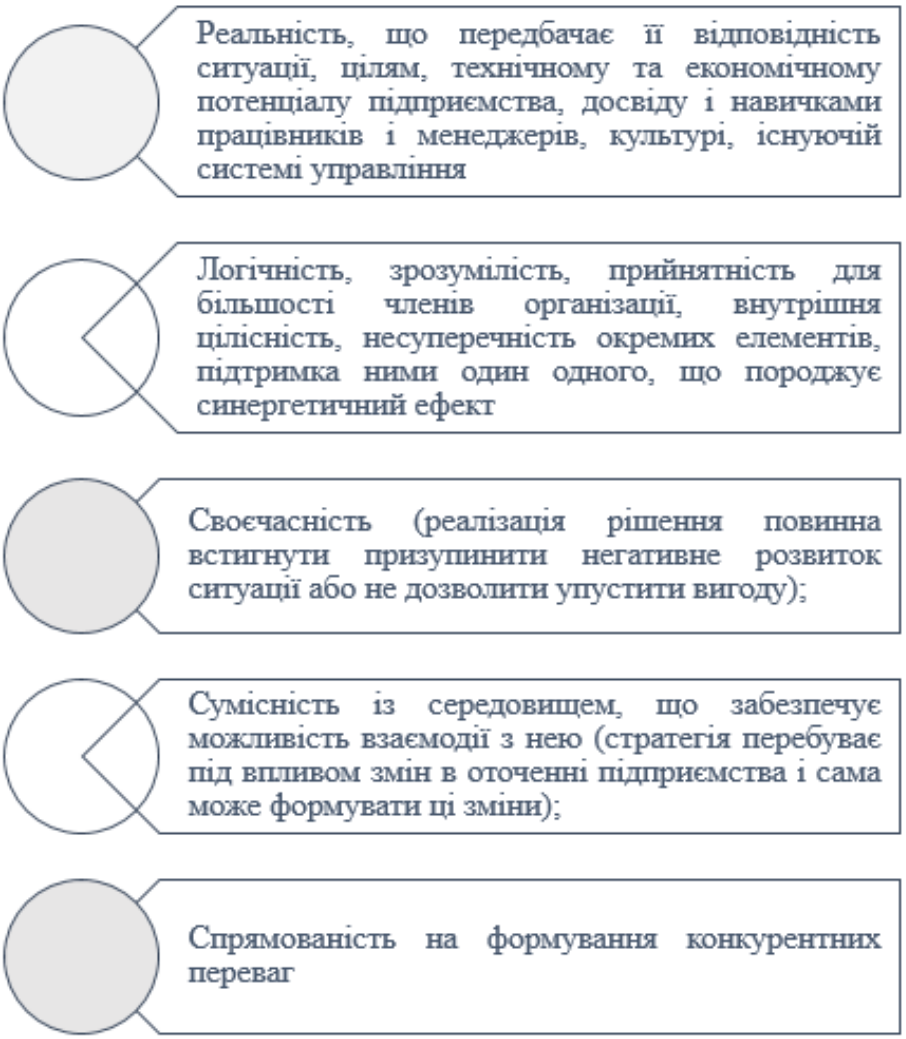

Рисунок 1.6 – Вимоги до прийняття стратегічних рішень

Здійснення заходів а також фактичного створення та формування організаційно технічної системи, повинна дотримуватись однойменних принципів, а саме принципу фундаментального аналізу та підбору, які будуть виражатись, діями та в чинками, характеризованими на підбір інформації, її попереднє формування, а протокол формування такого підбору повинен взаємодіяти із комплексом захисту, з метою недопущення формування логічних помилок.

Як правило до таких дій та заходів повинно належати:

– Формування та ототожнення конкретних помилок;

– Оперативна зміна і реагування на формування структури організації відділу чи підприємства в цілому ;

– –Вирахування окремих елементів реагування на проблематику з якою з стикаєтеся суб’єкт господарювання ;

– Створення сприятливих умов праці та середовища на підприємстві для керівного персоналу та інших посад відповідальних за створення технічної системи.

Окремими позиціями створення рішень стратегічного характеру, являєтеся саме здійснення формування основоположних завдань, які суб'єкт господарювання повинен при своїй діяльності набути у майбутньому. В подальшому результаті це дозволить створювати обирати та формувати кращі варіації підходів, а також створить нові стратегії оцінювання. [5].

Методичних рекомендацій для створення підходів формування стратегій не існує. Кожен фактор формує власну обставину та потребу у створенні нової системи захисту, яка може за умови існування інших впливів не спрацювати, що унеможливлює створення одного ситуаційного підходу.

Із врахуванням широкого розмаїття ситуацій, в яких необхідний захист інформації, загальна мета при вирішенні стратегічних питань полягала в тому, щоб розробити ряд стратегій захисту і вибрати мінімальний набір, який забезпечить розумний захист в кожній конкретній ситуації.

Загальними факторами захисту слід виділяти три стратегії захисту:

– оборонна – це первинна і фактична стратегія захист, котра працює автономно за запрограмованим алгоритмом ;

– наступальна – це стратегія котра унеможливлює можливість поширення потенційних загроз при формування первинних блочних кодів і варіацій системи, за допомогою врахування умов продуктивності системи та її структури;

– попереджувальна – це стратегія, формування якої забезпечує мінімізацію, або ж і виключення можливості порушення протоколу захисту у підсистемі..

Чи не єдиними фактором для забезпечення захисту інформації являєтеся і сама система розробки політики безпеки, як стратегії так і процесу розподілу критичної інформації в системі.

Політика безпеки здійснює важливу роль у особливостях процесу збору, поширення та обробки інформації. Це відображається шляхом аналізу організаційно-підготовчих заходів, до формування структури захисту інформації та її безпеки, адже для конкретної стратегії формування політики безпеки повинні враховуватись інформаційні новинки, конкретні технології формування обробки та захисту

інформації, індивідуальні програми розташування інформації та індивідуальні технічні засоби поширення інформації в веб ресурсі.

Політика безпеки організації встановлює вимоги до надання суб'єктам (користувачам) прав на використання підсистем і функцій над ними та покладає на них відповідальність за безпечну роботу підсистем. Система інформаційної безпеки є ефективною, якщо вона надійно підтримує виконання правил політики безпеки і навпаки. Етапи створення політики безпеки підприємства полягають у додаванні структури цінностей до визначення об'єкта та аналізу ризиків і визначенні правил з цією структурою цінностей для всіх процесів, які використовують доступ до ресурсів об'єктів автоматизації. Перш за все, необхідно детально визначити загальну мету створення системи безпеки організації. Існує ряд факторів, які є основою для визначення вимог до системи (і вибору альтернатив). Фактори безпеки можна розділити на правові, технічні, технологічні та організаційні відповідно. [6].

Розробка політики безпеки організації, як частини організаційного спрямування так і інженерно-технічної її частини є викликом для суб’єкта формування безпеки оскільки існують чинники та ризики, які перешкоджають цьому, серед них розглянемо найпростіші :

– Складність технологій: Швидкий темп розвитку технологій ускладнює завдання захисту інформації. Зловмисники постійно шукають нові способи атаки, що вимагає постійного оновлення стратегій і політики безпеки.

– Різноманітність загроз: Інформаційна безпека стикається з різноманітними загрозами, включаючи хакерські атаки, внутрішні проблеми безпеки, фізичні загрози та соціальні інженерні атаки. Врахування всіх цих аспектів у політиці безпеки важливо, але це також ускладнює процес створення.

– Культурні виклики: Політика безпеки повинна враховувати культурні особливості організації. Наприклад, різні галузі можуть мати різні стандарти безпеки, а також різні рівні чутливості до безпекових питань.

– Співпраця та координація: Врахування і врахування різноманітних відділів та структур в організації може бути складним завданням. Часто важливо забезпечити співпрацю між відділами IT, юридичними службами, внутрішніми аудиторами та іншими зацікавленими сторонами для розробки комплексної політики безпеки.

-Законодавчі вимоги: Багато організацій повинні відповідати законодавчим вимогам, які стосуються безпеки інформації. Розробка політики безпеки, яка відповідає цим вимогам, може бути складним завданням через технічну та юридичну складність вимог.

У сучасному світі слід виділяти наступні комплекси заходів та дій пов’язаних із політикою безпеки:

1. Комплекс заходів, пов'язаних з проведенням аналізу ризиків. До цієї групи можна віднести:

– склад матеріально-технічного забезпечення та цінностей;

– створення базисної моделі ліквідації практичної загрози;

– комплексна проектна документація, та експертиза ризиків захисту інформації, формування нових протоколів безпеки.

2. Заходи пов’язанні із забезпеченням аналізу підсистем обробки інформації, на стадії перевірки профілю користувача.

3. Аналіз фактичних етапів формування структури захисту інформації.

4. Обробка статистичних звітів про безпеку та аналоговість збору, обробки, поширення інформації та її роль на безпеку інформації.

Тезисними основами є безпеки профілю захисту інформації є варіації входу, а також варіації протокольності ведення та використання профілю відповідального за інформаційний збір даних про рух інформації в застосунку, чи веб ресурсі. [8].

Математична модель необхідна для аналізу початкової готовності підсистеми, щоб встановити фактичні характеристики та проаналізувати прогресивні дії.

Аналіз таких моделей повинен містити інформації та сукупний набір можливих ризиків, про перехід системи, у стан безпечної чи небезпечної,, а також надавати якісну оцінку безпеки профілю чи комплексу захисту інформації обраний підприємством, а також враховувати внесок управління в розвиток системи, що в подальшому убезпечить від непередбачуваних витрат.

Основним твердження при такому розрахунку та урахування факторів є саме те, що при використанні чи розробці стратегій, моделей та інших дій спрямованих на розвиток системи безпеки захисту інформації являєтеся саме використання математичних методів, серед яких профільне використання моделювання генерованих алгоритмів, аналіз на можливість втручання ШІ.

Тому при врахуванні фактів порушення політики безпеки чинників людського примусу і умислу слід формувати твердження, що протоколи, і алгоритми захисту інформації, які є нічим іншим, як частинами стратегії розвитку безпеки профілю захисту інформації, являються чи не першочерговими заходами організаційного характеру, і які потребують постійного вивчення, адже у своїй частинні і в частинні структури захисту інформації являються підґрунтям для проведення інженерно-технічних завдання захисту інформації.

РОЗДІЛ 2. ЗАХОДИ ЗАХИСТУ ІНФОРМАЦІЇ

2.1. Основні принципи організації КСЗІ їх вплив на захист

Інженерно-технічні заходи – є частинною формування комплексу системи захисту інформації, значна кількість яких спрямування на здійснення заходів моделювання, автоматичного аналізу, використання інформації, та чинників втручання людського фактору у роботу підсистеми захисту інформації.

Інженерно-технічні заходи захисту інформаційної інфраструктури організації включають використання захищених з'єднань, брандмауерів, розділення інформаційних потоків між сегментами мережі, шифрування та захист від несанкціонованого доступу.

Також неодноразовим фактом може служити те що під час виникнення потреб на підприємствах установах, закладах можуть бути встановленні додаткові системи інженерно-технічного складу, як для прикладу системи пожежогасіння, контроль доступу із використанням біометричних чи інших даних, серверів із двоетапними перевірками , тощо.

У разі крайньої необхідності можуть бути вжиті технічні та інженерні заходи, такі як встановлення серверів, систем пожежної безпеки та контролю доступу.

Деякі будівлі, в яких знаходяться серверні, чи інші модулі системи захисту інформації, можуть бути оснащенні також системами акустичного мовлення, як виду інформації.

Значним чинником є формування систем захисту інформації зображених на рисунку 2.1.

Рисунок 2.1 – Формування СЗІ

Слід якісно оцінювати можливості системного входу та варіацій Оцінювання інформації та можливості її захисту в цілому , а також методики їх оцінювання прямо пропорційно залежить від встановленим НД ТЗІ, а також залежить попереднього узгодження моделей інформації та ступені конфіденційності до яких вона належать, як до прикладу інформація із грифом «ДСК», чи «Цілком таємно» [10].

Найключовішим аспектом при формуванні і впровадженні захисту інформації на підприємств, є саме розроблення чіткої стратегії.

Чітка стратегія повинна мати безпосередньо оцінку та повинна здійснювати зменшення витрат при провадженні такої системи захисту інформації, адже це з обумовлює першочергово централізацію процесу захисту такої інформації в цілому, а також дозволяє здійснювати упереджене мислення для запобігання витрат підприємства, що в подальшому може призвести до неіррационального використання коштів з метою яких, і за рахунок яких формувалася система захисту інформації.

Реалізація ж таких заходів повинна відбуватися в рамках встановлених проектних моделей інформаційної системи, а також повинна бути обрана самостійно

власником розпорядником таких інформаційних ресурсів інформаційного вищим керівництвом, розпорядником вищого рівня.

Ці всі аспекти повинні чітко моделюватись та проектуватися для налагодження системи захисту інформації при розробці проектно-кошторисної документації (ПКД)і становити відносно сумлінну частину комплексної системи захисту інформації . [24].

Усі ці дії формують саме профіль безпеки такої підсистеми захисту інформації, що в подальшому підлягає документуванню уповноваженими особами які реагують на здійснення заходів, щодо ліквідації прориву комплексної системи захисту інформації відповідно до ролей та впливів на процес уточнення профілю безпеки, усі особи, які уповноважені на здійснення використання підсистеми розвитку комплексної системи захисту інформації а також відповідальні особи, які здійснюють зберігання та створення інформації повинні налаштовувати цільову програму профілю безпеки відповідно до покладених протоколів та алгоритмів комплексної системи захисту інформації що є на даному підприємстві.

Такі профілі безпеки передусім можна поділити на наступні категорії:

– профіль безпеки власника інформаційної системи розпорядника інформації

– профіль особи відповідальної за здійснення виготовлення проектно-кошторисної документації і система захисту інформації що неодноразово відомо що така роль користувача чи розробника безпосередньо поєдную функціональні обов’язки посадових осіб відповідальних за здійснення системи безпеки а також за проектування системи приватності і мобільності комплексної системи захисту інформації на підприємстві

– профіль особи користувача.

Налаштування являється частиною комплексу заходів, що реалізують входження окремих підвідомчих алгоритми протоколів та інших груп відповідальних за систему захисту інформації до циклічної бази, які реалізують КСЗІ.

Першочерговим є вибір самої системи і групи захист визначення кількість окремих алгоритмів та переліків можливого впровадження заходів захисту їх посилення відповідно до обраної стратегії, це здійснюється в послідовності відповідно до обраного методу захисту, або від відповідного способу посилення заходу, який здійснює захист в інформаційній системі такої інформації головного

розпорядника інформації, тому відповідно до спрямованих визначених заходів, а також відповідно до способу захисту слід обирати відповідні та встановлені раніше параметри захисту інформації, вони повинні бути зміні, які визначаються з списку запропонованих при формуванні діяльності організації, а також які будуть максимально забезпечувати профіль безпеки з урахуванням на структуру такої інформації на аналіз безпеки такої інформації у середовищі, а також на технічні характеристики, які можливі для коригування інформації в середовищі, а також не повинні впливати на організаційні можливості підсистеми безпеки, а також приватності зацікавленого підприємства яке впроваджує такі комплексні системи. [5].

Слід зазначити що це все відбувається відповідно до встановлених параметрів, вони можуть бути, як циклічно оброблені так і проводитись на виборні основі заходів захисту.

Щодо часткових заходів вони супроводжується в етапі стратегічного рішення при формуванні першочергових параметрів основоположних часток а також завдань, які підприємство самостійно обрано такі завдання можуть поділятися на етапність можуть поділятися на функції можуть поділятися на окремо виділені заходи, які потребують додаткового оцінювання характеристик вчинених дій та заходів в кінці усього при аналізі та завершенні циклу проводиться повторний аналіз про можливість переходу до наступної групи класу захисту інформації і можливості введення нових алгоритми захисту інформації

Також слід розглядати, можливість, коли, клас має посилений захист з цього випливає, що його заходи в таких випадках та використання окремих завдань покладених на підсилення заходів захисту інформації є недоцільним, атому можна здійснювати використання першочергово циклу програм та алгоритмів на яких безпосередньо буде виключено заходи посилення ЗІ усі ці вище перелічені аспекти цілісно та пропорційно спрямовані на посилення профілю безпеки і за результатами аналізу ризиків здійснюється коригування встановлених характеризуючих часток параметри самого профілю безпеки, який здійснює заходи захисту а також змінює перелік заходів і комплексів, які відображаються на інформації і змісту поширені та інше це дуже чітко видно на рисунку 2.2.

Рисунок 2.2 – Циклічність профілю безпеки і його заходів.

Документація таких заходів в цільовому профілі має здійснюватися на усіх етапах впровадження комплексної системи захисту інформації, документування при розробці безпосередньо забезпечить створення цілісного профілю безпеки при організації ПКД, де також мають бути враховані рекомендації, щодо документування технічні і загальні характеристики, які описують порядок впровадження системи безпеки, який повинен бути комплексний, аналізований на можливу групу ризики, а також відповідати встановленим нормативно-правовим актом відповідно до даного підприємства, адже в державних органах місцевого самоврядування в організаціях в інформаційно-комунікаційних системах є чітка вимога, щодо захисту інформації яка встановлена законом що не містить безпосередньо жодних чинники які можуть впливати на суспільство в цілому а також не належить до групи.

Серед окремих етапі потрібно розділяти такі, як встановлення тобто налагодження безпосередньо інформаційних підсистем коригування способів та

заходів захисту інформації, іншим є безпосередні інсталяція пакету даних, які будуть відповідати за введення і налагодження від системи, яка відповідає за профіль безпеки та заходи захисту інформації, а також про впорядкування встановленому інформаційної системи, яка буде відображати окремі результати документування плани звіти щодо аналізу безпеки. [11].

Усі ці підсистеми розроблення та оформлення безпосередньо затверджується робочою групою, яка відповідальна за заходи захисту інформації, чи уповноваженою на те особою, вона аналізується тестується на експлуатаційний стан вноситься на реалізацію попередньо проходить документально перевірку, щодо таких заходів тестовий хід і в разі необхідності її окремі складові частини можуть бути не розглянуті при здійсненні завершення заходів.

Серед іншого слід зазначити що деякі частини робочої документації яка містить безпосередні заходи управління і відображається у ЦПБ із компонентом документації необхідної для проведення систематичного пусконалагоджувального етапу а також для створення можливості проведення тестування випробування такої системи аналізу її подальшу при окремих аспектах, які можуть не враховуватись на першочергових етапах, заходи щодо налаштування параметрів окремих засобів захисту відповідно до вимог безпеки, які є відображені у проектно-кошторисної документації.

Чи не найважливішим аспектом при впровадженні є саме навчання осіб, які будуть мати роль користувачів та адміністраторів інформаційних системах захисту інформації такі навчання мають відбуватися в порядок визначений раніше встановленим протоколом, чи аналізом систем захисту інформації, особи повинні проходити безпосередньо на підприємстві підвищення кваліфікації по незалежності від розуміння цієї системи чи ні, адже заходи інформація також втручання впливу роботи комплексних систем заходів та профілю безпеки відбувається постійно, а постійне інформування таких користувачів про можливі заходи ризику безпосередньо зменшують кількість етапів на яких можна втратити таку інформацію. [4].

Навчання повинні проводитися безпосередньо для усіх користувачів тобто користувачів які здійснюють технічне обслуговування таких підсистем, персонал який відповідальний за моделюючу базу, це самі звичайні користувачі які не мають управління захисту інформація, тобто самої інформації якої не являється

розпорядником, а також простих інших користувачів які здійснюють збір та обробку інформації відповідно до положення затверджених документів заходів реалізації, які повинні забезпечувати правила політики безпеки інформації, а також які здійснюють перевірку на виявлення загроз.

Також ще немало важливим і безпосереднє здійснення перевірки на знання інформаційної системи кожним користувачем і неможливість реєстрації результатів навчання з метою відображення безпосередніх даних про необхідність доукомплектування окремими частинами інформації самого персоналу, усе це відбувається відповідно до уточненого профілю безпеки безпосередньо після відбору відповідного базового профілю слід здійснювати його налаштування постійно, але ці дії повинні бути безпосередньо узгоджені із розробником проектно-кошторисної документації, щодо запровадження захисту інформації, а також особами які здійснюють дії щодо процесу налаштування такої комплексної системи захисту чи профілю безпеки на визначення окремих параметрів які мають враховувати фактори управління безпеки серед користувачів найпростіших та самого розпорядника адже це є частиною структури захисту інформації, і в пливає на процеси розробки цільового профілю. [10].

Процеси профілю безпеки також є циклічним і серед них можна виділити основні, які зображенні на рисунку 2.3 нижче наведеному.

Рисунок 2.3 – Циклічність процесів профілю безпеки.

2.1 Інженерно-технічні заходи захисту інформації та комплект передових комплексних заходів призначених для захисту інформації

Статистичною частиною технічного захисту інформації є розподілення інформації до такої, що може становити державну чи іншу відповідно до чинних нормативно-правових актів України інформацію з грифом таємно, або для службового користування, що в подальшому створює приналежність до віднесення її до інформації з обмеженим доступом.

Інформація, яка є державною власністю і у володінні держави, розпорядження з обмеженим доступом інформація з обмеженим доступом в процесі діяльності створення її передбачає в собі окремі види такої інформації, а саме неможливість і отримання та нерозповсюдження в ресурсі широкого кола осіб адже поширення та зберігання безпосередньо регулюється нормативно-правовими актами задля унеможливлення розповсюдження її для в подальшого впливу та встановлення загроз нацбезпеки, безпеки суспільства, розповсюдження конфіденційної інформації та інше всі ці аспекти потребуються для унеможливлення витоку інформації порушення цілісності розпорядником інформації таких даних, а також з метою утвердження встановлених вимог закону. [10].

Окремо слід зазначити про схильність такої інформації яка не передбачає розповсюдження до впливу загроз, адже вона може призводити безпосередня до загроз безпеки, чи інших чинників які будуть порушувати права держави та осіб в цілому, ці аспекти формують якраз здатність віднесення інформації, до підтипів які потребують виявлення загроз, створення безпосередньої комплексної системи захисту.

На сьогоднішній день уповноваженими особами представниками структур органів державної влади державних підприємств здійснюється розробка безпосередніх програм, комплексів заходів інженерно-технічних заходів захисту інформації, передових комплексів призначених для захисту інформації з метою протидії загрозам впливу, витоку такої інформації, а також із нейтралізації

відповідних дій, чи бездіяльності для функціонування систему захисту інформації. Серед ключових інженерно-технічних заходів слід виділяти приймання робіт технічної системи захисту інформації розроблення і реалізація первинних технічних основоположних функцій програмного забезпечення використання спеціалізованих засобів забезпечення програмних комплексів проведення обстеження підприємств на визначення профпридатності мережі комплексу інформаційних телекомунікаційних каналів засобів зв'язків атестація учасників програмного використання, аналіз та інші

Першочергово слід розібрати поширення таких носіїв, поширення можливості витоку інформації з обмеженим доступом, для цього спеціально проводяться інженерно-технічні заходи, а саме:

– аналіз і створення ліній спеціального зв'язку підключення до системи сигналізації;

– керування енергетичної системи;

– створення спеціалізованого обладнання для інженерних споруд;

– створення єдиної системи комунікації споруди з програмним забезпеченням захисту інформації також інші елементи.

Здійснення порушення цілісності інформації з обмеженим Доступу є діяння за яке порушники відповідають відповідно до встановлених вимог закону, а саме КУпАПу та Кримінального кодексу України. [11].

З метою усунення таких перешкод, унеможливлення безпосередньо порушення роботи підсистеми, які здійснюють захист інформації особливого призначення та інших здійснюється модифікування таких комплексних систем захисту інформації вони можуть бути результатом загрози безпеки інформації, адже при здійсненні витоку інформації безпосередньо створюються нові системи і алгоритми дії, які передбачають створення покращеного середовище технічного захисту як вони правило підлягають інформатизації, а також постійному аналізу, адже інформація з обмеженим доступом носієм яких є безпосередньо установи та організації, ОМС, органи наділенні владними повноваженнями, котрі при здійсненні діяльності, не використовують окремих технічних засобів пересилання оброблення зберігання, а також створення інформації.

Ці всі аспекти належить до підсистеми інженерно-технічного спрямування. Роботи із формування захисту інформації з обмеженим доступом які в подальшому

унеможливлюють витоки інформації каналами побічних дій, чи спрямування складають із себе комплекс двох частин комплексної системи захисту інформації, адже відповідно жодні інженерно-технічні заходи контролю не виникають, без попередню розробленої стратегії, а також організації із підготовки таких заходів, адже технічні заходи повинні відбуватися відповідно до встановлених технічних завдань із захисту інформації, вони повинні бути безпосередньо створені на основі нормативно-правових актів, керувати ефектом роботи, а також повинні ліцензуватися державною службою України з питань технічного захисту інформації, а також іншими чинниками та структурами безпосередньо в залежності від самої інформації що підлягає окремому зберігання шифрування та інші. Слід розуміти що ці підготовчі заходи повинні відбуватися відповідно до переліку відомостей з обмеженим доступом, чи ті що під грифом таємно, що підлягають не тільки захисту сторони фізичної особи а також підпадають під визначений законодавством перелік що повинен забезпечуватися технічним захистом. [12 с.3].

Серед основного обґрунтування можливості введення таких цілісних систем і захисту інформації, що здійснюють збереження інформації з обмеженим доступом чи інформації, що носить собі інші таємні грифи являється саме унеможливлення витоку технічними каналами інформації, що не може бути представлена особам у вільному форматі що підлягає, безпосередньо постановці окремо гриф таємно для таких періодів і визначається окремий перелік заходів щодо обмеження доступу серед інженерно-технічних заходів є також і організаційні заходи які цілісно Та пропорційно пов’язані із підготовкою мереж підсистем програмних засобів людського фактору до захисту інформації
А саме серед таких можна виділити як встановлення окремих приміщень модельних базисних та інших кабінетів створення окремо серверних частин до яких не допускаються сторонні особи які не пройшли перевірку на можливість витоку інформації від осіб також визначається ще одиниць з технічних засобів застосуванні до якого не потрібно бути службовою особою а виключно виробничою це заходи щодо інженерних робіт монтажу такої системи адже безпосередньо під час таких робіт здійснюється чи не найважливіший процес, а саме влаштування підключення мереж до захищених ресурсів каналів та іншого.

Ще одним із ключових заходом є виявлення усіх мереж інженерно технічних мереж на приховані ресурси на можливість підключення до мережі електропостачання, водовідведення, що виходять за межі використовуваного приміщення які в подальшому можуть спричинити підключення до мережі де здійснюється комплексна система захисту інформації. [13].

За результатами таких періодів, уповноваженими особами та керівником здійснюється складання акту із етапами виконання таких робіт, якщо такі дії попередню не були облаштовані до вимог проектно-кошторисної документації раніше, яка затверджена розпорядником такої інформації чи органом вищого ступеня.

Слід зазначити що в ПКД має бути чітко зазначений окремий перелік заходів інженерно-технічного спрямування, а саме:

– опис приміщення в яких відбувається комплексні задачі системи захисту інформації ;

– окремість плану виділених приміщень з можливістю прокладання окремих схему організації автономного забезпечення каналізування;

– забезпеченість мережею електропостачання.

Переліком використовуваних ресурсів при створенні такої підсистеми, а саме кабелів їхньої довжини метражу кількості провідності, що підлягають безпосередньо оцінці та сертифікації інженерно-технічних характеристик, усього обладнання, що потребується для встановлення комплексної системи захисту інформації.

Підготовчі заходи щодо створення інженерно-технічних заходів повинні здійснюватися з метою блокування електроустановки перетворювання вокремі ліній електромереж, взагалі в цілому у світі безпосередньо передбачено можливість створення автономних ресурсів, які будуть генерувати електроенергію для підживлення такої системи захисту інформації, що унеможливлює підключення до ліній зв’язку та переміщати систему захисту інформації за межі даного приміщення і унеможливлює будь-який вплив навколишнього середовища на систему захисту інформації

Слід також що розрізняти, що для виконання вимог і захисту інформації з обмеженою діяльності, сідл упередити витік через радіо телекомунікаційні системи мережі, що виходять за дане приміщення де облаштована сама система захисту-серверна, це може бути забезпечений захист шляхом відключення провідних

гучномовців засобів телефонної комунікації та видаленням ресурсу найпростішого захисту пристроїв телекомунікаційних систем, єдиним що не може бути виключеним із мереж являєтеся телекомунікаційної системи окремі абонементів, пристроїв, які попереджають дане приміщення, яке облаштований для захисту оповіщенням, а саме сигналізація та інші окремі види які напряму з'єднані з центральним сервером окремим кабелем електроустаткування чи іншої системи. [12].

З метою попередження виключення каналу захисту інформації потребується безпосередньо електропостачання, яке буде автоматизований і не буде підключатися на період проведення закритих заходів чи відсутності електромережі.

Ще одним із ключових інженерно-технічним заходів із запобігання витоку, які спричинені окремими каналами, є системи протипожежної сигналізації чи охоронної системи, оповіщення датчиками руху, датчиками охорони, а також датчиками важливих заходів, які потребують підключення до центральної серверної бази мережі інтернет та інших ресурсів.

З метою унеможливлення такі роботи здійснюється за допомогою окремої системи в мережі каналів, які підключаються до телеприймачів радіоприймачі виводу головних екранів відеоспостереження на телевізори без доступу інших осіб також за допомогою звуку підсилювальний та звуко-записуючий апаратури а також за допомогою мереж дротових електроустаткування, які виводять та підключається безпосередньо до центрального каналу доступ до якого знаходиться у виключних осіб.

Ще одним фактором проведення інженерно-технічних робіт є безпосередні захист мережі кондиціонування, тобто унеможливлення допуску через систему кондиціонування інших ресурсів приміщень носіїв які можуть зашкодити серверній чи системі електронної системи підсистеми захисту інформації з обмеженою діяльність серед яких безпосередньо розповсюджується заходи з електроживлення від власної електростанції енергоресурсу на контрольовані території приватної чи іншої форми власності дає забезпечення виділення окремої території для розміщення таких об'єктів закритого типу як правило в нас виступають ЗТП(закрита трансформаторна підстанція), а також за допомогою систем автоматичного кондиціонування, які проектується і створюється при формуванні будівлі. [13].

Захист від витоку інформації з обмеженою діяльністю за допомогою устаткування електроживлення побутової техніки чи техніки, яка відповідальна за підключення до системи охоронної діяльності, чи сигналізації повинен відбуватися за допомогою окремого фідера системи електропостачання до якого мають доступ виключні уповноважені особи та сам розпорядник інформації.

Усі вище перелічені аспекти формують складову базу мережу запобігання втручання в діяльність інформації з обмеженим доступом конфіденційної інформації та інформації з грифом таємно за допомогою найпростіших інженерних мереж які найчастіше використовуються на підприємстві.

Серед технічних завдань є багато чинних норм які визначені окремими відповідальними і уповноваженими особами органами державної влади серед яких Держспецзв'язку, існують багато методичних рекомендацій щодо окремих видів як для систем електрифікації каналізування вентиляційних систем, систем пожежної охорони, систем охоронюваної системи, відео системи, спостереження та інше серед яких є окремі вимоги щодо встановлення будь-якого об'єкту на приміщенні чи у приміщенні де здійснюється моделювання захисту інформації наприклад не допускається формування 1 екрану Вальної системи мережив них кабелів шнурів живлення від підключення до центральної мережі електропостачання. [8].

Також чинними нормативно-правовими актами та методичними рекомендаціями при здійсненні захисту інформації забороняється живлення що мають вихід на мережу де є не захищений джерела електропостачання без встановлення окремої мережі шифрування інформації, а за живлення відбувається безпосередньо від окремих ліній чи енергоносіїв фільтраційних об'єктів, які відносяться до четвертої категорії допуску на низьких напругах і становленням раніше заземлювальних пристрої розміщених у межах закритої трансформаторної підстанції.

Ще одним із ключових інженерно-технічних заходів не враховуючи заходів щодо основних мереж є заходи щодо встановлення шуму продавлення шуму генерування, а також екранування проводів і кабелів в яких основних мереж таких, як газ світло водопостачання з'єднання із нероз'ємними трубами зварювання їхні, підключення до мереж, які неможливо здійснювати поточний чи капітальний ремонт

без основного втручання про що попередню попереджається розпорядника інформації.

Для розміщення таких інженерних мереж для проведення керування робіт поточного ремонту капітального ремонту такої мережі здійснюється прокладання кабелю розподільними роз'ємами і підключається до нової системи, яка утворюється зали з тобою сталі де здійснюється встановлення секційної коробки підключення каналу захисту зв'язку окремих каналів які підключається до органів центральної державної влади напряму здійснюється облаштування контру конструкції захисту таких інженерних мереж, а також встановлюється окремі лінії контакту флангів, які мають покриття що унеможливлює корозію руйнування, утворення іржі і пошкодження шляхом природнього фактору. [18].

Слід зазначити що висновки щодо ефективності і можливості облаштування таких інженерно-технічних заходів повинні розроблятися відповідно до фактичного місця розташування об'єкта встановленого ефективного способу контролю за заходами інженерно технічного захисту на етапі проектування, встановлення, затвердження та сертифікації жоден із цих чинників не може остаточно гарантувати безпеку профілю користувача, безпеку обладнання системи захисту ,безпеку надійності допуску до приміщення окремих осіб, адже виключно в налаштуванні мережі, як комплексно цілісного системного апарату це може оцінюватися виключно при кінцевому налаштуванні всіх аспектів включаючи людського фактору, адже без втручання людського фактору жодні підготовчі проектуванні чи монтуванні роботи із мережі технічного захисту інформації не можуть виконувати свою запрограмовану функцію на усі сто відсотків.

РОЗДІЛ 3. ВПРОВАДЖЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇНА ПІДПРИЄМСТВІ «ВЕЛИКОБЕРЕЗОВИЦЬКА СЕЛИЩНА РАДА» ТА ШЛЯХИ ВИРІШЕННЯ ЗУСТРІЧНОЇ ПРОБЛЕМАТИКИ.

3.1. Вимоги із захисту інформації на підприємстві.

Загальні відомості про підприємство:

Великоберезовицька селищна рада – орган місцевого самоврядування

Юридична адреса 47724, смт Велика Березовиця Тернопільського району Тернопільської області, специфікація діяльності (КВЕД) 84-11 державне управління

Відділ цифрової трансформації та зв'язків із громадськістю працює над програмним забезпеченням, який здійснює інформаційно-комунікативне забезпечення діяльності ОМС.

Час роботи понеділок-п'ятниця з 8:00 – 17:15, перерва 13:00 – 14:00, субота – неділя вихідні дні.

Щодо необхідності впровадження комплексної підсистеми захисту на підприємстві слід зазначити, що даний суб'єкт належить до переліку, що в обов'язковому порядку здійснюють створення комплексної підсистеми захисту інформації у своїй діяльності відповідно до постанов Кабінету Міністрів України.

Фактичною обставиною створення КСЗІ є встановленні вимоги закону, а також рекомендації органу державної влади, щодо створення на підприємстві, окремої системи захисту інформації, яка буде здійснюватися, як за допомогою організаційних засобів так і за допомогою комплексу інженерно-технічних засобів, які передбачають здійснення заходів, котрі обмежують, або напряму відмовляють користувачу у доступі до певних видів інформації, з метою забезпечення її цілісності та доступності.

Відповідно до Закону «Про захист інформації в інформаційно-телекомунікаційних системах» здійснення обробки інформації у підсистемах, їхні умови обробки такої інформації умови обробки інформації в системі встановлюються виключно розпорядником інформації, за умов, що попередньо розпорядником не було оформлено таку інформацію та не віднесено до інформації із грифами, чи не обмеженому доступі до неї.

Відповідальність за захист інформації в системі покладається на власника системи.

Об’єктивною та суб’єктивною стороною даного дослідження (далі OID) являєтеся сайт суб’єкта господарювання, а також інформаційно- телекомунікаційна система яка складається із таких застосунків, як СЕВ ОВВ, АСКОД (на етапі впровадження), ЄСІС та інші системи, які найчастіше використовуються органами місцевого самоврядування в у своїй роботі, для передачі, формуванні створенні інформації та інше. [10].

Дослідження проводились на відповідність та на допустимість відповідно до ДСТУ 3396.1. У ході такого дослідження, було виведено в окреме дослідження також дослідження середовища користувача та власника підсистеми (відповідно до можливостей системного адміністратора). [18].

Віднесення до певної категорії захисту інформації здійснюється самостійно розпорядником такої інформації, що у відповідності до методики стандартизації , протоколів вищого рівня розпорядника віднесено до категорії IV (четверта).

Адже використовується технічні засоби для обробки інформації з обмеженим доступом, яка не є державною таємницею, а також інформацію яка є загально доступною і гласною оскільки самим регламентом передбачено прозорість, публічність та відкритість, ведення інформації, що створюється таким органом, якщо іншим локальним актом не обмежено таку інформацію.

Приміщення забезпечене електромережою, автономним-опаленням, водопостачанням та водовідведенням, засобами пожежогасіння. живлення енергосистеми та інших функцій здійснюється автономно установами комунальної форми власності, що є на підпорядковуються даному підприємству, що відображено на рисунку 3.1.

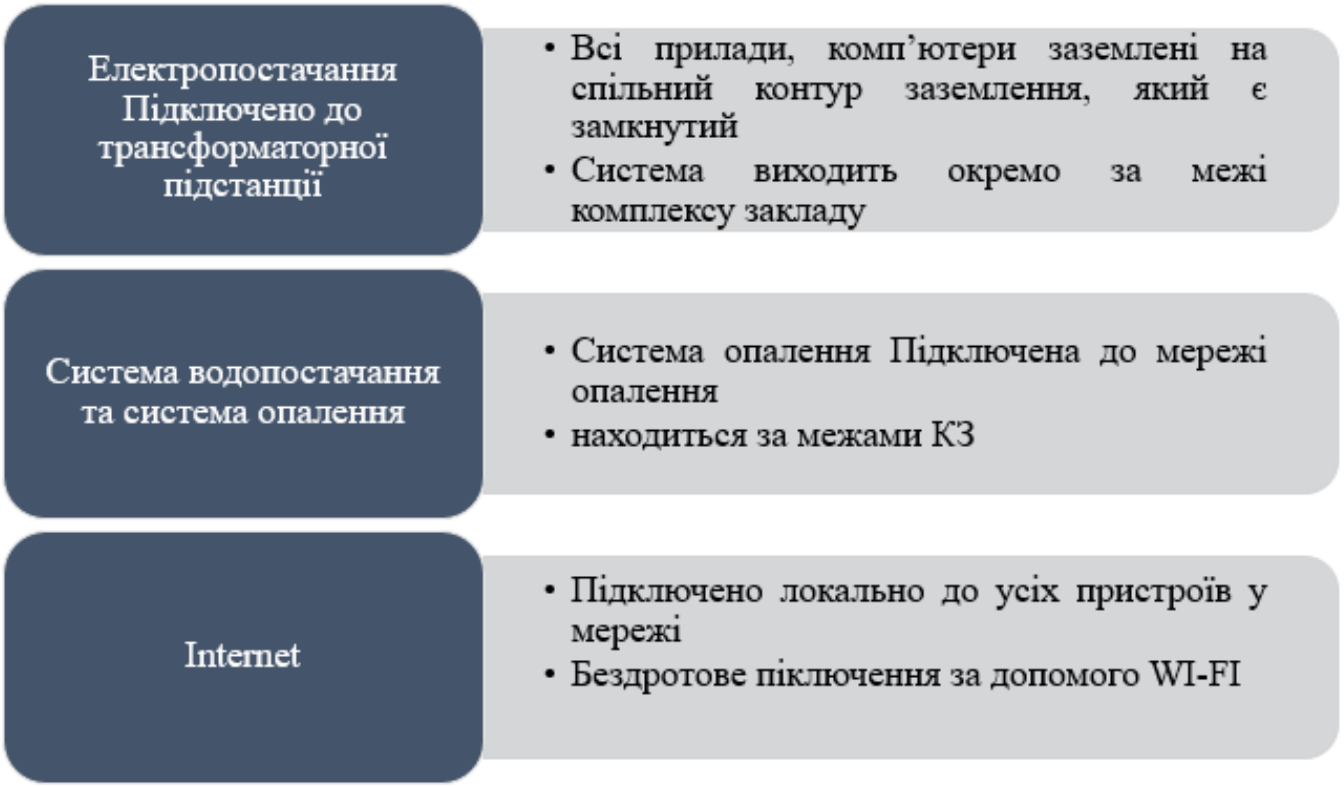

Рисунок 3.1 – Забезпечення підприємства

Щодо основної структури, яка відповідає за забезпечення, створення та формування інформації слід віднести наступні критерії посад: селищний голова, начальник відділу загальної та організаційної роботи, начальник відділу юридичного забезпечення та кадрової роботи, начальник відділу цифрової трансформації та зав'язків із громадськістю.

Інформація слід розділяти за такими критеріями:

– з обмеженим доступом;

– відкриту за запитом;

– публічну що не потребує захисту.

– Інформація з відкритим доступом в ІТ Сформується, як електронні документи, створені за допомогою ПЗ Microsoft Office 2010, 2007, 2003 та інші, Adobfine reeder або у паперовій формі.

Примірники паперового типу зберігаються уповноваженими особами у сейфах. Здійснення заходів щодо поділу та розподілу доступу та критерій інформації, чи інформаційних відомостей створюється керівником підприємства у нашому випадку селищним головою. Доступ до International Sports Organization for Disabled можуть отримувати лише посадові особи органів місцевого самоврядування уповноваженні

на це нормативно-правовим актом затвердженим селищним головою. Відомості що містять спеціальні грифи чи обмежуються простим користувачам, в своєму аналізі має велику значущість, адже передача таких даних несанкціонованому користувачу, або передача може призвести до необхідності створення нового протоколу захисту інформації, або створить умови для перетворення інформації, що в свою чергу потребуватиме спростуванню.

Слід зазначити, що класифікація інформації стосовно одного і того ж локального акту, чи іншої форми інформації може бути обмежена у доступі і використанні, або ж навпаки бути створена для гласності проте уз набранням чинності після спливу певного періоду часу, що повинен підлягати відкритості в частинні моменту набрання законної сили, і ці процеси залежать від кваліфікації інформації, що відображено в таблиці 3.1

Таблиця 3.1 – Класифікація Інформації

Опис	Правовий режим	Режим доступу	Тип представлення	Вимоги до захисту	Доступ мають
Організаційн о-розпорядча документація	Конфіденційна	ІзОД	Зберігається в кабінеті у керівника на паперовому носії та на сервері	Ц,Д	Керівник , системний адміністратор
Облік внутрішніх документів	Конфіденційна	ІзОД	Зберігаються в керівника директора на паперовому носії	К,Ц,Д	Керівник
Інформація про надання послуг, тарифи, контактна інформація підприємства	-Конфіденційна	Відкрита	Текстова та числовайнформація в цифровому та паперовому вигляді.	Ц,Д	Керівник, системний адміністратор
Інформація проробітників	-Конфіденційна	ІзОД	Зберігаються в кабінеті у керівника на паперовому носії	К,Ц,Д	Керівник
Статутні документи підприємства	-	Відкрита	Зберігається в кабінетіу керівника на паперовому носії	Ц,Д	Усі працівники
Облік та реєстрація вхідних та вихідних документів організації	Конфіденційна	ІзОД	Зберігається в кабінетіу керівника на паперовому носії та на сервері	К,Ц,Д	Керівник, системний адміністратор

Основним завданням при створенні окремих підрозділів захисту інформації в подальшому поза основним завданням їх контролю є організаційне забезпечення керування таких систем захисту інформації на обраних підприємствах, установах та

закладах, а саме здійснення контролю за втручанням до веб-ресурсу, в яких міститься інформація та їхнім функціонуванням на системи захисту інформації, їхні підрозділі, як правило покладається виконання робіт із встановленням вимог захисту такої інформації в аналітичні системі, який використовується підприємством та під час проектування кошторисної документації, а також з метою розроблення модельної системи захисту на підприємстві

Також неодноразово ми це можем зустрічати на етапі технічної підтримки такої системи підприємства, яка здійснює комплексний захист інформації а також на етапі контролю за захищеності даних в комплексному системі захисту інформації самого підприємства.

Для проведення окремих заходів з захисту інформації в КС, які пов'язані з напрямком діяльності інших підрозділів підприємства, керівник підприємства своїм наказом визначає перелік, строки виконання та підрозділи для виконання цих робіт.

Підрозділи захисту інформації повинні взаємодіяти із розпорядниками вищого ступеня, а також іншими державними органами, задля убезпечення інформації від несанкціонованого користувача.

У разі потреби підприємства також можуть скористатись послугами ліцензованого розробника, серед яких для ОМС можуть виступати відділ вищих установи, обласних адміністрації, Державна служба спецзв'язку та захисту інформації та інші.

Система захисту інформації в своїй роботі має мати комплекс завдань і забезпечувати щоби автоматичні системи та підсистеми здійснювали функції без втручання в роботу самої підсистема та без змін властивостей такої системи захисту інформації, оскільки це в подальшому може призвести до несанкціонованих витрат на підприємстві, а також повинна включати захист інформації в межах системи та поза її межами, відповідно до користувачів яким гарантований вхід на стадії циклу самої технології має здійснювати захист інформації з подальшим розвитком експлуатаційного конфігураційного стану, а також повинна включати можливість подальшого експлуатаційного вдосконалення такої інформаційної системи. [24].

При взаємодії автоматичних систем обробки інформації із незахищеними джерелами інформації повинен бути створений профіль безпеки, який буде

забезпечувати розділення інформації до обмеженого та необмеженого доступу у відповідності до протоколів, які є затверджені розпорядником інформації.

Також безпосередня застосування захисту інформації не повинно погіршувати екологічну ситуацію, адже при формуванні її інженерно-технічних заходів повинні удосконалюватися можливості на вчинення дій що унеможливлять ризики для безпеки навколишнього середовища, це супроводжується з тим що на будівлях, серверних та інших частинах об’єкту де знаходяться засоби захисту інформації створюються окремі підсистеми електро забезпечення, закриті трансформаторні підстанції та інші об’єкти, які можуть завдавати принципі шкоду навколишньому довкіллю і цим самим погіршувати екологічну ситуацію району де використовується комплексна система захисту інформації.

Також використання таких підсистем немає зумовлювати психологічного тиску на людину користувача або інженера який здійснює експлуатацію такої підсистеми захисту інформації.

Керування доступом до даної інформації повинна відбуватися, як на рівні автоматизованого користувача на віддалений функцію роботи так безпосередньо і під час розробки в приміщенні цього ж самого об’єкту де знаходиться система захисту інформації, також система вимогу поділяється і враховується на отримання збору комплексних даних їхні зберігання передачі інформація на ключові носії обробка цієї інформації аналіз і система безпеки моніторингу усіх санкціонованих та несанкціонованих користувачів даної підсистеми інформації, що в подальшому допомагає здійснювати контроль та технічну підтримку за цілісністю критичного інфраструктурного ресурсу програмного забезпечення від внутрішнього прориву бази даних витоку інформації та несанкціонованого доступу, що може відбуватися через наявні помилки програмного забезпечення, людського фактору, чи помилки при створенні інженерно-технічних заходів управління засобами захисту інформації.

3.2. Середовище користувачів інформаційно-телекомунікаційної системи підприємства та заходи, щодо його покращення.

Серед середовища слід розрізняти, що є користувачі, яким безпосередньо надано права доступу, як до веб-ресурсу так і загально доступна інформація, яка

міститься в системі захисту інформації в програмних забезпечення таких, як «Лелека», які визначають ступінь інформації та здійснюють захист її від несанкціонованого доступу.

Також бувають користувачі які наділені безпосередньо повноваженнями супроводжувати виключно комплексну систему захисту інформації, це як правило користувачі з функціональним обов'язком введення А також ті особи яким надано доступ до постачання обладнання технічних засобів і фахівці ІТ сфери що здійснюють монтаж налаштування програмного забезпечення дають безпосередні гарантійне становище.

Це все здійснюється відповідно до політики безпеки інформації в системі комплексного захисту інформації, які забезпечується штатними одиницям захист системного функціонування а також реалізують інформаційні ресурси і доступи до них що в подальшому забезпечує встановлення і оснащення основних і додаткових компонентів ви прес-інформаційно програмного забезпечення а також операційної системи. [19].

З метою дотримання безпеки інформації в комплексних системах захисту, щодо функціонування веб-сторінки відомчого ресурсу система електронної взаємодії органів державної влади «СЕВ ОВВ», для прикладу також система електронного документообігу на підприємстві також забезпечує безпосередньо цілісність внесення відомостей паперових носіїв в інформаційну систему, яку безпосередньо використовують користувачі

Для прикладу це є домінантні іменовані системі проксі-сервера і файлові трансферти протоколів ну та інші що взаємодіють з веб-сторінкою та мережею підприємств.

Доступи безпосередньо повинні надаватися користувачам відповідно до розробленої політики безпеки підприємства в даному випадку розглядається безпосередньо «Положення про систему захисту інформації про доступ до публічних даних», а також інші які не можуть бути перечисленні в зв'язку із нанесенням на них грифу таємно.

Для встановлення регламенту доступу цих користувачів до інформаційних сторінок що розробляється у відповідності до норм програм апаратів засобів системи захисту і кваліфікації комплексної системи захисту інформації проводиться

попередній тестинг, інсталяція і впровадження окремих підсистем програмного забезпечення, а також проводяться роботи відповідно до а раніше встановленого регламенту, щодо подолання функцій попереднього обслуговування обладнання, а також створюється опис відомостей, які містять кожне програмне забезпечення, їхні технічні характеристики зокрема компоненти, які необхідні для безпосереднього функціонування підсистеми комплексу захисту інформації, які використовуються на даних підприємств вони можуть бути безпосередньо поділені на категорії в залежності від типу інформації які вони місять відповідності до носіїв за допомогою яких вони працюють а також відповідно до потреб тестування. [21].

Серед таких середовищ ми можем бачити відповідні інформаційні ресурси, реєстри баз даних, які не працюють без попередньої авторизації користувача за власним сертифікатом, а саме сертифікатом чи токеном, як окремою системою захисту інформації через автентифікацію особи в цілому.

Також це можуть бути відображені файловими носіями такими і як ключ електронного підпису який надає доступ до реєстру за допомогою ідентифікації особи в реєстрі а також створення захищених шлюзів інформації серед таких реєстрів для прикладу можем взяти «Реєстр територіальної громади», де встановлюється окреме програмне забезпечення та VPN ресурс якийсь або Cisco any connect, який встановлює захист каналу інформації, яке забезпечує в подальшому використання програмного забезпечення шляхом авторизації клієнта через електронний носій, який підтягує сертифікат особи її найменування її реєстрації. Дані які безпосередньо попередньо надсилаються до розробника середовище такої комплексної системи захисту інформації і узгоджується канал захисту зв’язку.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Вимоги ергономіки до організації робочого місця оператора ПК

Ергономічна організація робочого місця користувача ЕОМ враховує як специфіку діяльності, що виконується, так і забезпечує комфортні умови перебування людини. Тому основними ергономічними завданнями щодо організації робочого місця є наступні:

– забезпечення просторових параметрів робочого місця, які відповідають антропометричним характеристикам користувача;

– раціональне розташування елементів робочого місця відносно користувача на підставі поглибленого кількісного та якісного аналізу діяльності, яка виконується;

– оптимізацію умов робочого середовища.

На рисунку 4.1 наведено робоче місце користувача ЕОМ та позначено основні ергономічні та просторові параметри його складових.

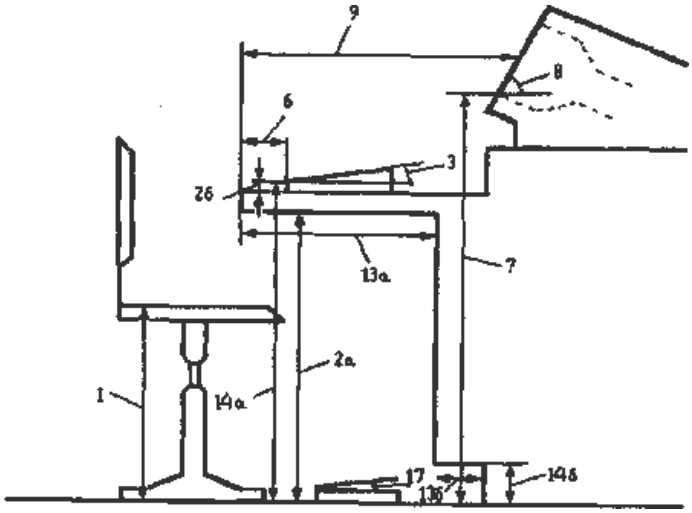

Рисунок 4.1 – Робоче місце користувача ЕОМ

Основні просторові параметри робочого місця користувача ЕОМ приведені в таблиці 4.1 [11].

Таблиця 4.1 – Просторові параметри робочого місця

Умовні позначення	Параметри	Спосіб вимірювання параметра	Значення параметра
1	Висота сидіння	Від підлоги до верхньої площини сидіння	400-500 мм
2	Висота клавіатури (від рівня підлоги)	Від підлоги до нижнього ряду клавіатури	600-700 мм
2а	Висота клавіатури (від рівня стола)	Від базової поверхні до нижнього ряду клавіатури	20 мм
3	Кут нахилу клавіатури	Від горизонтальної площини	7-15°
4	Ширина основної клавіатури	Визначається оптимальною зоною моторного поля	До 400 мм
5	Глибина основної клавіатури	Визначається оптимальною зоною моторного поля	До 200 мм
6	Відстань від клавіатури до краю стола	Від переднього краю стола до клавіатури	Понад 80 - 100 мм
7	Висота екрана	Від підлоги до нижнього краю екрана	950-1050 мм
8	Кут нахилу екрана	Від вертикальної площини	15°
9	Відстань від екрана до краю стола	Від переднього краю стола до екрана	500-700 мм
10	Висота поверхні для запису	Від підлоги	870-860 мм
11	Площа поверхні для запису	Визначається оптимальною зоною моторного поля	600 х 400 мм 900 х 600 мм
12	Кут нахилу поверхні для запису	Від горизонтальної площини	0 – 10°
13	Глибина простору для ніг на рівні колін	Від переднього краю стола	Понад 400 мм
13а	Глибина простору для ніг на рівні колін	Від підлоги	Понад 600 мм
14	Висота простору для ніг на рівні колін	Від переднього краю стола	Понад 600 мм
14а	Висота простору для ніг на рівні ступень	Від підлоги	Понад 100 мм
15	Ширина простору для ніг на рівні колін		Понад 500 мм
15а	Ширина простору для ніг на рівні		Понад 250 мм
16	Висота підставки для ніг	Від підлоги до передньої частини підставки	50-130 мм
17	Кут нахилу підставки для ніг	Від горизонтальної площини	0-25°
18	Глибина підставки для ніг	Від переднього краю підставки до її заднього краю	400 мм
19	Ширина підставки для ніг		300 мм
20	Пюпітр-підставка для документі в	Від горизонтальної площини	15 - 20°

В ході організації робочих місць на кожну ЕОМ виділяється площа, яка складає не менш, ніж 6 $м^2$, та об'єм, який становить не менш, ніж 20$^{м\ 3}$. Причому, зона, де розташовується робочий стіл, сервер або робоча станція, принтер, екран для графопроектора, займає відповідно 6-8 $м^2$. Висота приміщення не менша, ніж 4 м.

Робоче місце користувача ПК облаштоване одномісним столом та напівм'яким стільцем, висоту сидіння яких можна змінювати. Довжина стола користувача не менше 700 мм, ширина – забезпечує місце перед клавіатурою для розташування зошита або іншого приладдя. Поверхня стола має кут нахилу у межах 12-15, лише іноді припустимою є її розташування у горизонтальній площині [11].

На робочому місці користувача ПК забезпечена відповідність висоти краю стола і стільця до росту та антропометричних особливостей організму користувачів. Як нормативні визначають показники, що приведені у таблиці 4.2.

Таблиця 4.2 – Нормативні показники

Ріст, мм	Висота над підлогою, мм		
	стіл	простір для ніг	стілець
1450-1600	640	530	380
1610 -1750	700	590	420
Понад 1750	760	650	460

Глибина простору для ніг під столом не менше 450 мм, а у випадку застосування високого стола та низького стільця і, отже, відсутності відповідності росту користувача конструктивним елементам робочого місця, використовується підставка для ніг, ширина якої становить – 350 мм, довжина – 400 мм, кут нахилу опорної поверхні – 15^o.

Столи з ЕОМ розміщено без розривів між ними, але при незначній кількості робочих столів з відеотерміналами перевагу варто віддавати розташуванню їх біля внутрішньої стіни.

Робота з комп'ютерною технікою вимагає обов'язкового дотримування правильної посадки. Користувач ЕОМ повинен сидіти прямо, з невеликим нахилом (до 5° – 7°) голови вперед, не сутулитися, спираючись нижніми краями

лопаток на спинку стільця. Передпліччя повинні спиратися на поверхню стола, забезпечуючи зниження статичного напруження м'язів плечового поясу і рук, кути, що утворюються передпліччям і плечем, а також гомілкою і стегном, – складати не менш, ніж 90°.

Рівень очей припадає на центр екрана або на точку, яка розташована між верхньою та середньою третинами екрану, причому, лінія погляду є перпендикулярною до площини екрана, а її відхилення у вертикальній площині – знаходитися у межах ±5–10°. Оптимальний огляд у горизонтальній площині від центральної осі екрана у межах ±15–30°. Лише під час спостереження за інформацією, яка розміщена у найвіддаленіших ділянках екрану, кут огляду становить 40–45°.

Кут розглядання цифр та букв на екрані монітора не менше 20 кутових хвилин, а його величину розраховують за формулою 4.1 [11]:

$$tg\ \alpha\ /\ 2 = \frac{S}{2L},$$

Формула (4.1)

де S – висота букви або цифри, мм;

L – відстань від очей до об'єкта інформації на екрані, мм;

 – кут розглядання, кутові хвилини.

Оптимальна відстань від очей до площини екрана монітора складає 600 – 700 мм, допустима – не менше 500 мм. Розглядати інформацію на екрані з відстані менш, ніж 500 мм не рекомендується.

4.2 Організація служби охорони праці на підприємстві

Роботодавець зобов'язаний згідно Закону України «Про охорону праці» стаття 13 «Управління охороною праці та обов’язки роботодавця» створити на робочому місці в кожному структурному підрозділі умови праці відповідно до нормативно-правових актів, а також забезпечити додержання вимог законодавства щодо прав працівників у галузі охорони праці.

Із цією метою роботодавець забезпечує функціонування системи управління охороною праці, а саме:

– створює відповідні служби і призначає посадових осіб, які забезпечують вирішення конкретних питань охорони праці, затверджує інструкції про їхні обов'язки, права та відповідальність за виконання покладених на них функцій, а також контролює їх додержання;

– розробляє за участю сторін колективного договору і реалізує комплексні заходи для досягнення встановлених нормативів та підвищення існуючого рівня охорони праці;

– забезпечує виконання необхідних профілактичних заходів відповідно до обставин, що змінюються;

– впроваджує прогресивні технології, досягнення науки і техніки, засоби механізації та автоматизації виробництва, вимоги ергономіки, позитивний досвід з охорони праці тощо;

– забезпечує належне утримання будівель та споруд, виробничого обладнання та устаткування, моніторинг за їх технічним станом;

– забезпечує усунення причин, що призводять до нещасних випадків, професійних захворювань, та здійснення профілактичних заходів, визначених комісіями за підсумками розслідування цих причин;

– організовує проведення аудиту охорони праці, лабораторних досліджень умов праці, оцінку технічного стану виробничого обладнання та устаткування, атестацій робочих місць на відповідність нормативно-правовим актам з охорони праці в порядку і строки, що визначаються законодавством, та за їх підсумками вживає заходів з усунення небезпечних і шкідливих для здоров'я виробничих факторів;

– розробляє і затверджує положення, інструкції, інші акти з охорони праці, що діють у межах підприємства та встановлюють правила виконання робіт і поведінки працівників на території підприємства, у виробничих приміщеннях, на будівельних майданчиках, робочих місцях відповідно до нормативно-правових актів з охорони праці, забезпечує безоплатно працівників нормативно-правовими актами підприємства з охорони праці;

– здійснює контроль за додержанням працівником технологічних процесів, правил поведінки з машинами, механізмами, устаткуванням та іншими засобами виробництва, використанням засобів колективного та індивідуального захисту, виконанням робіт відповідно до вимог з охорони праці.

Спеціалісти служби охорони праці у разі виявлення порушень охорони праці мають право:

– видавати керівникам структурних підрозділів підприємства обов'язкові для виконання приписи щодо усунення наявних недоліків, одержувати від них необхідні відомості, документацію і пояснення з питань охорони праці;

– вимагати відсторонення від роботи осіб, які не пройшли передбачених законодавством медичного огляду, навчання, інструктажу, перевірки знань і не мають допуску до відповідних робіт або не виконують вимог нормативно- правових актів з охорони праці;

– зупиняти роботу виробництва, дільниці, машин, механізмів, устаткування та інших засобів виробництва у разі порушень, які створюють загрозу життю або здоров'ю працівників;

– надсилати роботодавцю подання про притягнення до відповідальності працівників, які порушують вимоги щодо охорони праці.

Ліквідація служби охорони праці допускається тільки у разі ліквідації підприємства чи припинення використання найманої праці фізичною особою.

Законодавство про охорону праці передбачає і обов'язки працівників.

Зокрема вони зобов'язані:

– дбати про особисту безпеку і здоров'я, а також про безпеку і здоров'я оточуючих людей у процесі виконання будь-яких робіт під час перебування на території підприємства;

– знати і виконувати вимоги нормативно-правових актів з охорони праці, правила поведінки з машинами, механізмами, устаткуванням та іншими засобами виробництва, користуватися засобами колективного та індивідуального захисту;

– проходити у встановленому законодавством порядку попередні та періодичні медичні огляди.

Працівник несе безпосередню відповідальність за порушення зазначених вимог. Дотримання правил безпеки і виробничої санітарії залежить не тільки від виконання роботодавцем своїх обов'язків, а й від того, наскільки кожен працівник знає і виконує правила під час роботи. Тому всі працівники при прийомі на роботу і в процесі роботи проходять на підприємстві інструктаж з охорони праці, надання першої медичної допомоги потерпілим від нещасних випадків, правил поведінки при виникненні аварій.

Навчання й інструктаж працівників з охорони праці є складовою частиною системи управління охороною праці і проводиться з усіма працівниками в процесі їхньої трудової діяльності. Інструктаж працівників залежно від характеру та часу його проведення буває вступний (при прийомі на роботу); первинний (на робочому місці з усіма працівниками: на роботах із підвищеною небезпекою - один раз на квартал, на інших роботах — один раз на півроку; проводиться або індивідуально, або з групою працівників, що виконують однотипні роботи, за програмою первинного інструктажу); позаплановий (при зміні правил з охорони праці, заміні устаткування чи за інших змін факторів, що впливають на безпеку праці); цільовий (при виконанні разових робіт, не пов'язаних із прямими обов'язками за фахом).

ВИСНОВОК

Комплексна система захисту інформації на підприємствах являєтеся однією з найнеобхідніших елементів збереження, створення та редагування інформації у них. Створення КСЗІ першочерговим етапом у формуванні надійного захисту на підприємстві, адже комплекс заходів, що потрібний для впровадження, визначається стратегією, котра формує подальші дії підприємства в частині формування інженерно-технічних заходів.

Слід розуміти, що із розвитком сучасних технологій, котрі дозволяють здійснювати різного типу атаки, здійснювати підбір ключових шифрів до систем авторизації, а також створювати варіативні способи проникнення до підсистем, котрі містять інформацію, створює необхідність постійного розвитку технічних можливостей підприємства для збереження інформації в цілому.

Під час дослідження було встановлено основні завдання, які покладаються на осіб, котрі відповідальні за постійний захисту інформації, створення принципу його безперервності, мають також дотримуватись принципу гнучкої системи захисту, метою якого виступає практичність для усіх користувачів. Працівникам системи слід використовувати алгоритми авторизації, автентифікації, адже це призводить до покращення структури функціонуючих алгоритмів, та стратегії захисту інформації, це також створить принцип простого захисту котрий не потребує, додаткових витрат для підприємства, не спричинить ускладненого навчання користувачів із даною підсистемою, а також буде сприяти можливостям зміни системи захисту інформації у випадку виявлення непередбачуваних ситуацій.

Це безпосередньо створить умови у використанні баз даних та інформації, здійснить можливість правильного застосування та відтворення спільних даних і не створить складного алгоритму користування спільною інформацією, що міститься на одному сховищі, чи ресурсі.

У результаті проведеної роботи виявлено, що важливою частиною КСЗІ, являєтеся саме політика відновлення, адже при порушенні функціонування системи, особи відповідальні за захист даних повинні здійснити заходи та дії, які

передбаченні протоколом, для адміністрування таких даних, а також для унеможливлення витоку інформації із баз даних, або автоматичного відтворення інформації поза межами рідного середовища. Дані аспекти повинні бути враховані при розробці середовища конфігурації інформації, при здійсненні розробки технічної підтримки системи захисту інформації, а також повинно пройти попередні випробування, що в свою чергу наблизить користувача до аналізу на вимоги приналежності машинної обробки, інформації системної обробки, протокольного доступу, а також надасть змогу здійснити доопрацювання, щодо політики безпеки інформації в середовищі.

Ці вище переліченні аспекти необхідні не тільки для створення уже цілісної і комплексної системи захисту інформації та задля створення базових моделей загроз, аналізу структури комплексної системи захисту інформації, з метою моделювання. Тестування підвідомчих мереж на підприємстві, створення та супровід технічних основ обраної на підприємстві моделі комплексної системи захисту інформації залежить від попередньо обраної моделі стратегії.

На стадії експлуатації системи захисту інформації слід першочергово створювати особливості верифікації входу, проводити аналіз, на здійснення можливості витоку інформації на базі першочергово порушника підсистеми захисту інформації, серед яких виділяють першочергово саме розробника чи користувача такої підсистеми, а також слід створювати можливість для здійснення запуску фіксованого набору завдання на етапі найменшого коливання в середовищі, адже такі коливання, як правило створюється при наявності загрози здійснення спроби редагування програмного забезпечення на можливість повернення фрейм системи, чи на внесенні неправдивих даних до системи автентифікації, чи при запуску автоматичного підбору(генератору) паролей з метою авторизації у системі та необхідності отримання інформації у незаконний спосіб.

Після проведення дій із влаштування атак на систему захисту інформації, яка міститься у Великоберезовицькій селищній раді, було виявлено ряд проблем із захистом інформації, а саме проблему із захищеними каналами зв’язку такими як VPN, Cisco anyconnect, котрі на стадії авторизації при неправильній

авторизації налагоджують канал зв’язку із доменом сервера, без застосування протоколу захисту інформації, а задля усунення помилки необхідно імпортувати в сховище сертифікатів операційної системи сертифікат сертифікаційного центру що діяв раніше, після чого також було здійснено модернізацію програмного забезпечення, безпосередньо скориговано політику безпеки середовища.

Розв’язання виявлених проблем дозволить органу місцевого самоврядування розв’язати проблему комплексної системи захисту інформації, а також попередити пошкодження цілісності інформації її втрату та надасть можливість ефективніше виявляти втручання в підсистему.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Деякі питання документування управлінської діяльності. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/55-2018-п.#Text (дата звернення: 30.05.2024).
2. Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text (дата звернення: 30.05.2024).
3. Зразки проектів професійних стандартів. Кваліфікаційний центр інформаційних технологій та кібербезпеки ДержНДІ технологій кібербезпеки. URL: https://qc.csi.cip.gov.ua/uk/pages/dev-sampl (дата звернення: 30.05.2024).
4. Інститут інформації, безпеки і права Національної академії правових наук України. URL: https://ippi.org.ua/sites/default/files/2023-8.pdf (дата звернення: 30.05.2024).
5. ІПС ЛІГА:ЗАКОН - система пошуку, аналізу та моніторингу нормативно-правової бази. URL: https://ips.ligazakon.net/document/LG1WZ00A (дата звернення: 30.05.2024).
6. Електронне урядування та електронна демократія: навч. посіб.: у 15 ч. / за заг. ред. А.І. Семенченка, В.М. Дрешпака. – К., 2017. Частина 9: Електронний документообіг. Реінжиніринг адміністративних процесів в органах публічної влади / [С.П. Кандзюба, Р.М. Матвійчук, Я.М. Сидорович, П.М. Мусієнко]. – К.: ФОП Москаленко О. М., 2017. – 64 с.
7. Бекер, І., Тимощук, В., Маслянка, Т., & Тимощук, Д. (2023). МЕТОДИКА ЗАХИСТУ ВІД ПОВІЛЬНИХ ТА ШВИДКИХ BRUTE-FORCE АТАК НА IMAP СЕРВЕР. Матеріали конференцій МНЛ, (17 листопада 2023 р., м. Львів), 275-276.
8. Ванца, В., Тимощук, В., Стебельський, М., & Тимощук, Д. (2023). МЕТОДИ МІНІМІЗАЦІЇ ВПЛИВУ SLOWLORIS АТАК НА ВЕБСЕРВЕР. Матеріали конференцій МЦНД, (03.11. 2023; Суми, Україна), 119-120.

9. Про Державну службу спеціального зв'язку та захисту інформації України. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 30.05.2024).

10. Про електронні документи та електронний документообіг. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 30.05.2024).

11. Про електронну ідентифікацію та електронні довірчі послуги. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 30.05.2024).

12. Про електронну ідентифікацію та електронні довірчі послуги. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 30.05.2024).

13. Про захист інформації в інформаційно-комунікаційних системах. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 30.05.2024).

14. Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/3-2002-п#Text (дата звернення: 30.05.2024).

15. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України". Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/96/2016.#Text (дата звернення: 30.05.2024).

16. Рада національної безпеки і оборони України. Рада національної безпеки і оборони України. URL: https://www.rnbo.gov.ua/ua/Ukazy/417.html (дата звернення: 30.05.2024).

17. Деркач, М. В., Хомишин, В. Г., & Гудзенко, В. О. ТЕСТУВАННЯ БЕЗПЕКИ ВЕБРЕСУРСУ НА БАЗІ ІНСТРУМЕНТІВ ДЛЯ СКАНУВАННЯ ТА ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ.

18. ТЗІ - інформаційна безпека та захист інформації. URL: https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf (дата звернення: 30.05.2024).

19. Іваночко, Н., Тимощук, В., Букатка, С., & Тимощук, Д. (2023). РОЗРОБКА ТА ВПРОВАДЖЕННЯ ЗАХОДІВ ЗАХИСТУ ВІД UDP FLOOD АТАК НА DNS СЕРВЕР. Матеріали конференцій МНЛ, (3 листопада 2023 р., м. Вінниця), 177-178.

20. Демчук, В., Тимощук, В., & Тимощук, Д. (2023). ЗАСОБИ МІНІМІЗАЦІЇ ВПЛИВУ SYN FLOOD АТАК. Collection of scientific papers «SCIENTIA», (November 24, 2023; Kraków, Poland), 130-130.

21. Чирський Ю.В. Запровадження системи електронного документообігу в Україні. URL: http://old.minjust.gov.ua/7546 (дата звернення: 30.05.2024).

22. Що таке електронне урядування? (поширення практик електронного урядування в бібліотеках) : методичні поради / Ярмолинецька ЦРБ, уклад. Слободян О.Л. – Ярмолинці, 2014. – 16 с.

23. Kulchytskyi, T., Rezvorovych, K., Povalena, M., Dutchak, S., & Kramar, R. (2024). LEGAL REGULATION OF CYBERSECURITY IN THE CONTEXT OF THE DIGITAL TRANSFORMATION OF UKRAINIAN SOCIETY. Lex Humana (ISSN 2175-0947), 16(1), 443-460.

24. T. Lechachenko, R. Kozak, Y. Skorenkyy, O. Kramar, O. Karelina. Cybersecurity Aspects of Smart Manufacturing Transition to Industry 5.0 Model. CEUR Workshop Proceedings, 2023, 3628, pp. 325–3