Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії

Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній ступінь (освітньо-кваліфікаційний рівень))

на тему: Дослідження безпеки операційних систем інформаційно-комунікаційної системи ТОВ «Телесвіт»

Виконала: студентка IV курсу, групи СБс 42

спеціальності (напряму підготовки) 125 Кібербезпека
(шифр і назва спеціальності (напряму підготовки))

_____ Занько К.В.
(підпис) (прізвище та ініціали)

Керівник _____ Муж В.В.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Кареліна О.В
(підпис) (прізвище та ініціали)

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

Рецензент _____ _____
(підпис) (прізвище та ініціали)

Завідувач кафедри _____

м. Тернопіль – 2021

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В
(підпис) (прізвище та ініціали)
« » _____ 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

студентці Занько Катерині Віталіївні
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження безпеки операційних систем інформаційно-комунікаційної системи ТОВ «Телесвіт»

Керівник роботи Муж Валерій Вікторович кандидат юридичних наук, доцент кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «16» лютого 2021 року № 4/7-114

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи технічна документація, інтернет-джерела.

4. Зміст роботи (перелік питань, які потрібно розробити)

1. ХАРАКТЕРИСТИКА ТА ІНФОРМАЦІЙНА ДІЯЛЬНІСТЬ ПІДПРИЄМСТВА
2. АНАЛІЗ ЗАГРОЗ
3. РЕКОМЕНДАЦІЇ

.

Безпека життєдіяльності, основи охорони праці. Діяльність. Її види ти розуміння в безпеці праці. Психологічні чинники небезпеки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Гурик О.Я., доцент кафедри МТ		

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	16.02 – 19.02	*Виконано*
2.	Підбір джерел про загрози мережевій безпеці	16.02 – 19.02	*Виконано*
3.	Опрацювання джерел про загрози мережевій безпеці	19.02 – 02.03	*Виконано*
4.	Підбір джерел про існуючі засоби захисту мережевої інфраструктури	02.03 – 10.03	*Виконано*
5.	Опрацювання джерел про існуючі засоби захисту мережевої інфраструктури	10.03 – 16.03	*Виконано*
6.	Аналіз діяльності підприємства	16.03 – 01.04	*Виконано*
7.	Розробка політик безпеки	01.04 – 10.04	*Виконано*
8.	Вибір програмно-апаратних засобів	10.04 – 16.04	*Виконано*
9.	Оформлення розділу «Огляд мережевих систем»	16.04 – 25.04	*Виконано*
10.	Оформлення розділу «Дослідження об’єкта діяльності»	25.04 – 05.05	*Виконано*
11.	Оформлення розділу «Побудова мережевої системи безпеки»	05.05 – 16.05	*Виконано*
12.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи хорони праці»	16.05 – 22.05	*Виконано*
13.	Оформлення кваліфікаційної роботи	22.05 – 08.06	*Виконано*
14.	Нормоконтроль	08.06 – 10.06	*Виконано*
15.	Перевірка на плагіат	10.06 – 16.06	*Виконано*
16.	Попередній захист кваліфікаційної роботи	16.06 – 19.06	*Виконано*
17.	Захист кваліфікаційної роботи	24.06	

Студентка _____ *Занько К.В.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Муж В.В.*
(підпис) (прізвище та ініціали)

Анотація

Дослідження безпеки операційних систем інформаційно-комунікаційної системи ТОВ «Телесвіт»// Кваліфікаційна робота освітнього рівня «Бакалавр» // Занько Катерина Віталіївна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-42 // Тернопіль, 2021 // С.56 , рис. – 12, табл. – 3, кресл. – 0, додат. – 0, бібліогр. – 20.

Ключові слова: операційні системи, ІКС, інформаційна безпека, політики безпеки, модель порушника.

Кваліфікаційна робота присвячена питанню по дослідженню безпеки операційних систем.

Мета роботи полягає у вивченні та використанні сучасних технологій у забезпечені інформаційної безпеки для здобуття досвіду задля працевлаштування в майбутньому на одну з наступних позицій: «Адміністратор безпеки», «Аналітик кібербезпеки» чи «Системний адміністратор».

В першому розділі кваліфікаційної роботи досліджується інформаційна діяльність, структура та інформаційно-комунікаційна система філії ТзОВ «Телесвіт» телекомунікаційної компанії Воля.

В другому розділі кваліфікаційної роботи досліджуються та проводиться аналіз загроз. В ході роботи розробляється модель порушника.

В третьому розділі розробляються політики безпеки, а також надаються рекомендації щодо посилення безпеки діючих в ІКС операційних систем.

.

ANNOTATION

Operation systems safety study of LLC “Telesvit” information-communication system // Qualification work of the educational level «Bachelor» // Zanko Kateryna // Ternopil National Technical University named after Ivan Pulyuy, Faculty of Computer Information Systems and Software Engineering // Ternopil, 2021 // Explanatory note size –pages 56, illustrations, tables , bibliography items .

Keywords: operating systems, ICS, information security, security policy, message model.

Qualification work is devoted to the study of the security of operating systems of information and communication system of LLC "Telesvit".

The purpose of the work is to study and use modern technologies in information security to gain experience for future employment in one of the following positions: "Security Administrator", "Cyber Security Analyst" or "System Administrator".

In the first section of the qualification work the information activity, structure and information-communication system of the branch of the telecommunication company Volya are investigated.

The second section of the qualification work examines and analyzes threats. In the course of work the model of the violator is developed.

The third section develops security policies and provides recommendations for enhancing the security of operating systems operating in ICS.

ЗМІСТ

ЗМІСТ 6

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 8

ВСТУП 9

1. ХАРАКТЕРИСТИКА ТА ІНФОРМАЦІЙНА ДІЯЛЬНІСТЬ ПІДПРИЄМСТВА ... 11

1.1 Структури управління та основних видів діяльності підприємства та його підрозділів. 11

1.1.1 Структура компанії 11

1.1 Функції інформаційно-комунікаційної системи підприємства. 14

1.3 Характеристика об’єктів інформаційної діяльності та виду інформації, яка на них обробляється. 15

1.4 Топологія мережі і модель мережі підприємства 16

1.5 Обладнання 18

1.5 Програмне забезпечення 20

1.6. Класифікація автоматизованої системи 21

2 АНАЛІЗ ЗАГРОЗ 23

2.1 Підготовчий етап. Короткий огляд об’єктів захисту 23

2.2 Розширена система оборони Defense in depth 25

2.3 Модель порушника 26

2.4 Визначення загроз 28

3 РЕКОМЕНДАЦІЙНИЙ РОЗДІЛ 35

3.1 Політика безпеки 35

3.1.1 Політика та процедури безпеки операційної системи 35

3.1.2 Політика контролю доступу (ACP) 36

3.1.3 Перелік правил 36

3.2 Загартовування/ посилення безпеки в ОС 39
3.2.1 Посилення безпеки ОС сімейства Windows 39
3.2.2 Посилення безпеки ExtremeXOS 43
4. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ 48
4.1. Діяльність. Її види ти розуміння в безпеці праці. 48
4.2. Вимоги безпеки до робочих місць виконання робіт. 50
ВИСНОВКИ 55

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ВОЛЗ – волоконно-оптичні лінії зв’язку;

ІБ – інформаційна безпека;

ІКС – інформаційно –комунікаційна система

ІС – інформаційна система;

ІТС – інформаційно-телекомунікаційна система

КС – комп'ютерна система;

НД – нормативний документ;

ОС – операційна система;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

ТзОВ – товариство з обмеженою відповідальністю;

ACL – Access Control List(списки контролю доступу)

ВСТУП

Технологічні досягнення, котрі й досі не стоять на місці призвели до майже невідворотного використання гаджетів в повсякденному житті людей і також не є винятками для використання в організаціях різного типу. Організаціям все зручніше користуватися комп'ютерними системами для обробки своєї інформації.

Багато людей досі не мають уявлення про важливість інформаційної безпеки, особливо, для компаній. Не мало керівників мають хибне уявлення про те, що їх інформація повністю захищена та не містить жодних загроз . І це велика помилка! Одного разу радник американських президентів з питань безпеки в кіберпросторі Річард Кларк досить різко висловився – «Якщо ви витрачаєте більше на каву, ніж на ІТ-безпеку, вас зламають. Більше того, ви заслуговуєте на те, щоб вас зламали!»

І навіть в ситуації, коли компанія вживає заходів, але не оновлюючи їх століттями, не можна сподіватись на те, що дані ніхто не поцупить.

Інформаційно-комунікаційна система підприємств є дуже громіздкою і багатосекторною. Для того, щоб вона була безпечною потрібно весь час проводити дослідження різних систем на безпеку.

Зловмисники не сидять склавши руки, з розвитком технологій кібератаки теж швидко поновлюються. Компаніям особливо потрібно зважати на важливість внутрішньої інформації яка протікає в установі та її участі у власному капіталі,тому що через неакуратність поводження з інформацією і нехнуванням забезпеченням безпеки інформації. Якщо їй заподіяно шкоду, це може мати ефект доміно , що спричиняє кілька неприємних наслідків, таких як пошкодження іміджу компанії, викриття секретів, а також вплив на плани. І без різниці велика компанія чи ні це може призвести навіть до банкрутства установи.

Задля упередження наслідків викрадення інформації або хоча б зменшення розмір втрат, дослідження операційних систем ІКС ТзОВ «Телесвіт» є актуальним і через те, що операційні систем складаються з величезної кількості компонентів, які не завжди добре відтестовані, а тому залишають «дири» в безпеці інформаційно-комунікаційних систем.

Відповідно актуальність даної роботи полягає в тому, що проведений науково обґрунтований аналіз можливих та потенційних загроз захисту інформації в ІКС на базі індивідуально визначеного підприємства з урахуванням особливостей інформації, яка підлягає захисту. Даний підхід дозволяє провести аналіз загроз не тільки для цього підприємства, а й для всіх типових в Україні.

Об’єкт дослідження: засади захисту інформації в інформаційно-телекомунікаційній системі підприємства.

Предмет дослідження : дослідження безпеки операційних систем інформаційно-комунікаційної системи ТОВ «Телесвіт»

Мета: дослідити проблемні питання захисту інформаціх на обєктах інформаційної діяльності та інформаційних системах наприкладі юридичної особи.

В рамках даного дослідження поставлено наступні завдання:

1) закріпити теоретичні знання з обстеження об’єкта інформаційної діяльності та отримати навички практичного застосовування системного підходу до розробки комплексу організаційних заходів захисту інформації, враховуючи особливості функціонування підприємства та вирішуваних ним завдань;
2) дослідити ІКС підприємства;
3) формування уміння аналізу загроз інформації та отримання практичних навичок аналізу протиправних дій в системі та розробки моделей порушника та загроз;
4) розробити політики безпеки.

1. ХАРАКТЕРИСТИКА ТА ІНФОРМАЦІЙНА ДІЯЛЬНІСТЬ ПІДПРИЄМСТВА

1.1 Структури управління та основних видів діяльності підприємства та його підрозділів.

Для написання кваліфікаційної роботи, досліджуватиметься Тернопільська філія ТзОВ «Телесвіт».

Тернопільська філія ТзОВ «Телесвіт» це відокремлений підрозділ групи телекомунікаційних компаній «Воля - кабель», що розташований поза межами головного офісу та здійснює частину її функцій (виконує роботи, надає спектр послуг від імені компанії Воля).

Воля є досвідченим українським телекомунікаційним провайдером, який надає послуги кабельного телебачення, широкосмугового доступу в Інтернет, хостингу серверів та хмарні сервіси. Компанія представлена майже по всій території України в 19 областях та в 34 містах. Проте, в 2012 році, через 10років існування компанії з’явилась і перша тернопільська філія .

У Тернополі ТзОВ «Телесвіт» надає послуги: швидкісного інтернету, кабельного телебачення, надання обладнання в оренду, технічної підтримки користувачів.

1.1.1 Структура компанії

Під організаційною структурою компанії розуміють регульовану сукупність взаємопов'язаних елементів зі стійкими зв’язками між ними, що дозволяють забезпечити їх функціонування і розвиток як однієї цілісності.

У структурі управління є управлінський процес до якого входить потік інформації, а також ухвалення керівничих рішень. Суть процесу заключається в розмежуванні завдань та функцій управління та наділенням відповідальності осіб за їх виконання.

Так як організаційна структура керування філією відображує завдання та цілі організації; об'єм повноважень та функціональний розподіл обов'язків працівників управління і при тому керується політикою, правилами та посадовими інструкціям. То цьому опису підпадає ієрархічний тип структур управління, а саме лінійно-функціональна організаційна структура(див рис.1.1).

Поняття ієрархічної структури управління передбачає чіткість в розподілі праці, ієрархічну модель управління, існування формальних норм і правил та здійснення процедури найму відбувається відповідно до кваліфікаційних вимог до посади.

В основі лінійно-функціональної організаційної структури покладений принцип зв'язного графа без циклів – дерево. Цей принцип дає можливість розділити спеціалізації управлінського процесу по функціональним підсистемам організації і по кожній з них сформувати ієрархію .

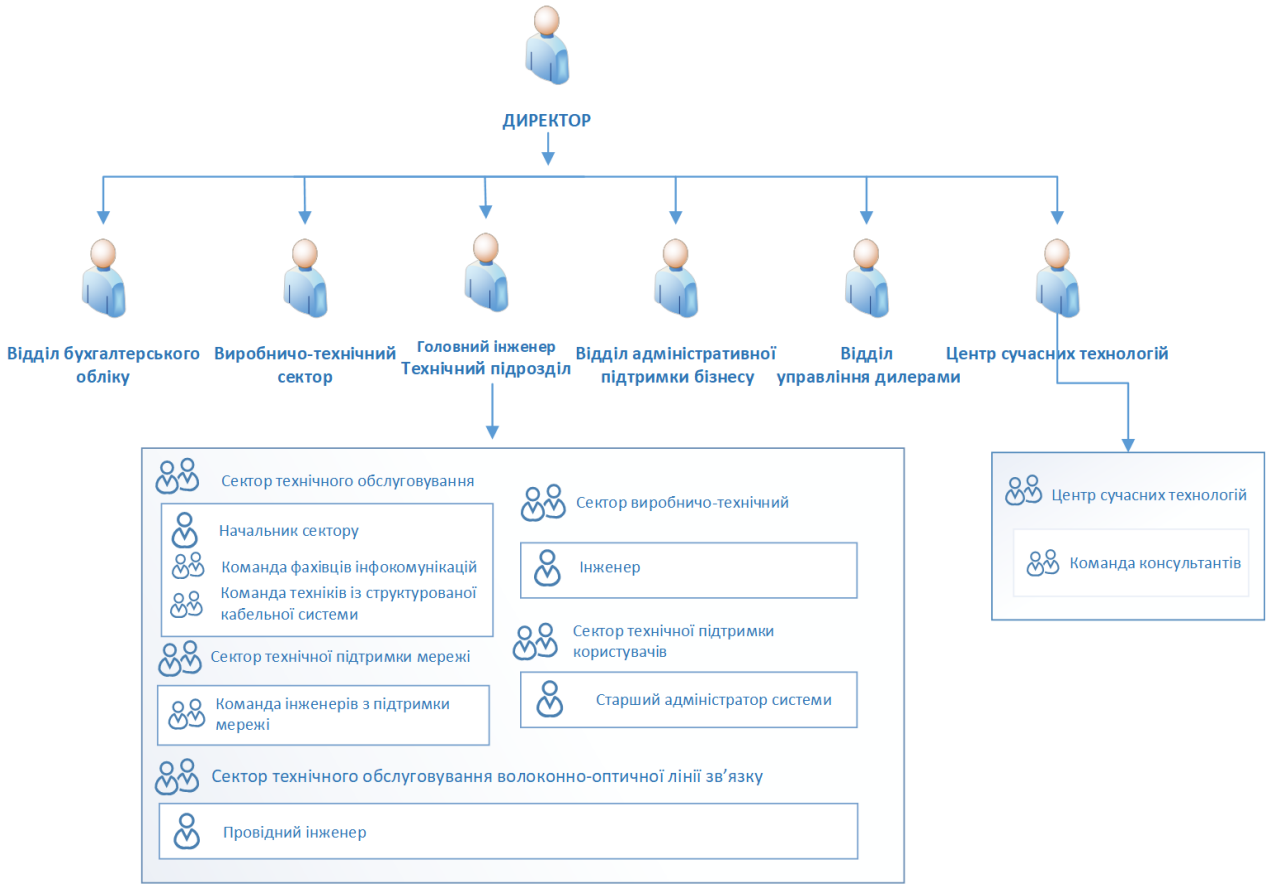

Рисунок 1.1 - Структура філії ТзОВ «Телесвіт»

Детальніше розглянемо структуру технічного підрозділу це в ході дослідження загроз допоможе сформулювати уявлення про користувачів системи.

Технічний підрозділ включає в себе п’ять секторів, кожен з яких виконує конкретно свої завдання.

Сектор технічного обслуговування.

Сектор технічного обслуговування складається з команди фахівців інфокомунікацій, команди техніків із структурованої кабельної системи та керівника який контролює роботу цього сектору.

Завданнями сектору технічного обслуговування є: проведення контролю роботи інформаційно-телекомунікаційних систем та технічного обслуговування відповідно до завдань, поставлених інженером; оброблення статистичних даних(результатів вимірювань параметрів ІКС), виявлення пошкоджень та аварій на системному устаткуванні; оформлення технічних паспортів ІКС.

Сектор технічної підтримки мережі.

В обов'язки спеціаліста технічної підтримки мережі входить робота з UNIX та іншими мережами, серверами, внутрішніми корпоративними IT-системами, проведення консультацій користувачам з питань IT, початкове адміністрування мережі, забезпечення функціонування робочих станцій, проведення регламентних робіт по догляду за обладнанням,моніторинг працездатності програмного забезпечення робочих станцій користувача, планування і реалізація стратегії безпеки для захисту даних і загальних мережевих ресурсів, і тп.

Сектор технічного обслуговування волоконно-оптичного зв’язку (ВОЛЗ).

До завдань технічного обслуговування ВОЛЗ відносяться : незалежна інвентаризація і паспортизація ВОЛЗ, застосування програмного продукту для інвентаризації кабельних систем ліній, проведення регламентних робіт по забезпеченню інформації про мережу ВОЛЗ і підтримці в робочому стані відповідно до технічних норм, планування, реєстрація подій і робіт на мережі в єдиній інформаційній системі, забезпечення 365/24 доступу до інформаційної системи, застосування систем автоматичного моніторингу ВОЛЗ, контроль параметрів кабельних ліній, проведення робіт із захисту кабелів від механічних пошкоджень,

усунення місць зниження ізоляції оболонки кабелю, аварійно-відновлювальні роботи, та інші.

Виробничо-технічний сектор.

Виробничо-технічний сектор вираховує вартість виконаних робіт і витрат; складає звітність по обсягу виконаних робіт; складає акти на виконані роботи і довідки про вартість виконаних робіт;своєчасно надає замовникам необхідні технологічні документи, паспорти і сертифікати на використовувані матеріали, тощо.

Сектор технічної підтримки користувачів.

Робота консультантів техпідтримки заключається в культурному обслуговуванні клієнтів, у вживанні заходів для запобігання і уникнення конфліктних ситуацій, інформуванні з питань наявних послуг. Також важливим обов'язком є звітування керівництву підприємства про наявні недоліки в організації обслуговування відвідувачів.

Сектор технічної підтримки користувачів забезпечує роботу з ефективного і культурного обслуговування відвідувачів. Створює для них комфортні умови. Здійснює контроль за збереженням матеріальних цінностей. Консультує відвідувачів з питань наявних послуг. Вживає заходів щодо запобігання і ліквідації конфліктних ситуацій. Розглядає претензії, пов'язані з незадовільним обслуговуванням відвідувачів, і вживає відповідних організаційно-технічних заходів. Інформує керівництво підприємства про наявні недоліки в організації обслуговування відвідувачів, вживає заходів щодо їх ліквідації, здійснює контроль за виконанням працівниками вказівок керівництва підприємства.

1.1 Функції інформаційно-комунікаційної системи підприємства.

Інформаційно-комунікаційна система (ІКС) – комплекс із інформаційних і телекомунікаційних систем, які діють спільно та призначені для ефективнішої передачі інформації та кращої організації роботи функцій підрозділів. Основними елементами ІКС є: ЕОМ, які використовуються кінцевими користувачами; активне(сервери, маршрутизатори, концентратори, тд.) і пасивне

обладнання(забезпечує з’єднання між активним обладнанням); канали зв’язку; мережеве програмне забезпечення.

Так як ІКС складається з різних програмних та апаратних елементів, які повинні працювати спільно, через це виникає необхідність в, щоб всі елементи розуміли одне одного і дотримувались певних правила. Така сукупність правил, яка забезпечує керування при передачі інформації між двома об’єктами називається протоколом.

Відповідно функціями ІКС буде: встановлення факту з’єднання між двома сторонами, розрахунок оптимального маршруту для передавання даних, далі деяка первинна обробка даних і управління потоком переданої інформації.

1.3 Характеристика об’єктів інформаційної діяльності та виду інформації, яка на них обробляється.

Забезпечувати ефективну комунікацію та обробку інформаційних ресурсів організації є найважливішим завданням ІКС.

Інформаційно-комунікаційна система підприємства за функціональним критерієм(відноситься до тих систем, які забезпечують зберігання та безпечний доступ то інформації) є інформаційною системою. Крім того, діяльність ІКС спрямована і на підтримки бізнес-процесів. Така класифікація ІКС називається інформаційно-аналітичні системи.

Філія компанії, загалом, має довірче керування доступом до інформації, тобто у користувачів є дозвіл керувати доступом до об’єктів свого домену. А власне вже адміністративний доступ до інформації належить безпосередньо «Волі». Тому для отримання особливого доступу до інформації залишається запит на дозвіл до такої інформації. Всі важливі дані зберігаються на захищених серверах в компанії «Воля». Локальні дані філії зберігається на місцевому сервері, а також деякі резервні копії можуть зберігатись в хмарних сервісах.

1.4 Топологія мережі і модель мережі підприємства

Під топологією зазвичай розуміють взаємне розташування відносно один одного вузлів мережі. До вузлів мережі в даному випадку відносяться комп'ютери, мережеве обладнання тощо . Мережева структура, що містить більше двох топологій, називається - гібридна топологія або змішана.

Так як мережа підприємстава є великою і розбита на підмережі, тому тут змішана топологія використовуючи кільце і зірку(див рис.1.2).

Гібридний тип об'єднує в собі переваги цих двох по суті різних типів топологій в одній єдиній топології. Такий підхід дозволяє модифіковуватись відповідно до потреб і є надзвичайно гнучкою. Також до переваг відноситься надійсність, можливість обробки великого трафіку даних, легко масштабованість , оскільки гібридні мережі побудовані таким чином, що дозволяють без зайвих клопотів інтегрувати нові апаратні компоненти. Особливо добре підходить для великих мереж, бо дає можливість безперебійно усунути неполадки.

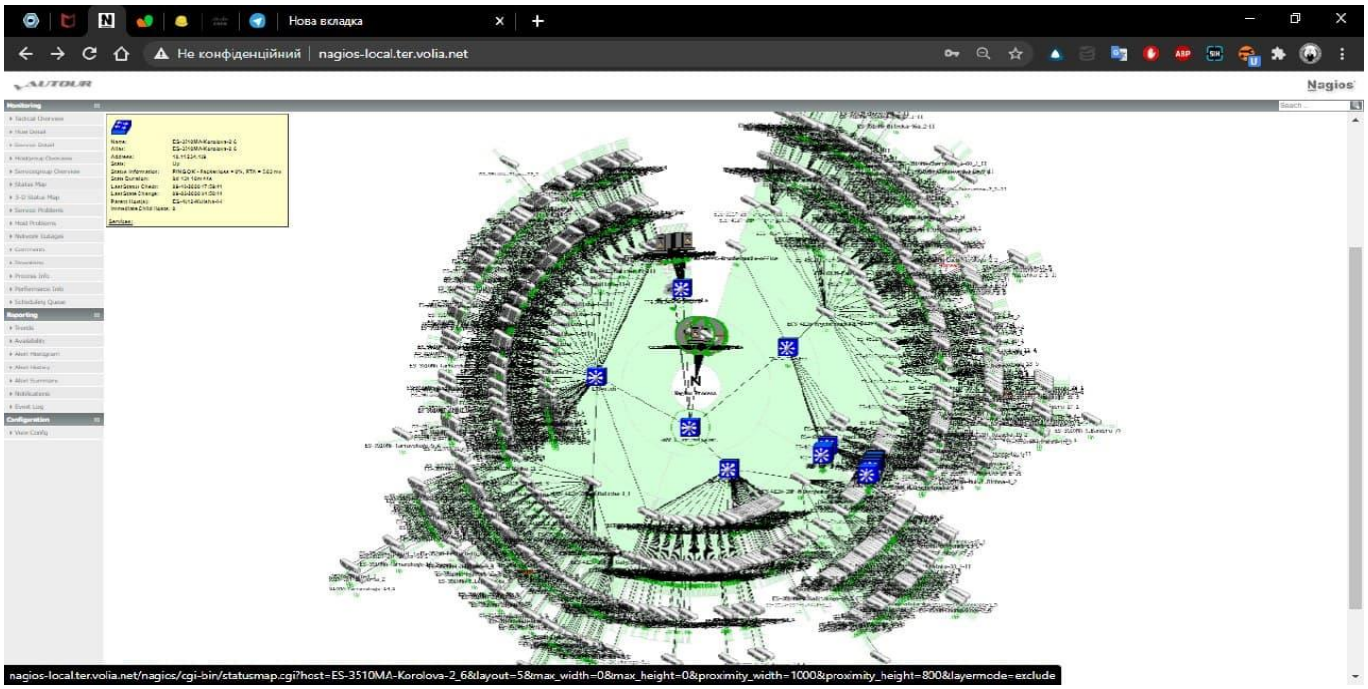

Рисунок 1.2 - Загальний вигляд структури мережі тернопільської філії

На підприємстві використовується ієрархічна модель мережі, яка продемонстрована нище на рисунку 1.3.

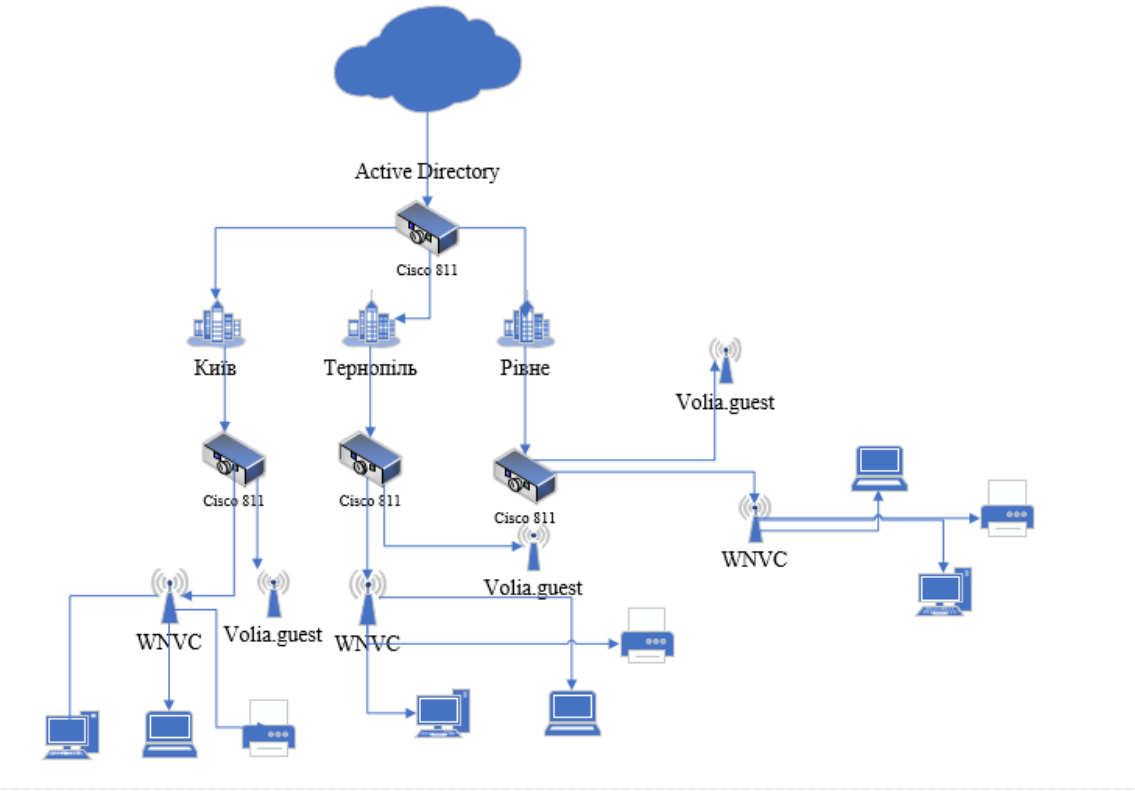

Рисунок 1.3 – Загальна схема мережі

Ієрархічна модель мережі представляє собою трирівневу модель організації мережі компанії. Ця модель запропонована інженерами Cisco Systems . Вона поділяє мережу компанії на три рівні ієрархії: ядро мережі (core layer), рівень розподілу (distribution layer) та рівень доступу (access layer).

Рівень доступу служить для підключення робочих станцій і серверів до мережі компанії. У більшості випадків рівень доступу представлений в мережі комутаторами другого рівня (також в окремих випадках можуть використовуватися і L3-комутатори). Як правило, для організації цього найпростішого рівня ієрархічної моделі встановлюються оптимальні за ціною пристрою, які не потребують складної конфігурації. Основне завдання таких пристроїв - надання доступу робочих станцій і серверів до наступного рівня (розподілу) ієрархії.

Цей рівень є «найрозумнішим» в ієрархічній моделі. На рівні розподілу вирішуються завдання агрегації широкомовних доменів і доменів маршрутизації, фільтрації і налаштування QoS , агрегації великих дротових мереж в комунікаційній «шафі», забезпечення високого рівня доступності ядра для кінцевих користувачів. Маршрутизатори , що використовуються тут також можуть брати на себе функції забезпечення доступу в Інтернет для підрозділів компанії.

Ядро мережі представляє комплекс мережевих пристроїв (маршрутизаторів і комутаторів), що забезпечують резервування каналів і високошвидкісну передачу даних між різними сегментами рівня розподілу.

1.5 Обладнання

Без пристроїв між якими відбувається комунікація (активне обладнання) не можливе існування інформаційно-комунікаційної системи. В організації присутні як і робочі станції користувачів(ПК) так і мережеві пристрої.

З мережевих засобів, які діють на території підприємства- мережеві комутатори, Wi-Fi маршрутизатори, міжмережеві екрани, сервери.

Нище наведено деякі випадки обладнання мережі, яке використовується філією.

а) Міжмережеві екрани Cisco ASA, зокрема Cisco ASA5585-S60F60-K9(рис.1.4)

Cisco ASA(Adaptive Security Appliance) це сімейство захисних пристроїв,

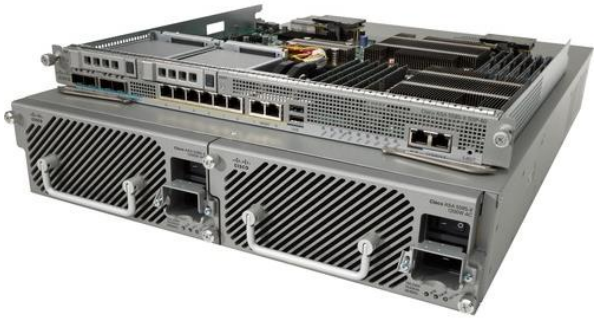

Рисунок 1.4 - Міжмережевий екран Cisco ASA5585-S60F60-K9

для захисту корпоратвних мереж та центрів обробки даних від зовнішніх атак і вторгнень. ASA 5500 Series - це пристрої першої лінії оборони, що забезпечують надійность і безпеку корпоративної мережі.

б) Комутатор Extreme Summit X440-G2-48t-10GE4 (рис.1.5)

Комутатори Extreme Summit - це універсальне рішення для мереж на рівні доступу(access layer), корпоративного сегмента, невеликих центрів обробки даних. Особливістю є гнучкий і широкий діапазон комплектації комутаторів 10/100 / 1000BASE-T портів - до 48 портів. Підтримка технології POE є дає можливість подавати живлення на IP-камери, точки доступу WI-FI та інші пристрої. Низький рівень шуму.

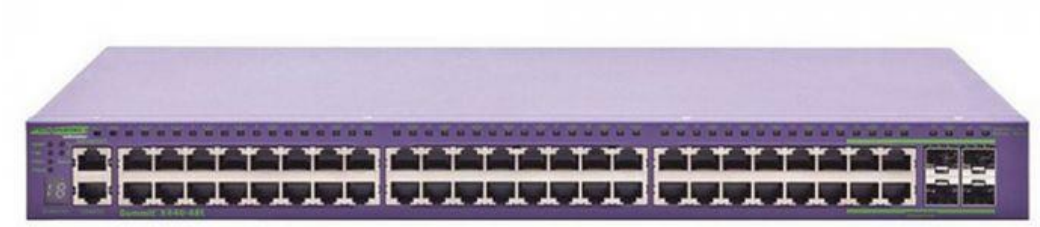

Рисунок 1.5 - Комутатор Extreme Summit X440-G2-48t-10GE4

в) Маршрутизатори Cisco 881-SEC-K9 (див. рис. 1.6)

Маршрутизатори Cisco 880 Series Integrated Services Routers (ISR) поєднують доступ в Інтернет, безпеку, бездротові послуги все в один захищений пристрій, який легкий у використанні і управлінні для малого бізнесу і підприємств невеликих філій і навіть для роботи з віддаленими співробітниками. Серія Cisco 880 забезпечує невеликі офіси, включаючи брандмауер та фільтрацію URL-адрес (Cloud Web Security), фільтрацію вмісту, VPN та бездротові локальні мережі (WLAN) на швидкості широкосмугового зв’язку. Захищє дані - стримує загрози і виявляє шкідливу активність, приховану в зашифрованому трафіку - від рівня периметра до хмари і через будь-яке з'єднання. Дозволяє підключення до 20 користувачів.

Cisco 881 дає можливість централізувати управління, щоб спростити розгортання мереж SD-WAN і засобів їх захисту при збереженні дії політик на

тисячах об'єктів. Cisco SD-WAN технологія для безпечного підключення будь-якого користувача, будь-якої програми в будь-якому місці за допомогою хмарних технологій.

Рисунок 1.6 – Зовнішній вигляд Cisco 881

Ці маршрутизатори мають невеликий форм-фактор через це є невибагливими в розміщенні та мають безвентиляторну конструкцію для більш тихої роботи.

1.5 Програмне забезпечення

Програмне забезпечення відіграє теж значну роль, бо саме завдяки йому пристрої можуть розуміти правила одне одного і комунікувати один із одним.

На підприємстві дотримуються стратегії використання ліцензованих продуктів, тому на всіх робочих станціях встановлені ліцензійні версії операційних систем.

Щодо системного ПЗ, яке використовується для робочих станцій, то здебільшого використовуються операційні системи Microsoft Windows 10 x64, поодинокі випадки Microsoft Windows 8.1 x64. Так як філія має широкоспектровий вид діяльності, також можна знайти комп'ютери, де налаштовані Linux операційні

системи як Fedora x64 та Debian x64. Крім того, для сервера використовується ОС Windows Server 2016.

Нище перераховино короткий перелік прикладного програмного забезпечення, що використовується співробітниками на підприємстві :

- пакет програм Microsoft Office;

- браузери (Google Chrome, Microsoft Edge, Mozila Firefox);

- продукти Nagios – набір інстументів для моніторингу інфраструктури інформаційних технологій та ПЗ всієї організації;для аналізу мережі; для виявлення аномальної поведінки в мережі, що дозволяє розкрити загрозу до її настання, а також дозволяють формувати уявлення про всю інфраструктуру мережі, що забезпечує оперативне реагування на події в системі чи в мережі.

- McAfee Endpoint Security – продукт для захисту кінцевих пристроїв від шкідливого, небажанного ПЗ, що дозволяє реагувати на загрози та керувати ними за допомогою активних засобів захисту та засобів виправлення.

- Foreman - це інструмент для серверів як фізичних так і віртуальних, який спрощує автоматизацію повторюваних задач, пришвидшує розгортання програм та дозволяє керувати серверами локально чи в хмарі.

1.6. Класифікація автоматизованої системи

Згідно НД ТЗІ 2.5-005 -99 – «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» - Автоматизована система(АС) такий комплекс з організаційних і технічних систем, куди як компонент входить ОС, фізичне середовище, персонал та оброблювана інформація. Цей документ виділяє три ієрархічні класи АС.

Автоматизована система філії ТзОВ «Телесвіт» відповідає класу «2».

До класу «2» відносяться локально розміщенні багатокористувачевий комплекси, що здійснюють обробку інформацію різних ступенів обмеження доступу.

В межах кожного класу АС також можна класифікувати класифікувати звертаючи увагу на вимоги до забезпечення певних властивостей інформації. З точки зору безпеки інформацію характеризують за трьома основними власнивостями: конфіденційністю, цілісністю і доступністю. Наприклад властивість конфіденційність говорить про те, що персональні дані чи відомості, які відносяться до комерційної таємниці без дозволу власників інформації не повинні поширюватись. Чи от цілісність – це властивість яка означає, що інформація не піддавалась зміні в ході передачі. Доступність забезпечує невідмовне використання для авторизованих користувачів. Тому у зв’язку з цим, дана АС відноситься до підкласу - автоматизована система, де є підвищення по вимогам до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації . Це є підкласи «х.КЦД».

2 АНАЛІЗ ЗАГРОЗ

2.1 Підготовчий етап. Короткий огляд об’єктів захисту

Перед тим, як розкрити сутність другого розділу, буде висвітлено базові поняття на яких ґрунтуватиметься викладений матеріал.

Так от, щодо операційних систем. Силуетно операційні системи є складними програмами, діють як зв’язний компонент між апаратною складовою та програмною і користувачем. Зазвичай, ОС направленні на ефективний розподіл ресурсами(пам’яттю, застосунками, процесорами, пристроями).

В інформаційно-комунікаційній системі вживаються різні типи ОС Одна операційна система не може бути коректно використана для різних типів пристроїв, саме тому важливо звертати увагу не лише на операційні системи, які використовуються на робочих станціях працівників. Тому на території філії присутні також і серверні ОС – Windows Server 2012, Linux Debian. В порівнянні зі звичайною ОС, серверні платформи, як правило, має змогу обробляти більшу кількість підключень користувачів, більший обсяг пам'яті і може виступати в якості веб-сервера, сервера баз даних та сервера електронної пошти. Вони також є ефективними для управління мережею, а не для одного користувача, що означає, що серверна ОС може обробляти кілька робочих столів.

Так як в інформаційно - комунікаційній системі є пристрої на, яких підтримуються версії Windows 8.1(хоч випусків нових немає, проте ще є підтримка системи до 2022року), то для організації автентифікацій використовується Windows Server 2012 для кращої сумісності.

Linux Debian позиціонує себе як багатоцільова операційна система, яку можна використовувати і для робочих станцій, і для розгортання серверів, і як вбудовану систему. Це є одна із стабільних і безпечних збірок на ядрі Linux. І хоча випуски нових версій операційної системи випускаються, тільки після тестування і коли повністю система працює, та як і решта операційних систем чи великих продуктів – не є застрахованими від збоїв там помилок. Та поки, що Debian навіть не засвітився у списку загальновідомих вразливостей інформаційної безпеки CVE(Common

Vulnerabilities and Exposures), що говорить що система є досить безпечною. Але не треба виключати той факт, що погано сконфігурована система не є вразливою.

Крім цього в ІКС філії наявні мережеві ОС, які керують мережевими пристроями, зокрема, операційна система ExemeXOS(також іноді коротко називають ExOS). Це операційна система розроблена компанією Extreme Networks з нуля, для забезпечення хорошої продуктивності і можливостей, необхідних для всього: від великих хмарних додатків і дата-центрів, до інтелектуальних, складені корпоративних граничних мереж високого рівня. Використовується на мережевих комутаторах Extreme Networks. Безпека важлива і на рівні мережевого обладнання, тому ExOS має вбудовані функції безпеки забезпечують контроль доступу до мережі управління ідентифікацією та захисту мережевого управління. З ExtremeXOS дозволяє розширити можливості мережі за рахунок інтеграції спеціалізованих додатків, таких як пристрої безпеки в мережі, забезпечуючи контроль в мережі, додатків і користувачів.

Загалом безпека будь-якого інформаційного середовища не є одиничним заходом, а по суті є процесом забезпечення принаймні основних властивостей - цілісності, конфіденційності та доступності. Порушення, будь-якої, з властивостей сигналізує, що механізм забезпечення безпеки інформації не є достатньо хорошим.

Порушення конфіденційності - викрадення приватної або конфіденційної інформації, наприклад комерційної таємниці, патентів, виробничих процедур, фінансової інформації тощо.

Порушення цілісності - Несанкціоноване внесення змін до даних, що може мати серйозні непрямі наслідки. Наприклад, можна змінити вихідний код програми, щоб відкрити діри в безпеці в системах користувачів перед тим, як їх опублікувати.

Порушення доступності - несанкціоноване знищення даних, щоб спричинити відмову працездатності системи.

Також захищаючи системи від навмисних атак (внутрішніх чи зовнішніх), від осіб, які навмисно намагаються викрасти інформацію, пошкодити інформацію або іншим чином навмисно заподіяти хаос якимось чином варто не забувати ще про такі типи порушень як:

Викрадення служби(Theft of Service) – це несанкціоноване використання ресурсів, таких як крадіжка циклів процесора, установка демонів(програми в Unix-подібних системах, які запускаються системою в фоновому режимі, зазвичай це робота протоколів), що працюють на несанкціонованому файловому сервері, або працюють як прослуховування телефонних або мережевих сервісів .

Відмова в обслуговуванні, DOS - Заборона чинним користувачам використовувати систему, часто перевантажуючи та перевантажуючи систему надлишком запитів на обслуговування.

Безпека ОС визначається етапами та заходами, які спрямовані на захист ОС, спрямову.чи на захист інформаційних активів від загроз; небажаного, шкідливого ПЗ; вірусів та від віддаленого вторгнення зловмисниками, і тп.

До основних способів по забезпеченню безпеки належать роботи по відслідковуванню та регулярному встановленню оновлень(патчів) з елементами виправлення неполадок в ОС. Також сюди відносяться оновлення ПЗ (особливо важливими є те, яке працює на виявлення, запобігання і фільтрацію небажаної активності в системі); перевірка мережевого трафіку, який надходить і виходить з рамок інфраструктури мережі; хороше адміністрування системи з розподілом користувачів системи, лише з необхідними привілеями.

2.2 Розширена система оборони Defense in depth

На жаль, жити в часи, коли моментально продовжують розвиватися технології та де миттєво поширюється інформація немає єдиного діючого способу, який би захистив все інформаційне середовище від проникнень чи викрадень даних. Тому важливо використовувати розширений підхід по реалізацію оборони, щоб хоча би ускладнити зловмисникам задачу і таким чином відсіяти більшість можливо погано-освічених зловмисників.

Концепція Defense in depth передбачає рівні контрою безпеки, через що дозволяє підвищити рівень виявлення ризику атак, зменшити шанс хакеру отримати доступ.

До захисту рівня даних(data) відносяться заходи спрямовані на використання списків контролю доступу(ACL), складних паролів та стратегії створення резервних копій та можливістю відкату системи.

Рівень застосунків передбачає – загартовування програм, тобто ручні налаштування по встановленню правил поведінки програми з мінімальною кількістю необхідних дозволів.

Рівень хостів відповідає за працездатність кінцевих пристроїв, тому сюди відносяться оновлення безпеки ОС, автентифікацію, антивірусні оновлення.

Мережевий рівень повинен передбачати фільтрацію трафіку, захист граничних маршрутиризаторів, налаштування глобальних і внутрішніх сегментів мережі, створення і використання технологій захищених віртуальних мереж.

І не менш важливим є організаційний рівень, який слугує для підвищення обізнаності персоналу на цьому рівні працюють політики безпеки, проведення ознайомчих бесід.

2.3 Модель порушника

Для дослідження безпеки якоїсь системи часто відповідальні за неї схиляються до розробки моделі порушника, аби проаналізувати та сформувати уявлення від кого і чому потрібно захищати інформацію, причини(мотиви), збагнути який досвід має потенційний порушник. Треба, визначити, що порушником є той хто перевищив свої повноваження і отримав доступ до інформації в системі.

Для створення моделі поведінки порушника нище приведені класифікації по різному типу.

За типом дій користувача в системі, що привели до порушення безпеки – випадкові та навмисно націлені.

За класифікацією осіб, які в змозі здійснити порушення – внутрішні та зовнішні. Це ті порушники, які за якихось умов отримали або мають доступ до приміщення з обладнанням на якому є ОС.

До внутрішніх осіб відносяться працівники з різними привілеями доступу:

- системний адміністратор,
- адміністратор безпеки
- бухгалтерський відділ,
- консультант,
- технічний персонал,
- обслуговуючий.

До зовнішніх можна віднесити клієнтів, сторонніх осіб, кур'єрів та представників організацій.

Також можна категоризувати по мірі знань і вмінь:

- недосвідчений користувач системи (наприклад новий працівник, який становить низький потенціал загрози чи здійснення атаки),
- досвідчений користувач системи
- експерт(наприклад спецслужби).

Недосвідчений користувач через свою необізнаність може своїми діями ненавмисно нашкодити системі, тим самим зробити систему вразливою, але це все ще є низьким потенціалом для проведення атак. Для упередження таких дій використовують розмежування користувачів з різними політиками безпеки.

Досвідчені користувачі систем становлять низький або середній потенціал для здійснення порушення. До низького потенціалу відносяться ті користувачі які добре володіють і знають структуру операційних систем, їх особливості, проте використовують загальнодоступні засоби і методи з інтернету(можливо застарілі). До середнього потенціалу вже відносяться ті користувачі, які вміють проводити аналіз ПЗ, співставляти дані, знаходити і застосовувати на практиці вразливості.

Експерти в порівнянні з попередніми є найбільш загрозливим представником порушника. Експерти з високим потенціалом вміють заносити програмно-технічні закладки, застосовують спеціальні засоби проникнення в систему і проводять спеціальні дослідження.

Також можна специфікувати дії порушника за часом:

- в неробочий(бездіяльний) час системи,

- під час роботи користувача в системі.

Ця класифікація сформована для нагадування, що при адмініструванні системипотрібно ускладнити порушнику доступ до системи і налаштуати мінімальне число хвилин в час бездіяльності системи після чого вона блокуватиметься.

Використовуваними засобами і методами порушника можуть бути відстеження модифікацій існуючих засобів обробки інформації, підключення нових пристроїв, збір інформації і даних, несанкціоновані дії з файлами системи, використання спеціалізованих утиліт, впровадження програмних закладок в систему, підключення до каналів передачі даних.

В ході адміністрування операційної системи та при налаштуванні безпеки варто не забувати про хоть і потенційний, але таки допомічний профіль зловмисника.

2.4 Визначення загроз

Ще одним з підходів до отримання стійкого і безпечного середовища ОС є визначення загроз і ознайомлення з ними аби в подальшому змогти уникнути їх.

Загрози інформаційної безпеки не проявляються самостійно, вони з’являються через можливу взаємодію з найбільш слабкими ланками системи захисту, що і є фактора уразливостей. Загроза призводить до порушення діяльності систем

Щоб побудувати модель загроз операційних систем необхідно в першу чергу зрозуміти їх складову. Головними компонентами операційної системи є:

– ядро – центральна частина, що реалізує зв’язок між прикладними пристроями і процесами;
– файлова система – система зберігання даних на пристрої даних;
– інтерпретатор команд користувача – відповідає за взаємодію та обробку дій користувача з системою;
– служби – програмне забезпечення, що виконує функції для підтримки роботи системи.

Існує велика кількість операційних систем, що різняться як за призначенням, функціональними можливостями та сферою використання.

Вразливості операційних систем є значною проблемою, адже не усі вразливості є виявленими, а у випадку появи нових вразливостей необхідно швидко та якісно вирішити проблему. Для цього співробітник, що відповідає за ці задачі повинен бути проінформованим та знаходитися в курсі усіх досліджень пов’язаних з безпекою ОС. Існують також вразливості, що були виявлено протягом існування та підтримки ОС та не були виправлені розробки. Саме такі вразливості і необхідно враховувати в моделі загроз.

Найпопулярнішими операційними системами в ІКС філії є операційні системи сімейства Microsoft Windows (Windows 10; Windows 8.1; Windows Server 2012), також наявні і Unix-подібні ОС, такі як Linux Debian 10 та мережеві ОС.

Задля підтримання безпеки важливо, переглядати оновлення в списках вразливостей операційних систем і перевіряти чи в ході адміністрування не було допущено цих проблем.

Слідкуючи за оновленими зафіксованими вразливостями на спеціалізованих сайтах CVE, можна знайти статистику тенденцій по різним рокам. На рисунку 2.1 зображенно тенденції загроз Windows Server 2012. Де зібрані дані по вразливостях і типах відповідно до колонок:

1) рік,
2) загальна кількість вразливостей;
3) кількість Dos атак – відмова в обслуговуванні;
4) кількість вразливостей з виконанням коду;
5) переповнення;
6) пошкодження пам'яті;
7) ін’єкція Sql;
8) XSS – Cross-site scripting- атака введення коду на стороні клієнта. Зловмисник прагне виконати шкідливі сценарії у веб-браузері жертви;
9) обхід каталогів - це вразливість веб- безпеки, яка дозволяє зловмисникові читати довільні файли на сервері, на якому запущена програма.
10) Http Response ;

11) обхід чогось - лазівка або вразливість, яка дозволяє зловмисникові хакеру використовувати програму на ПК, не вимагаючи імені користувача або пароля;

12) ціль- інформація;

13) ціль – привілеї;

14) File Inclusion ;

15) кількість експлойтів.

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2012	4		1	1						1		2			
2013	50	13	16	17	4			1		2	2	21			4
2014	38	9	11	4	3					6	6	12			4
2015	155	16	46	14	9			1		31	26	60			1
2016	156	8	42	19	7					16	28	76			
2017	234	24	50	19	4		1			6	108	15			
2018	164	11	34	6	1		1			13	25				
2019	314	25	116	1	6			1		9	33				
2020	443	13	85	67	8					9	65	33			
2021	170	11	65		1					13	17				
Total	1728	130	466	148	43		2	3		106	310	219			9
% Of All		7.5	27.0	8.6	2.5	0.0	0.1	0.2	0.0	6.1	17.9	12.7	0.0	0.0	

Рисунок 2.1 - Часові тенденції загроз Windows Server 2012

На рисунку нище діаграма вразливостей Windows Server 2012 відсортованих по типу вразливостей.

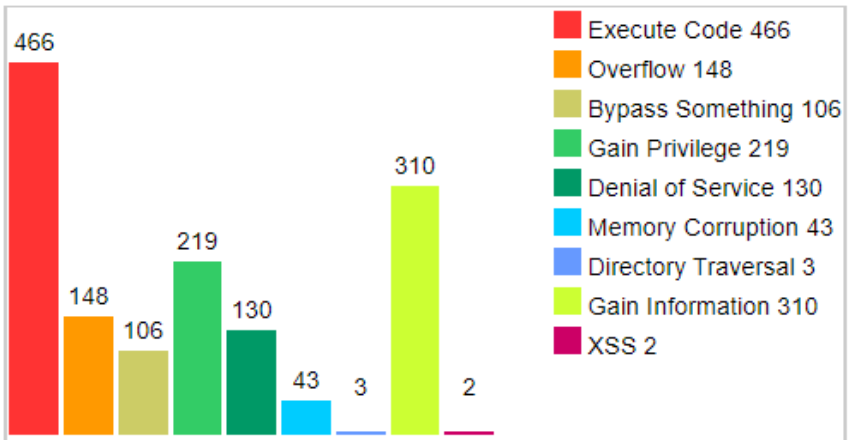

Рисунок 2.2 - Статистика по типу вразливостей Windows Server 2012

Такі статистики складаються складається щороку для різних ОС. Стратистики для ОС Windows 8.1 та ExtremeXOS відповідно на рисунках 2.3-2.4.

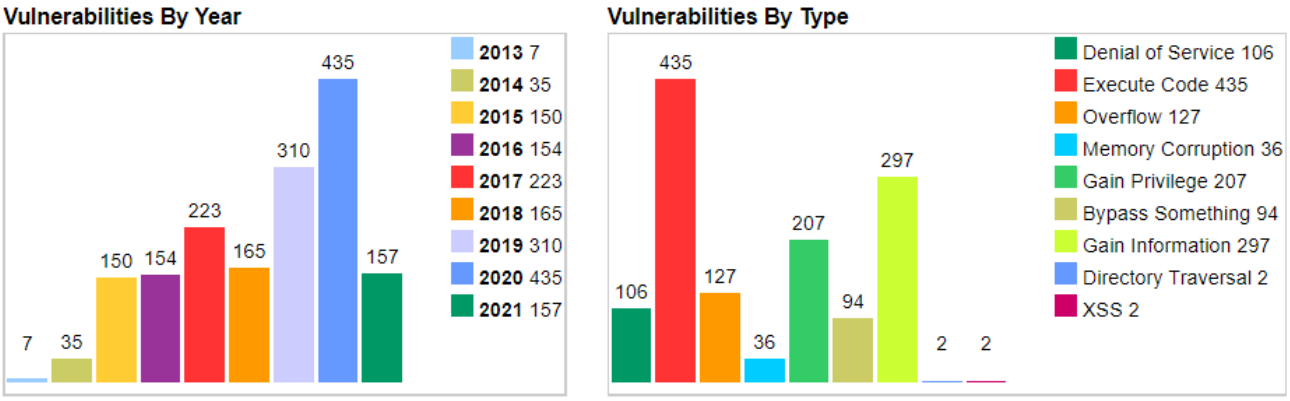

Рисунок 2.3 - Статистики кількості вразливостей по часу та типу використаних атак в період з 2013-2021рр ОС Windows 8.1

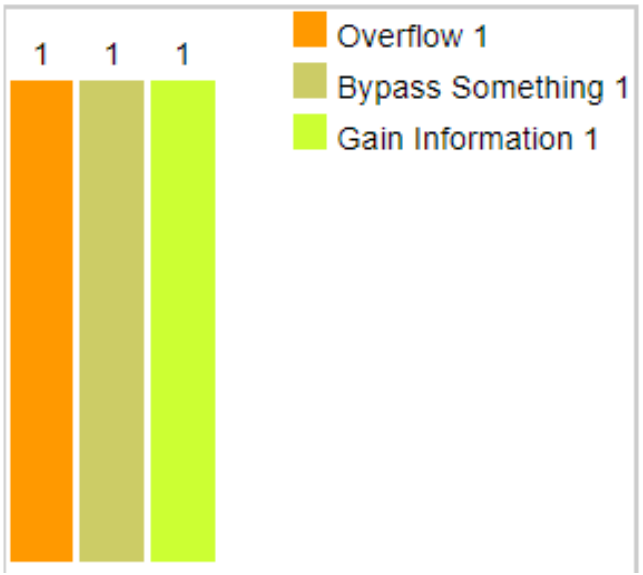

Рисунок 2.4– ExtremeXOS. Статистика по типу вразливостей за час існування

Так як операційні системи сімейства Windows є одного сімейства то буде розглядатись загальна модель загроз для усіх систем, що є актуальними(таблиця 2.1).

Скорочення в таблиці 2.1:

- К – порушення конфіденційності.
- Ц – порушення цілісності
- Д – порушення доступності.

Таблиця 2.1 – Модель загроз для ОС сімейства Windows.

№ з/п	Загрози	Можливий механізм реалізації	Наслідки
1	2	3	4
1	CVE-2021-31193	Служба Windows SSDP підвищує вразливість привілеїв.	К, Ц, Д
2	CVE-2021-31186	Уразливість розкриття інформації протоколу віддаленого робочого столу Windows (RDP)	К
3	CVE-2019-11510	Віддалений зловмисник може без аутентифікації відправити спеціально підготовлений URI на сервері Pulse Secure VPN, щоб здійснити читання довільного файлу. Баг може привести до розкриття ключів або паролів	Ц, Д
4	CVE-2020-5902	Traffic Management User Interface (TMUI) на проксі-серверах і балансувальник навантаження F5 BIG-IP вразливий перед RCE-багом, який допускає віддалене виконання довільного коду і повну компрометацію пристрою	К, Ц, Д
5	CVE-2019-19781	Системи Citrix Application Delivery Controller (ADC) і шлюзи компанії уразливі перед проблемою обходу каталогів, яка може привести до віддаленого виконання довільного коду без будь-яких облікових даних. Об'єднавши ці проблеми, можна повністю скомпрометувати системи Citrix	К, Ц

Продовження таблиці 2.1

1	2	3	4
6	CVE-2020-8193, CVE-2020-8195, CVE-2020-8196	Набір помилок в шлюзах і Citrix ADC. Ці проблеми також небезпечні для SDWAN WAN-OP. Уразливості дозволяють отримати нерозпізнаних доступ до певних ендпоінтам URL і ведуть до розкриття інформації низько привілейованих користувачів	Д, Ц
7	CVE-2020-5505	RCE-уразливість в MobileIron MDM, яка дозволяє віддаленим зловмисникам виконувати довільний код і захоплювати віддалені сервери	К, Ц
8	CVE-20201350	RCE-уразливість на серверах Windows Domain Name System, яка зводиться до того, що вони не можуть належним чином обробляти запити	Д
9	CVE-2020-1472	Вразливість, спирається на слабкий криптографічний алгоритм, який використовується в процесі аутентифікації Netlogon. Дозволяє видати себе за будь-який комп'ютер в мережі під час аутентифікації на контролері домену, відключити захисні механізми; змінювати паролі в Active Directory контролера домену	К, Ц
10	CVE-2018-6789	Відправка створеного вручну повідомлення Exim може спровокувати переповнення буфера. Це може використовувати для віддаленого виконання коду і захоплення поштових серверів	К, Ц

11	CVE-2019-3396	Макрос The Widget Connector в Atlassian Confluence 17 Server дозволяє віддаленим хакерам здійснювати обхід шляху (path traversal) і віддалене виконання коду на Confluence Server або Data Center за допомогою ін'єкцій шаблону на стороні сервера	Ц
12	CVE-2020-0601	Спуфінговий баг присутній в Windows CryptoAPI (Crypt32.dll) під час валідації сертифікатів Elliptic Curve Cryptography (ECC). Зловмисник може використовувати підроблений сертифікат для підписання коду шкідливих виконуваних файлів, створюючи враження, ніби малваре відбувається з надійного, легітимного джерела	К, Ц
13	CVE-2019-0803	Вразливість підвищення привілеїв в Windows, пов'язана з тим, що компонент Win32k некоректно обробляє об'єкти в пам’яті	К, Ц

З таблиці вище видно, що кількість загроз, що існують у сімействі Windows є дуже великою, так як складається з дуже виликої кількості компонентів. Більшість загроз спрямовані для отримання повного контролю над системою.

3 РЕКОМЕНДАЦІЙНИЙ РОЗДІЛ

3.1 Політика безпеки

Серед великої кількості різних типів політик безпеки загально - політика безпеки спрямована на захист та обмеження розповсюдження даних лише тими, хто має санкціонований доступ.

Розробка ефективної політики захисту інформації та забезпечення відповідності є важливим кроком у запобіганні таким інцидентам, як витоки даних та порушення даних . Політика інформаційної безпеки (ISP-information security policy) - це набір правил, політик та процедур, призначених для забезпечення того, щоб усі користувачі та мережі в організації відповідали мінімальним вимогам щодо IT-безпеки та захисту даних.

3.1.1 Політика та процедури безпеки операційної системи

Існує багато різних типів політик та процедур безпеки операційної системи (ОС), які можуть бути реалізовані. Політика безпеки ОС - це та, яка містить інформацію, яка окреслює процеси забезпечення ОС підтримує певний рівень цілісності, конфіденційності та доступності.

Політика безпеки охоплює всі профілактичні заходи та методи для забезпечення захисту ОС, мережі, до якої вона підключається, та даних, які можна вкрасти, відредагувати або видалити.

Оскільки політика та процедури безпеки ОС охоплюють широку область (тобто від загроз до атак), існує безліч способів їх вирішення. Деякі з цих областей включають:

1. Забезпечення регулярного виправлення або оновлення систем
2. Встановлення та оновлення антивірусного програмного забезпечення
3. Встановлення брандмауера та забезпечення його правильної конфігурації для моніторингу всього вхідного та вихідного трафіку

4. Впровадження процедур управління користувачами забезпечує захист облікових записів та привілеїв користувачів.

3.1.2 Політика контролю доступу (ACP)

Access control policy(ACP) визначає, що працівники буде мати доступ та містити інформацію щодо:

1. Особливостей доступу.
2. Правил складності паролів.
3. Політики зміни пароля.
4. Контроль доступу користувачів та мережі.

Детальніший опис в пункті 3.1.3 – Перелік правил.

3.1.3 Перелік правил

Цей розділ відобразить перелік загальних політик безпеки для працівників філії в ситуація, які можуть виникнути і як реагувати на них(див. таблицю 2).

Таблиця 3.1 – Політики безпеки для персоналу

Інцидент/ ситуація	**Дія**
1	2
Втрата доступу користувачів до системи	1. Дізнайтесь в адміністратора свої ідентифікатори для авторизації в системі 2. Не зберігайте їх на видних і незахищених ресурсах. 3. В разі потреби під наглядом системного адміністатора відновіть свої індентифікатори.

Продовження таблиці 3.1.

1	2
Злом або розкриття пароля	1. Використовуйте хороші, дивакуваті паролі, які важко вгадати. 2. Перевірте чи такого паролю немає серед викрадених і злитих в інтернет. Наприклад використову.чи сервіс haveibeenpwned. 3. Ніколи не діліться та не розкривайте свої паролі навіть людям чи організаціям, яким ви довіряєте 4. Використовуйте різні паролі для робочих та неробочих облікових записів. 5. Майте унікальний пароль для кожного облікового запису. 6. Змінюйте початковий і тимчасовий паролі та скидайте їх як можна швидше, коли це можливо. Вони, як правило, менш захищені.
Небезпечне зберігання або передача персональної інформації та іншої конфіденційної інформації	– Не розміщуйте конфіденційні дані в незахищених папках та середовищах. – Перконайтесь та не розміщуєте конфіденційну інформацію в місцях, які є загальнодоступними з Інтернету – Не надсилайте незашифровані конфіденційні дані електронною поштою та миттєвими повідомленнями

Продовження таблиці 3.1

1	2
Відсутні «патчі» та оновлення. Дозволяють зловмисникам використовувати вразливими місцями в (ОС) та додатках, якщо вони не були належним чином виправлені або оновлені. Це ставить під загрозу всі дані цієї системи та інших підключених систем	1. Переконайтеся , що всі системи , підключені до мережі Інтернет та мають всю необхідну кількість додатків безпеки , «патчів» і оновлення. операційної системи.
Робоча станція заражена вірусом або іншим шкідливим програмним забезпеченням Комп'ютери, які не захищені антивірусним програмним забезпеченням, є вразливими. Застаріла антивірусна програма може не виявити відоме шкідливе програмне забезпечення, роблячи ПК вразливим .	1. Встановіть антивірусне ПЗ та переконайтесь, що воно завжди оновлене. 2. Не натискайте на невідомі або несподівані посилання чи вкладення. 3. Не відкривайте надіслані файли на машині, що містить конфіденційні дані - ці файли можуть обходити антивірусний контроль. 4. Використовуйте Sandbox, якщо є нагальна потреба відкрити завантажений файл з невідомого джерела.
Неправильно налаштоване або ризиковане програмне забезпечення:	1. Не встановлюйте неперевірений софт. 2. Запросіть дозвіл в адміністатора безпеки на скачування потрібного ПЗ.

Продовження таблиці 3.1.

1	2
Не заблокована робоча станція При бездіянні і відходженні від системи до незаблокованого чи не виключеного комп'ютера зловмисник без перешкод може отримати доступ.	1. Переконайтесь , що комп'ютер вимкнено чи заблоковано, перед тим як покинути робоче місце.

В цьому пункті висвітлено загально-організаційні правила, щодо забезпечення безпеки користувачів в програмних оболонках для робочих станцій.

3.2 Загартовування/ посилення безпеки в ОС

Загартовування безпеки у робочому середовищі є важливим процесом, який передбачає зменшення ризику за допомогою виявлення та усунення вразливостей по всій поверхні атаки системи. Система, як правило, має більше вразливостей або більшу поверхню атаки в міру збільшення її складності або функціональності.

3.2.1 Посилення безпеки ОС сімейства Windows

Проактивні методи безпеки можуть значно зменшити ризик який появляється відповідь на постійно зростаючу поверхню атаки, нище в пункті 3.2.1 наведено список базових рекомендацій з посилення ОС Windows 8.1/10 Pro, можна використовувати , як підказку для перевірки налаштувань. Рекомендації, щодо посилення безпеки ОС Windows відображені в таблиці 3.2.

Таблиця 3.2 - Рекомендації, щодо посилення безпеки ОС Windows

USER ACCOUNTS:
- Застосовуйте принцип найменших привілеїв, - Деактивовуйте такі облікові записи як Default accounts та Unused accounts(акаунти за замовчуванням).
АВТОЗАПУЩЕННІ ПРОГРАМИ І СЕРВІСИ:
- Повимикайте або видаліть будь-які непотрібні виконувані файли або служби, що працюють під час запуску / входу (Sysinternals Autoruns(див.рис.3.1) – хороший інструмент для цього).
WINDOWS DEFENDER FIREWALL:
- Вмикайте всі профілі, - виключивши вхідний трафік за замовчуванням, увімкнути вхідний і вихідний трафік по правилам які необхідні для сервісів
WINDOWS DEFENDER ANTIVIRUS:
- Переконайтесь, що встановлені оновлення та антивірус включений.
Оновлення WINDOWS:
- запевніться, що всі відповідні виправлення, виправлення та пакети оновлень застосовуються на разі.
ОБ’ЄКТИ ГРУПОВИХ ПОЛІТИК:
- *Політики паролів* (мінімальна довжина паролю – 12 символів; максимальний термін дії паролю – 60днів; паролі включають комплексний підхід, тобто складаються з різного типу символів, великий та малий регістри і цифри.) - *Політика блокування* (блокуваннння акаутну через 15 хвилин бездіяння; кількість хибних аутертифікацій -10; сидання лічильника через 15 хвилин .)

Продовження таблиці 3.2

- *Контроль за обліковими записами* (

  Administrator account: Enabled – режим схвалення адміністратора для вбудованого облікового запису адміністратора: увімкнено

  Admin Approval Mode: Enabled – запуск усіх адміністраторів у режимі затвердження адміністратора: увімкнено)
- *Інтерактивний вхід(*

  межа бездіяльності машини: 900 секунд

  нагадування користувачеві змінити пароль до закінчення терміну дії: 14 днів
- *Мережний доступ*

  увімкнути заборону на анонімне перерахування облікових записів SAM(Security Account Manager);

  увімкнути заборону на анонімне перерахування облікових записів SAM та спільного використання.
- *Мережева безпека*

  встановлення 5 рівня автентифікації LAN Manager.(відправляти лише відповідь NTLMv2)
- *Оновлення Windows*
- скасувати доступ, щоб використовувати всі функції Windows Update
- *Додаткові примітки*

  Applocker: обмежити виконувані файли для певних користувачів

  Bitlocker: шифрувати диски через Провідник файлів або об’єкт групової політики

  Пароль: встановити захист на вікно заставки.

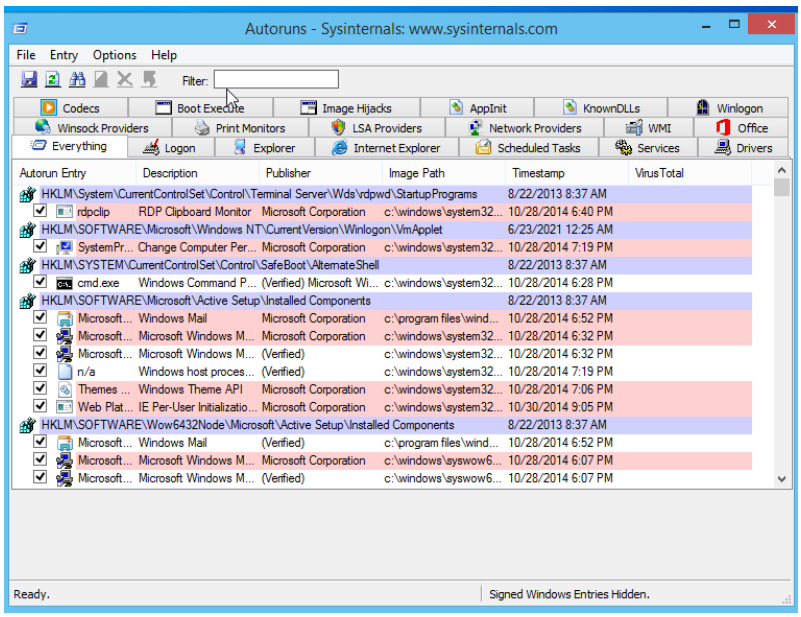

Рисунок 3.1- вигляд програми Sysinternals Autoruns Windows 8.1

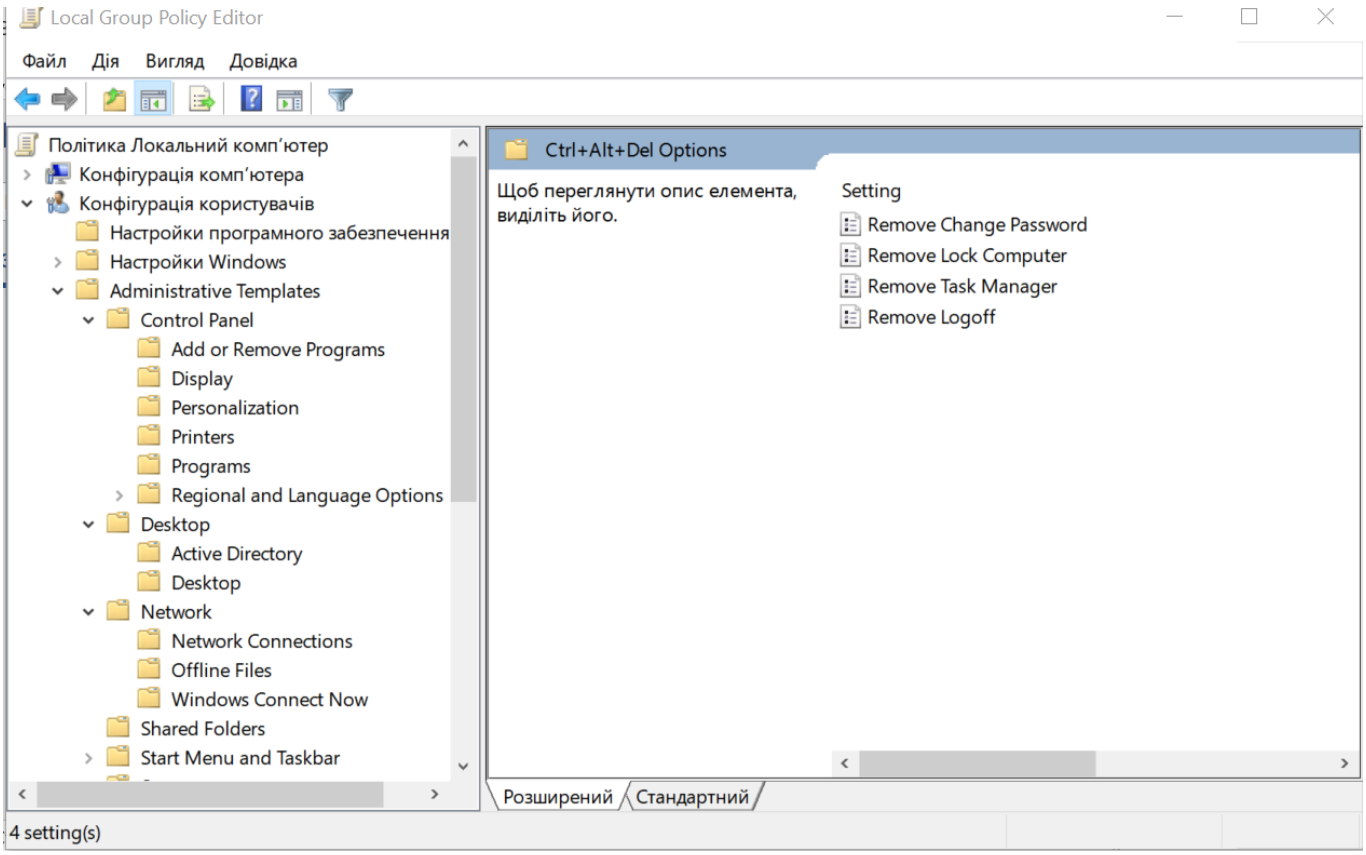

Рисунок 3.2 - Вигляд вікна налаштувань групової політики Sysinternals Autoruns win.8.1

3.2.2 Посилення безпеки ExtremeXOS

ExtemeXOS(EXOS) є мережевою операційною системою, яка працює як вбудована ОС на базі комутаторів Extreme Summit. Завданням операційних систем для комутаторів є налаштування юезпечних правил комунікування на 2 І 3 рівнях мережевої моделі OSI.

У наведеному нижче контрольному списку узагальнено найважливіші завдання безпеки, які слід виконати на операційній системі комутатора. Кожен елемент повинен використовуватися на всіх рівнях мережі ExtremeXOS.

Першим і важливим кроком перед початком роботи з налаштування повинно бути скидання попередніх налаштувань комутатора. Під час початкового завантаження комутатор повинен бути незконфігурований, і з відключеними всіма портами.

- Наступним, усі «default» порти слід видалити із VLAN командою:

configure vlan <vlan_name> delete ports <port_list>, де vlan_name означає найменування віртуальної локальної мережі, port_list – вказані порти.

- Далі слід налаштувати банер, який попереджає, що несанкціонований доступ до комутатора заборонений. Щоб додати банер до свого комутатора:

– Виконайте команду «налаштувати банер»:

configure banner{after-login| { before-login} { acknowledge} | before-login {acknowledge} save-to-configuration}.

За допомогою цієї команди можна налаштувати банер сповіщення яке буде відображатись перед входом на комутатор так і після входу в систему.

– введіть потрібний банер;

– виконайте show banner – для відображення збережених конфігурацій.

Виконання коду зображено на рисунку 3.3.

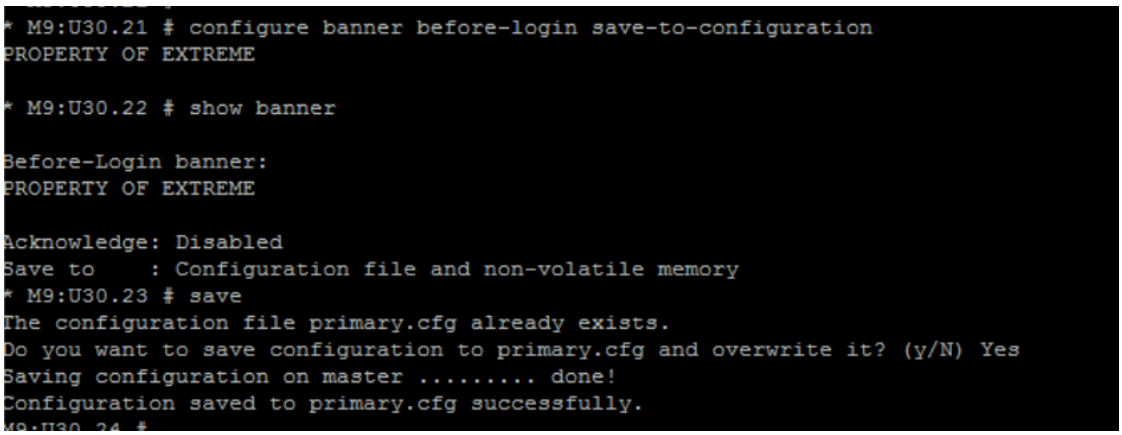

Рисунок 3.3 – Виконання коду налаштування банеру сповіщення

- Налаштування складності та довжину пароля на EXOS виконується командою:

configure account all password-policy char-validation all-char-groups

а) налаштування мінімальної довжини паролю:

conf account all password-policy min-length <num_characters>, де num_characters – кількість символів;

В результаті нескладних операцій буде налаштована безпека складності та встановлено фіксовано мінімальну довжину паролю із використанням різних типів символів.

Також існують інші параметри з допомогою яких можна ввести блокування через невірне введення паролю по результатах декількох раз. Можна вказувати час існування без зміни паролю, перевірку введеного паролю в історії паролів. Таким чином можна створити складну систему перевірки та забезпечення аутентифікації в системі.

– Створення нового облікового запису на рівні адміністратора та видалення облікових записи користувачів за замовчуванням.

а) для створення акаунта необхідно виконати таку команду:

create account admin <account-name> , де account-name назва облікового запису;

б) для видалення акаунта необхідно виконати таку команду:

delete account admin , де admin назва облікового запису який є позамовчуванню;

Виконання цього кроку потрібне аби не дозволити потенційному зловмиснику використовувати облікові записи, які йдуть в стандартних конфігураціях.

– Переналаштовування облікового запису Failsafe . Потрібно виконати команду:

configure failsafe-account {[deny | permit] [all | control | serial | ssh {vr vrname} | telnet {vr vr-name}]}

– Призначення внутрішньосмугового IP-адресу VLAN та SSH для віддаленого доступу виконується командою:

configure vlan <vlan_name> ipaddress <ip_address>/<subnet_mask>

– Налаштування політики доступу, яка обмежує доступ SSH лише до авторизованих хостів або мереж. Що в свою чергу дозволяє відсіювати підроблені хости або мережі. Для того, щоб виконати поставлену задачу необхідно ввести в командній строці такі команди:

а). vi SSH-access.pol - для створення політики з назвою SSH;

б) а далі створити ACL список:

```
entry AllowTheseSubnets {
if match any {
source-address 10.203.133.0 /24;
source-address 10.203.135.0 /24;
} then {
permit;
}
}
```

– Налаштування VLAN на сегментацію різних груп трафіку.

Усі невикористані порти слід відключити. Використовуйте протоколи маршрутизації, що підтримують автентифікацію. Extreme Networks рекомендує OSPF. Якщо протоколи безпечної маршрутизації використовувати не вдається, статичну маршрутизацію можна використовувати в крайньому випадку. Команда для цього:

create [{vlan} vlan_name] {tag tag } {description vlan description} {vr name } , де vlan_name вказує ім'я VLAN (до 32 символів).; tag: значення тегу 802.1q; vlan-description вказує опис VLAN (до 64 символів); назва VR: вказує екземпляр VR або віртуальної маршрутизації та переадресації (VRF), в якому потрібно створити VLAN.

– Слід увімкнути захист від відмови в сервісу(DOS).

Перед тим як забезпечити захисту від відмови необхідно врахувати те, що процесор обробляє трансляцію та невідомі mac-адреси призначення від користувацького трафіку в мережі. ЦП також повинен обробляти пакети управління протоколами, такими як OSPF / VRRP / MPLS тощо. Отже, також слід враховувати конфігурацію цих протоколів. Для налаштування необхідно виконати команду:

configure dos-protect type l3-protect alert-threshold <number of packets>

– Обмеження передачі широкосмугового трафіку. Для цього прописується:

configure ports <port_list> rate-limit flood multicast <PPS>

Налаштований ліміт повинен бути встановлений настільки високим, щоб це не впливало на звичайний трафік, який залежатиме від локальної мережі.

– Налаштування сервера syslog виконується командами:

enable syslog
configure syslog add <ip_address> vr <virtual-router> local0
configure syslog <ip_address> vr <virtual-router> local0 severity info

enable log target syslog <ip_address>:<port> vr <virtual-router> local0

Конфігурація сервера syslog вкрай потрібна для відслідковування подій які відбуваються в системі. Повідомлення , які реєструє syslog в подальшому, дозволять вчасно виявити, якісь системні збої.

4. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ

4.1. Діяльність. Її види ти розуміння в безпеці праці.

До процесу свієї своєї діяльності люди підходять комплексно. Використовують не тільки свої фізичні можливості, а й затрачають значні психологічні зусилля(відносяться особливості характеру, сила волі, розумові здібності тощо).

Діяльність людини можна поділити на дві категорії – фізичну та розумову.

Фізична діяльність – діяльність, пов'язана з конкретними предметними діями (наприклад, перевезення вантажу, інструментальне виробництво).

Розумова діяльність пов'язана з психічними процесами, під час яких людина планує свої дії, оперуючи образами та мовними символами.

Людина в діяльності виступає як особистість, що має певні мотиви і намічені цілі. Мотивами можуть виступати потреби, почуття тощо. Для здійснення діяльності необхідно мати об'єкт діяльності, внутрішні спонуки, а також співвідношення спонук і цілей людини, які вона хоче досягнути в результаті своєї діяльності. Наприклад, людину до діяльності спонукає або особисте збагачення (задоволення особистих потреб), або неможливість фізичного існування без діяльності.

На відміну від фізичної, розумова діяльність супроводжується меншими витратами енергетичних запасів, але це не означає, що вона є легкою. Основним робочим органом під час такого виду діяльності виступає мозок. Під час розумової діяльності «значно активізуються аналітичні та синтетичні функції центральної нервової системи, «ускладнюється прийом і переробка інформації, виникають функціональні зв'язки, нові комплекси умовних рефлексів, зростає роль функцій уваги, пам'яті, напруження зорового та слухового аналізаторів і навантаження на них. Для розумової діяльності характерні: напруження уваги, неприйняття, пам'яті, велика кількість стресів, малорухомість, вимушена поза.

Все це зумовлює застійні явища у м'язах ніг, органах черевної порожнини і малого тазу, погіршується постачання мозку киснем, зростає потреба в глюкозі. Погіршуються також функції зорового аналізатора: стійкість; ясного бачення, гострота зору, зорова працездатність, збільшується час зорово-моторної реакції.

Розумовій праці притаманний найбільший ступінь напруження уваги - в середньому у 5 - 10 разів вищий, ніж при фізичній праці. Завершення робочого дня зовсім не переривається процесу розумової діяльності. Розвивається особливий стан організму – втома, що з часом може перетворитися на перевтому. Все це призводить до порушення нормального фізіологічного функціонування організму.

Люди, що займаються розумовою діяльністю, навіть у стані перевтоми здатні довгий час виконувати свої обов'язки без особливого зниження рівня працездатності і продуктивності.

Переважно люди розумової діяльності нездатні вимкнути механізм переробки інформації на ніч; вони працюють не лише 8 - 12 годин на добу, а майже постійно з короткими переключеннями. Це і є підтвердженням так званої інформативної теорії, згідно з якою людина, під час сну перероблює інформацію, отриману в період активної бадьорості.

Фізичний і розумовий види діяльності вимагають різного напруження різних функціональних систем організму, тому навантаження необхідно класифікувати відповідно до важкості і напруженості. Важкість праці - це напруження функціональних систем, які зумовлені фізичним навантаженням. Напруженість, своєю чергою, характеризує рівень напруження центральної нервової системи.

На філії підприємства наявні два типи діяльності. В обов'язки працівників технічного підрозділу секторів технічного обслуговування, технічної підтримки ВОЛЗ та , технічної підтримки мережі входить як і фізична діяльність так і розумова. А от сектори технічної підтриски користувачів і виробничо-технічний здебільшого їхня діяльність спрямована на розумову діяльність.

На успіх діяльності особливо впливає стан людини, тому що будь-який вид діяльності викликає втому.

Втома - це зниження продуктивності діяльності через витрату енергетичних ресурсів організму людини.

Цей стан виникає через певне ставлення людини до праці, звички до фізичного та розумового напруження. Якщо таких звичок немає, то втома може настати ще до початку фізичного навантаження, на самому початку роботи. Втома після важкої, але

потрібної людям праці, пов'язана з позитивним емоційним станом. Відпочинок, особливо активний, зміна виду діяльності поновлюють силу, створюють можливість продовження діяльності. Об'єктивним показником втомлення є уповільнення темпу роботи, а також зниження її якості.

Люди зі станом перевтоми характеризуються порушенням сну, відсутністю повного відновлення працездатності до наступного робочого дня, зниженням опору до дії несприятливих факторів довкілля, підвищенням нервово-емоційної збудливості. Такий стан може призвести до загострення багатьох захворювань - серцево-судинних, ендокринних, бронхо-легеневих, хронічних тощо.

4.2. Вимоги безпеки до робочих місць виконання робіт.

Робоче місце – це така структура, в якій поєднуються в єдине ціле формальні елементи організації та особисті, людські риси працівника, утворюючи систему "людина – робота".

Вихідним елементом будь-якого підприємства є робоче місце, в межах якого відбувається цілеспрямована діяльність (тобто праця) конкретного працівника.

Конструювання робочого місця є процесом визначення завдань, котрі мають виконуватися працівником, носієм конкретних знань, навичок і здібностей.

Кожне робоче місце має бути відповідним чином обладнане, тобто забезпечене необхідним обладнанням, інструментами тощо. Система заходів щодо обладнання робочого місця всім необхідним називається його організацією. З погляду менеджменту організація робочого місця – це процес створення певного комплексу організаційно-технічних умов для високопродуктивної та безпечної роботи.

Добра організація робочого місця означає, що кожний предмет перебуває на своєму місці. Основу організації робочого місця становить його планування, тобто оптимальне розміщення в межах робочого місця засобів і предметів праці, необхідних для виконання роботи.

Непродумане планування збільшує витрати, тому що час виконання конкретної роботи стає тривалішим.

Робоче місце і його оснащення - важливий елемент умов праці. Умови праці – це сукупність елементів виробничого середовища, котрі впливають на здоров'я та працездатність людини, задоволеність працею, а відтак і на її результати.

До будь-якого робочого місця на практиці висуваються відповідні вимоги, які можуть бути частково виражені кількісними показниками – нормами і нормативами, а деякі піддаються лише якісному опису.

Ряд вимог, перш за все в галузі санітарії, техніки безпеки, правил експлуатації обладнання тощо, є обов'язковими, і за порушення їх керівник може понести відповідальність включно з кримінальною. Інші відносять, поки що, до бажаних (естетичність, ергономічність тощо), але нехтування ними безпосередньо впливає на продуктивність праці, а тому для підприємства вони мають важливе значення.

Вимоги до організації робочих місць можна згрупувати так: інформаційні, економічні, ергономічні, гігієнічні, естетичні, технічні, організаційні.

Інформаційні вимоги охоплюють комплекс заходів з інформаційного забезпечення робочого місця: визначення обсягів і структури інформації, котра надходить та оброблюється на ньому, створюється і передається на інші робочі місця; проектування інформаційних потоків, до системи яких входить дане робоче місце, та інших; інформація має бути достатньою для виконання службових зобов'язань працівників.

Економічні вимоги передбачають організацію робочого місця в апараті управління з мінімальними витратами на його утримання, але достатніми для його нормального функціонування. Доцільне також оцінювання робочого місця за критерієм оптимальності, тобто ефект від діяльності працівника на робочому місці має перевищувати витрати на утримання цього робочого місця.

Ергономічні вимоги пов'язані зі створенням для людини оптимальних умов праці, що роблять її високопродуктивною та надійною і водночас забезпечують людині необхідні зручності, зберігаючи сили, здоров'я та працездатність. Таким чином, усе, що оточує людину, котра працює, створюючи їй відповідне робоче середовище, – меблі, помешкання, устаткування, машини, механізми та інші знаряддя праці – має відповідати вимогам ергономіки (наука про функціональні можливості

людини в трудових процесах) і бути максимально пристосованим до людини, до її фізичної, фізіологічної, естетичної природи.

Гігієнічні вимоги передбачають забезпечення таких норм: освітлення робочих місць; повітрообміну, температурного режиму; вологості; шуму й інших чинників робочого середовища, що впливають на здоров'я і працездатність людини.

Естетичні вимоги до зовнішнього оформлення робочого середовища: вигляд приміщення і засобів праці, їхня кольорова гама, наявність квітів у інтер'єрі тощо.

Технічні вимоги передбачають дотримання норм необхідного простору для виконання визначеної роботи. Це площа, на якій установлюють необхідні меблі й обладнання, місце самого працівника, а також площа проходів до столу, устаткування, іншого робочого місця тощо.

Згідно з діючими санітарними нормами встановлено приблизно такі розміри робочих місць для різних категорій управлінського апарату, м^2:

1) керівник підприємства: 25–55;
2) заступник керівника: 12–35;
3) керівник великого структурного підрозділу: 12–35;
4) керівник відділу, його заступник, головний фахівець: 8–24;
5) фахівець: 4–8;
6) старший діловод: 5–7;
7) завідуюча машбюро, друкарка, молодший діловод: 3–4.

Однак ці норми можуть бути лише орієнтиром при організації та плануванні робочих місць, оскільки вони не враховують усього різноманіття умов праці працівників різних професій. Тому для визначення загальної площі робочого місця (П). У кожному конкретному випадку доцільно використовувати сумарний метод розрахунку, при якому враховують площу трьох складових частин робочого місця:

$$П = П + 17 + Пп , \quad (4.1)$$

де П – площа, яку займає устаткування;

Пп – площа для проходів.

Відповідно до організаційних вимог необхідно визначити сферу компетенції кожного працівника на конкретному робочому місці, його права, обов'язки, підпорядкованість, вертикальні й горизонтальні зв'язки з іншими робочими місцями, форми і методи стимулювання ефективної праці. Ці питання вирішуються розробкою положень про структурні підрозділи апарату управління і посадових інструкцій працівників.

Робоче місце фахівця з інформаційної безпеки, як правило, обладнане великою кількістю технічних пристроїв. Це перш за все персональний комп’ютер, принтер, сканер, додатковий монітор, і різноманітні засоби телефонного зв’язку: телефон, факс.

Організація робочого місця користувача ЕОМ повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування вимогам ГОСТ 12.2.032 “Рабочее место при выполнении работ сидя. Общие эргономические требования”; характеру та особливостями трудової діяльності.

При розміщенні робочих місць з ЕОМ необхідно дотримуватись таких вимог:

1. Відстань між бічними поверхнями ЕОМ має бути не меншою за 1,2м.

2. Відстань між тильною поверхнею однієї ЕОМ та екраном іншої не повинна бути меншою 2,5 м.

3. Прохід між рядами робочих масцьмає бути не менш 1 м.

Конструкція робочого місця користувача ЕОМ (при роботі сидячи) має забезпечувати підтримання оптимальної робочої пози з такими ергономічними характеристиками: ступні ніг – на підлозі або на підставці для ніг стегна – в горизонтальній площині; передпліччя – вертикально; лікті – під кутом 70°-90° до вертикальної площини; зап’ястя зігнуті під кутом не більше 20° відносно горизонтальної площини, нахил голови - 20°відносно вертикальної площини.

Висота робочої поверхні столу для ЕОМ має бути в межах 680-800 мм, а ширина – забезпечувати можливість виконання операцій в зоні доасяжності моторного поля.

Рекомендовані розміри столу: висота – 725 мм, ширина – 600-1400мм, глибина

– 800-1000 мм.

Робочий стіл для ЕОМ повинен мати простір для ніг висотою не менше 600 мм, шириною не менше 500 мм, глибиною на рівні колін не менше 450 мм, на рівні витягнутої ноги – не менше 650 мм.

Робочий стіл для ЕОМ, як правило, має бути обладнаним підставкою для ніг шириною не менше 300 мм та глибиною не менше 400 мм, з можливістю регулювання по висоті в межах 150 мм та кута назилу опорної поверхі – в межах 20 град. Підставка повинна мати рифлену поверхню та бортик на передньому краї заввишки 10 мм.

ВИСНОВКИ

Загалом операційні системи можна описати як те що дозволяє покращити життя апаратних систем. Також можна рахувати ОС основним компонентом, який завантажується в систему і дозволяє системі стати робочою та керованою. Операційні системи управляють всіма програмами та процесами на комп'ютері.У загальній безпеці системи надзвичайно важливу роль грає безпека ОС, так як вона є центром управління комп'ютера, а тим паче якщо вона є частиною інформаційно-комунікаційної системи .

В ході розробки першого розділу кваліфікаційної роботи було сформоване уявлення про те чим займається компанія для того, щоб ця інформація могла в подальшому дозволила розробити модель порушника, політики безпеки та провести аналіз загроз. Представленно характеристики і опис об'єктів інформаційної діяльності в ІКС.

В наступному розділі підведено, що підхід до забезпечення безпеки, має бути комплексним і розбитим на рівні, так як самі операційні системи є громіздким продуктом, тому не можна цей процес узагальнювати. Також на основі матеріалу з першого розділу було проаналізовано загрози операційних систем та розроблена модель порушника.

І в останньому розділі було розроблено політики безпеки та надано рекомендації щодо загартовування операційних систем, які варто не уникати, інакше інформація може бути втраченою.

Безпека інформації забезпечується найкращим чином лише при сумарному використанні всього арсеналу наявних засобів захисту в усіх структурних елементах виробничої системи і на всіх етапах технологічного циклу обробки інформації. З'ясовано, що найбільший ефект досягається тоді, коли всі використовувані засоби, методи і заходи поєднуються в єдиний цілісний механізм – систему захисту інформації. До того ж важливо впроваджуючи вимоги до безпеки в культуру компанії, а не відноситись до цього як до одноразової акції. Навіть при цьому

функціонування системи повинно контролюватися, оновлятися і доповнюватися залежно від зміни зовнішніх і внутрішніх умов.

В ході дослідження та з урахуванням поставлених завдань прийшли до наступних висновків:

1) інформаційно-комунікаційна система працює задля ефективної передачі та організації ресурсів в інформаційному середовищі і саме, тому її компоненти потребують особливого нагляду. І так як ІКС складається з різних програмних та апаратних елементів, які повинні працювати спільно, тому ніякі прогалини в системі безпеки не є допустимими, інакше буде порушено продуктивну комунікацію між компонентами.

2) безпека інформації є нескінченним процесом і задля підтримки системи в доброму стані, бо ніхто не застрахований від вразливостей, то час від часу корисною звичкою буде відслідковування інформації актуальних загроз, проведення аналізу їх та формування нових моделей порушника як порушника так і загроз. Від цих дій напряму залежать безпека ваших систем. Роздумуючи над існуючими чи потенційними загрозами та використовуючи аналіз даних в голові формується хороше уявлення про дії, які відбуваються чи можуть відбуватись в інформаційному середовищі. Це є хороша практика.

3) в якості організаційного заходу, можна долучати до процесів розробки моделей зловмисника та загроз робочий персонал аби розширювати їх обізнаність в інформаційній безпеці.

4) політики безпеки є хорошим профілактичним засобом для підтримання захищеності даних, які можна викрасти, відредагувати, видалити. Розробка політик безпеки – це сукупність правил, політик та процедур, призначених для забезпечення того, щоб усі користувачі та мережі були проінформовані мінімальними вимогам щодо IT-безпеки та захисту даних.

Врешті по виконанню всіх завдань було систематизовано та закріплено здобуті теоретичні знання.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основи компьютерной безопасности. М.: Радио и связь, 2006.

2. Закон України. Про захист інформації в автоматизованих системах [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2594-15#Text.

3. ЗАКОН УКРАЇНИ від 20.03.2020, підстава - 524-IXПро захист персональних даних [Електроний ресурс]: https://zakon.rada.gov.ua/laws/main/2297-17#Text.

4. Законодавство України [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws.

5. Extremeportal [Електронний ресурс] – Режим доступу до ресурсу: https://extremeportal.force.com/ExtrSearch?q=#t=All&sort=relevancy.

6. Безпека у Windows [Електронний ресурс] – Режим доступу до ресурсу: https://support.microsoft.com/

7. Инструментальный контроль и защита информации: учебное пособие. Воронеж: Воронежский государственный университет инженерных технологий, 2013. – 192 с.

8. Инструментальный контроль и защита информации: учебное пособие. Воронеж: Воронежский государственный университет инженерных технологий, 2013. – 192 с.

9. Охорона праці в галузі комп'ютингу: підручник / Л. А. Катренко, А. В. Катренко ; [за наук. ред. В. В. Пасічника] ; М-во освіти і науки, молоді та спорту України. — Л. : Магнолія 2006, 2012. — 544

10. Жидецький В.Ц. Охорона праці користувачів комп’ютерів. Навчальний посібник. – Вид. 2-ге., доп. – Львів.: Афіша, 2000.

11. Киреенко А. Е. Современные проблемы в области информационной безопасности: классические угрозы, методы и средства их предотвращения [Текст] / А. Е. Киреенко // Молодой ученый. — 2012. — №3. — С. 40-46.

12. Как организована безопасность вашей операционной системи [Електронний ресурс] – Режим доступу до ресурсу: https://lib.itsec.ru/articles2/Inf_security/bezopasnost-OS.

13. Кіберугрози [Електронний ресурс] – Режим доступу до ресурсу: http://www.iso27000.ru/chitalnyi-zai/kiberugrozy-i-kiberterrorizm.

14. Портал Cisco [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/.

15. Портал з нормативними документами щодо захисту інформації.Термінологія в галузі захисту інформації. [Електронний ресурс] – Режим доступу до ресурсу: https://tzi.ua/ua/nd_tz_1.1-003-99.html.

16. Форум программистов и сисадминов Киберфорум [Електронний ресурс] – Режим доступу до ресурсу: https://www.cyberforum.ru/.

17. Foreman. The complete lifecycle management tool for physical and virtual servers. [Електронний ресурс] – Режим доступу до ресурсу: https://www.theforeman.org.

18. McAfee | Антивирус, мобильная безопасность и VPN ... [Електронний ресурс] – Режим доступу до ресурсу: https://www.mcafee.com.

19. Яковина В.С. Основи безпеки комп’ютерних мереж: Навчальний посібник. Львів: НВФ "Українські технології", 2008.

20. Halevi S., Krawczyk H. Security under key-dependent inputs, in: Proc. of the 14th ACM Conference on Computer and Communications Security – CCS ’07 (P. Ning et al., eds.), Alexandria, Virginia, USA, 2007, ACM, New York, NY, USA, 2007, pp. 466–475, URL: http://doi.acm.org/10.1145/1315245.1315303