МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Освітньо-професійна програма «Комп'ютерна інженерія

Спеціальність 123 «Комп'ютерна інженерія»

Група: 2БКС-27

БАКАЛАВРСЬКА

КВАЛІФІКАЦІЙНА РОБОТА

студента денного відділення

БКС 27.01.000.00 БКР

Аверіна Володимира Михайловича

м. Одеса
2023 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «Одеський технічний фаховий коледж ОНАХТ»

Освітньо-професійна програма: «Комп'ютерна інженерія»
Спеціальність 123 «Комп'ютерна інженерія»
Група БКС-27

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи бакалавра на тему:

«Аналіз новітніх технологій кібербезпеки в період пандемії Covid-19 та воєнного часу»

Проектний матеріал складається з пояснювальної записки на _72_ сторінках та мультимедійної презентації на _12_ сторінках.

Здобувач освіти _____ (Аверін В.М.)
Керівник роботи _____ (Харченко Р.Ю.)

Консультанти:
з охорони праці _____ (Чорновол Н.І.)
за дотриманням вимог ЄСКД _____ (Петрашова В.І.)
старший консультант _____ (Кривченко Ю.В.)

До захисту допущений
Завідувач кафедри _____ (Іванова Л.В.)
Завідуючий відділенням _____ (Скорнякова О.В)

Захист «26» 06 2023 р. Протокол ДКК № 3
Оцінка ДКК 5 (відмінно)
Секретар ДКК _____

АНОТАЦІЯ

Спостерігається значне збільшення загроз у кіберпросторі проти українських стратегічних цілей, що доволі очікувано може розповсюдитися на прибічників та союзників України. Уряд Росії зробив рішучі заяви щодо дій, які він збирається вживати проти суб'єктів підприємницької діяльності, які намагаються вийти з країни, включаючи націоналізацію активів. Організації повинні бути готові до потенційного збільшення кібератак у відповідь на такі рішення. Крім того, ті підприємства, які є частиною критичної інфраструктури, включаючи енергетичні, телекомунікаційні, медіа та фінансові компанії, також мають бути у режимі підвищеної готовності, оскільки саме ці галузі часто вважаються пріоритетними цілями у період війни. Незалежно від того, чи локалізована бізнес діяльність компаній в Україні чи інших країнах, вони повинні оцінити свою готовність до кіберінцидентів і свою здатність відновитися після кібератак.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «Одеський технічний фаховий коледж ОНАХТ»

Відділення *Комп'ютерних систем* Кафедра *Комп'ютерної інженерії*

Освітньо-професійна програма *«Комп'ютерна інженерія»*

Спеціальність *123 «Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР Беркань І.В.

"_____" _____ 20____ р.

ЗАВДАННЯ

на кваліфікаційну роботу бакалавра

здобувачу освіти *Аверіну Володимиру Михайловичу*

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Аналіз новітніх технологій кібербезпеки в період пандемії Covid-19 та воєнного часу*

затверджена наказом по коледжу від "___" *02* 20 *23* р. №_____

2. Термін здачі студентом кваліфікаційної роботи _____

3. Вихідні дані до роботи *1. Складові інформаційної безпеки; 2. Типи загроз кібербезпеки; 3. Серверні інструменти оцінки вразливості; 4. Моніторинг кібербезпеки; 5. Закон України Про основні засади забезпечення кібербезпеки України*

4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити)

1. Інформаційна безпека та кібербезпека;

2. Роль кібербезпеки в період пандемії covid-19 та воєнного часу;

3. Аналіз сучасних процесіву кібербезпеці

5. Перелік графічного матеріалу (слайдів мультимедійної презентації)

Основні складові інформаційної безпеки; Типи загроз кібербезпеки; Профілі навичок у кібербезпеці Топ-30 найпотужніших кібердержав світу; Інциденти безпеки; TCP SYN flood атаки Місце та роль кіберзахисту у забезпеченні кібербезпеки; Схема DoS атаки; TCP flood атака Роль і місце Держспецзв'язку в системі кібербезпеки; Модель кібербезпеки

6. Консультанти по кваліфікаційній роботі, із зазначенням розділів, що стосуються їх

Розділ	Консультант	ПІДПИС	
		Завдання видав	Завдання прийняв
Основний	*Харченко Р.Ю.*		
Охорона праці	*Чорновол Н.І.*		
Нормоконтроль	*Петрашова В.І.*		
Старший консультант	*Кривченко Ю.В..*		

7. Дата видачі завдання 01.05.2023

Керівник роботи *Харченко Р.Ю.* _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	*Аналіз предметної галузі*	5.05.2023	
2.	*Аналіз технічного завдання та пошук літератури*	7.05.2023	
3.	*Кібербезпека як частина інформаційної безпеки*	9.05.2023	
4.	*Огляд ризиків при несанкціонованому доступі*	11.05.2023	
5.	*Аналіз інформаційної безпеки*	13.05.2023	
6.	*Аналіз типів загроз кібербезпеки*	16.05.2023	
7.	*Аналіз рейтингу наймогутніших кібердержав світу*	18.05.2023	
8.	*Аналіз інцидентів безпеки пов'язаних з корона вірусом*	20.05.2023	
9.	*Аналіз кіберзагроз та заходи із захисту від них*	23.05.2023	
10.	*Огляд питань кібербезпеки в умовах воєнного часу*	25.05.2023	
11.	*Аналіз заходів щодо кібербезпекив період пандемії*	27.05.2023	
12.	*Огляд моніторингу кібербезпеки*	30.05.2023	
13.	*Розробка моделі кібербезпеки*	3.06.2023	
14.	*Огляд трендів кібербезпеки*	5.06.2023	
15.	*Розробка питань з охорони праці*	8.06.2023	
16.	*Оформлення креслень та тексту ПЗ*	10.06.2023	

Здобувач освіти _____
(підпис)

Керівник роботи _____
(підпис

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			БКС 27. 01. 000. 00 БКР	***Випускна робота бакалавра***		
А4			***БКС 27. 01. 000. 00 БКР ПЗ***	***Пояснювальна записка***	*1*	

Зм.	Арк.	№ докум.	Підпис	Дата	*БКС 27. 01.000. 00 БКР*		
Розробив		Аверін В.М.			*Аналіз новітніх технологій кібербезпеки в період пандемії Covid-19 та період воєнного часу*	Літ.	Аркуш 4 / Аркушів
Перевірив		Харченко Р.Ю.				У Д П	
Н. Контр.		Петрашова В.І.				*ОТФК ОНТУ, гр. 2БКС-27*	
Затверд.		Кривченко Ю.В.					

ЗМІСТ

ВСТУП

В даний час дуже широко використовується термін «комп'ютерна безпека». За останній час відсоток використання комп'ютерних мереж, а особливо Інтернету значно виріс, тому сьогодні термін «комп'ютерна безпека» використовується для опису проблем, пов'язаних з мережевим використанням комп'ютерів і їх ресурсів. Сучасні інформаційні технології потребують організації високого рівня захисту даних. Комп'ютерна безпека має велике значення для забезпечення захищення систем обробки та зберігання даних. Об'єктами комп'ютерної безпеки є інформаційні ресурси, канали інформаційного обміну і телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури. Особливості захисту персональних комп'ютерів (ПК) обумовлені специфікою їх використання. Загалом, об'єктом захисту в інформаційній системі є інформація з обмеженим доступом, яка циркулює та зберігається у вигляді даних, команд, повідомлень, що мають певну обмеженість і цінність як для її власника, так і для потенційного порушника технічного захисту інформації.

З початку війни Україна стала ціллю чисельних кібератак, які охопили державні установи, приватні організації та громадян. Ті підприємства, які є частиною критичної інфраструктури, зокрема енергетичні, телекомунікаційні, медіа та фінансові компанії, також мають бути у режимі підвищеної готовності, оскільки саме ці галузі часто вважаються пріоритетними цілями у період війни. Бізнес має бути готові протидіяти цим викликам – компанії повинні оцінити свою готовність до кіберінцидентів і свою здатність відновити діяльність.

1 ТЕХНОЛОГІЧНИЙ РОЗДІЛ

1.1 Інформаційна безпека та кібербезпека

1.1.1 Інформаційна безпека

Інформаційна безпека – це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації. Інформація є відомостями, що передаються в усній та письмовій формах за допомогою знаків, технічних механізмів, жестів, програм.

Інформація, безпеку якої необхідно забезпечити, використовується у різноманітних сферах життя: політичній, економічній, соціальній та духовній. Важливо оберігати її від витоку, щоб мінімізувати можливі несприятливі наслідки. Наприклад, економічні втрати на державному рівні.

Інформація вважається безпечною, якщо вона у повному обсязі захищена від будь-яких видів загроз. Найпоширенішими вважаються випадки витоку інформації про платежі та персональні дані (близько 80 % випадків). Правильний підхід у забезпеченні захищеності – це здійснення запобіжних заходів, здатних зменшити згубний вплив усередині та зовні системи.

Інформаційна безпека – це практична діяльність, спрямована на попередження несанкціонованого доступу, застосування, виявлення та перетворення даних. Внутрішні та зовнішні інформаційні загрози можуть завдати шкоди загальнодержавним та міжнародним відносинам, конкретним громадянам. Захист інформації – сукупність юридичних, технічних та організаційних засобів попередження несанкціонованих дій з даними. Вона встановлюється в інформаційних системах та характеризується комплексом заходів та дій, спрямованих на захист даних від стороннього впливу.

В інформаційну систему входять такі елементи:

- суб'єкти – власники інформації та механізмів (інфраструктури);

❖ база – комп'ютерні приміщення, різноманітні системи (електропостачання), лінії зв'язку, обслуговуючий персонал.

1.1.2 Основні складові інформаційної безпеки

Основні складові інформаційної безпеки – це сукупність елементів, що включає доступність, конфіденційність та цілісність інформаційних ресурсів та підтримуючої інфраструктури, (рис.1.1).

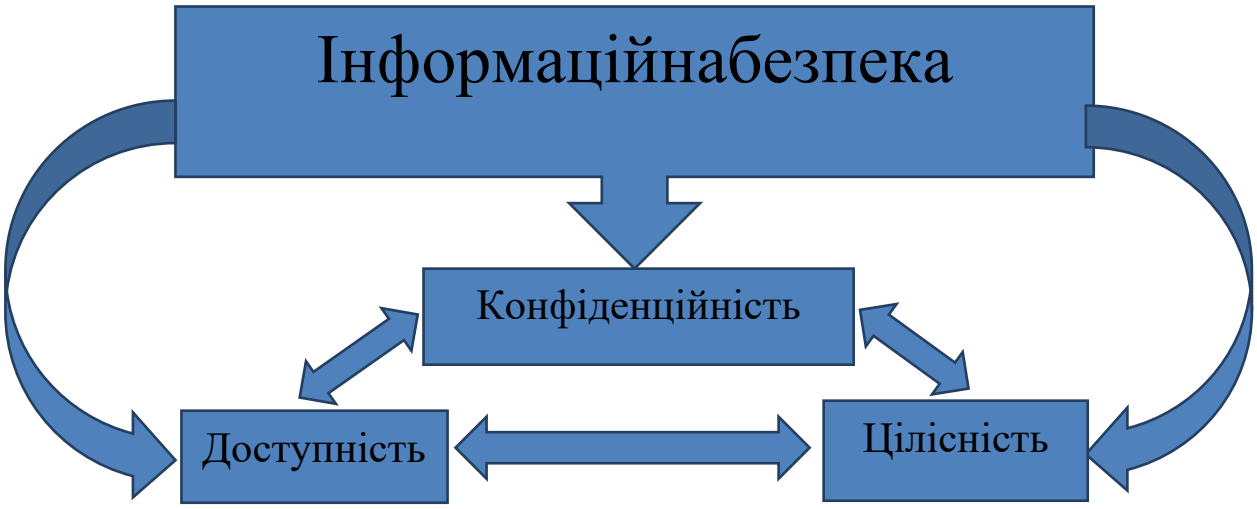


Рисунок 1.1 Основні складові інформаційної безпеки

Доступність – це можливість за прийнятний час одержати необхідну інформаційну послугу.

Інформаційні системи створюються для отримання певних інформаційних послуг. Якщо за тими або іншими причинам надати ці послуги користувачам стає неможливо, це, очевидно, завдає збитку всім суб'єктам інформаційних відносин. Тому, не протиставляючи доступність решті аспектів, ми виділяємо її як найважливіший елемент інформаційної безпеки.

Особливо яскраво основна роль доступності виявляється в різного роду системах управління - виробництвом, транспортом тощо. Зовні менш драматичні, але також вельми неприємні наслідки - і матеріальні, і моральні -

може мати тривала недоступність інформаційних послуг, якими користується велика кількість людей (продаж залізничних та авіаквитків, банківські послуги тощо).

Під **цілісністю** мається на увазі актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованої зміни.

Цілісність можна поділити на статичну (тобто незмінність інформаційних об'єктів) і динамічну (що відноситься до коректного виконання складних дій (транзакцій)). Засоби контролю динамічної цілісності застосовуються, зокрема, при аналізі потоку фінансових повідомлень з метою виявлення крадіжки, переупорядковування або дублювання окремих повідомлень.

Цілісність виявляється найважливішим аспектом інформаційної безпеки в тих випадках, коли інформація служить "керівництвом до дії". Рецептура ліків, наказані медичні процедури, набір і характеристики комплектуючих виробів, хід технологічного процесу - все це приклади інформації, порушення цілісності якої може опинитися в буквальному розумінні смертельним. Неприємно і спотворення офіційної інформації, будь то текст закону або сторінка Web-сервера якої-небудь урядової організації.

Конфіденційність – це захист від несанкціонованого доступу до інформації.

Конфіденційність – найбільш опрацьований у нас в країні аспект інформаційної безпеки. На жаль, практична реалізація заходів по забезпеченню конфіденційності сучасних інформаційних систем натрапляє на серйозні труднощі. По-перше, відомості про технічні канали просочування інформації є закритими, так що більшість користувачів позбавлене можливості скласти уявлення про потенційні ризики. По-друге, на шляху призначеної для користувача криптографії як основного засобу забезпечення конфіденційності стоять численні законодавчі перепони і технічні проблеми.

Якщо повернутися до аналізу інтересів різних категорій суб'єктів інформаційних відносин, то майже для всіх, хто реально використовує ІС, на першому місці стоїть доступність. Практично не поступається їй за важливістю цілісність - який сенс в інформаційній послузі, якщо вона містить спотворені відомості?Нарешті, конфіденційні моменти є також у багатьох організацій (навіть у згадуваних вище учбових інститутах прагнуть не розголошувати дані про екзаменаційні білети до іспиту та окремих користувачів, наприклад, паролі).

1.1.3 Кібербезпека як частина інформаційної безпеки

У світі спостерігається стрімке зростання числа кіберзагроз. Стрічки новин світових ЗМІ щодня повідомляють про нові інциденти. Бізнес та держструктури намагаються вистояти під шквалом атак, хакери спустошують банківські рахунки простих громадян і тому надійний захист від загроз цифрового світу стає базовою потребою. Давайте розберемося, що таке кібербезпека і чому вона така важлива для кожного з нас.

Закон України «Про основні засади забезпечення кібербезпеки України» дає наступні визначення:

Кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі.

Кіберпростір – середовище (віртуальний простір), яке надає можливості (послуговує) здійсненню комунікацій та/або реалізації суспільних відносин, утворене внаслідок функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням Інтернет та/або інших глобальних мереж передачі даних.

Кібербезпека - це захист підключених до Інтернету систем (обладнання, програмного забезпечення та даних) від кіберзагроз.

Рисунок 1.2 Визначення кібербезпеки

Кібербезпека забезпечує захист ресурсів (інформація, комп'ютери, сервери, підприємства, приватні особи). Кібербезпека покликана захистити дані на етапі їх обміну та збереження. Комп'ютерна безпека - це сукупність проблем у галузі телекомунікацій та інформатики, пов'язаних з оцінкою і контролюванням ризиків, що виникають при користуванні комп'ютерами та комп'ютерними мережами і розглядуваних з точки зору конфіденційності, цілісності і доступності. Створення безпечних комп'ютерних систем і додатків є метою діяльності мережевих інженерів і програмістів, а також предметом теоретичного дослідження як у галузі телекомунікацій та інформатики. У зв'язку із складністю і трудомісткістю більшості процесів і методів захисту цифрового обладнання, інформації та комп'ютерних систем від ненавмисного чи несанкціонованого доступу вразливості комп'ютерних систем становлять значну проблему для їхніх користувачів.

Поняття «кібербезпека» та «інформаційна безпека» досить часто використовуються як синоніми. Проте насправді ці терміни сильно різняться і є взаємозамінними. Під кібербезпекою розуміють захист від атак у кіберпросторі, а під інформаційною безпекою – захист даних від будь-яких форм загроз, незалежно від того, чи вони є аналоговими чи цифровими.

1.1.4 Завдання кібербезпеки

Практики кібербезпеки можуть застосовуватися в різних областях — від промислових підприємств до мобільних пристроїв звичайних користувачів:

- ❖ Безпека критичної інфраструктури – заходи захисту комп'ютерних систем, мереж об'єктів критичної інформаційної інфраструктури (КІІ). До об'єктів КІІ належать електричні мережі, транспортна мережа, автоматизовані системи управління та інформаційно-комунікаційні системи та багато інших систем, захист яких має життєво важливе значення для безпеки країни та благополуччя громадян.
- ❖ Безпека мережі — захист базової мережевої інфраструктури від несанкціонованого доступу та неправильного використання, а також від крадіжки інформації. Технологія включає створення безпечної інфраструктури для пристроїв, додатків і користувачів.
- ❖ Безпека програм — заходи безпеки, які застосовуються на рівні програм і спрямовані на запобігання крадіжці, злому даних або коду програми. Методи охоплюють питання безпеки, що виникають під час розробки, проектування, розгортання та експлуатації додатків.
- ❖ Хмарна безпека – взаємопов'язаний набір політик, елементів керування та інструментів захисту систем хмарних обчислень від кіберзагроз. Заходи хмарної безпеки спрямовані на забезпечення безпеки даних, онлайн-інфраструктури, а також додатків та платформ. Хмарна безпека має низку загальних концепцій із традиційною кібербезпекою, але в цій галузі є також власні передові методи та унікальні технології.
- ❖ Навчання користувачів. Програма підвищення обізнаності у сфері інформаційної безпеки (securityawareness) є важливим заходом для побудови надійного захисту компанії. Дотримання працівниками правил цифрової гігієни допомагає посилити безпеку кінцевих точок. Так, користувачі, поінформовані про актуальні загрози, не відкриватимуть вкладення з підозрілих електронних

листів, відмовляться від використання ненадійних USB-пристроїв і перестануть прикріплювати на монітор наклейки з логіном та паролем.

❖ Аварійне відновлення (планування) безперервності бізнесу — сукупність стратегій, політик та процедур, що визначають, яким чином організація має реагувати на потенційні загрози чи непередбачені стихійні лиха, щоб належним чином адаптуватися до них та мінімізувати негативні наслідки.

❖ Операційна безпека — процес управління безпекою та ризиками, який запобігає попаданню конфіденційної інформації до чужих рук. Принципи операційної безпеки спочатку використовували військові, щоб дати секретної інформації потрапити до противника. В даний час практики операційної безпеки широко використовуються для захисту бізнесу від потенційних витоків даних.

1.1.5 Типи загроз кібербезпеки

Технології та найкращі практики кібербезпеки захищають критично важливі системи та конфіденційну інформацію від стрімкого зростання обсягу витончених кібератак. Нижче наведено основні типи загроз, з якими бореться сучасна кібербезпека:

❖ Шкідливе програмне забезпечення

Будь-яка програма або файл, які можуть завдати шкоди комп'ютеру, мережі чи серверу. До шкідливих програм належать комп'ютерні віруси, черв'яки, трояни, програми-вимагачі та програми-шпигуни. Шкідливі програми крадуть, шифрують та видаляють конфіденційні дані, змінюють або захоплюють основні обчислювальні функції та відстежують активність комп'ютерів або програм.

❖ Соціальна інженерія

Метод атак, заснований на людській взаємодії. Зловмисники втираються у довіру до користувачів та змушують їх порушити процедури безпеки, видати конфіденційну інформацію.

❖ Фішинг

Форма соціальної інженерії. Шахраї надсилають користувачам електронні листи або текстові повідомлення, що нагадують повідомлення з довірених джерел. При масових атаках фішингових зловмисники виманюють у користувачів дані банківських карт або облікові дані.

❖ Цільова атака

Тривала та цілеспрямована кібератака, при якій зловмисник отримує доступ до мережі та залишається непоміченим протягом тривалого часу. Цільові атаки зазвичай спрямовані на крадіжку даних у великих підприємств чи урядових організацій.

❖ Внутрішні загрози

Порушення безпеки чи втрати, спровоковані інсайдерами — співробітниками, підрядниками чи клієнтами — із злим наміром чи через недбалість.

❖ DoS-атака, або атака типу "відмова в обслуговуванні"

Атака, за якої зловмисники намагаються унеможливити надання послуги. При DoS-атаці шкідливі запити надсилає одна система; DDoS-атака виходить із кількох систем. В результаті атаки можна заблокувати доступ практично до всього: серверів, пристроїв, служб, мереж, додатків і навіть певних транзакцій усередині додатків.

❖ Сталкерське ПЗ

Програмне забезпечення призначене для прихованого стеження за користувачами. Сталкерські програми часто поширюються під виглядом легального ПЗ. Такі програми дозволяють зловмисникам переглядати фотографії та файли на пристрої жертви, підглядати через камеру смартфона в

режимі реального часу, дізнаватися про місцезнаходження і читати листування в месенджерах і записувати розмови.

❖ Криптоджекінг

Відносно новий тип кіберзлочинів, при яких шкідливе програмне забезпечення ховається в системі і викрадає обчислювальні ресурси пристрою, щоб зловмисники могли їх використовувати для видобутку криптовалюти. Процес криптоджекінгу повністю прихований від очей користувачів.

❖ Атаки на ланцюжок поставок

Атаки на ланцюжок поставок експлуатують довірчі відносини між організацією та її контрагентами. Хакери компрометують одну організацію, а потім просуваються вгору ланцюжком поставок, щоб отримати доступ до систем інший.

❖ Атаки з використанням штучного інтелекту

За таких атак зловмисник намагається обдурити машинний алгоритм, змушуючи його видавати неправильні відповіді. Зазвичай кіберзлочинці використовують метод «отруєння даних», пропонуючи нейромережі для навчання свідомо некоректну вибірку.

Рисунок 1.3 Типи загроз кібербезпеки

Ці фактори, серед інших, говорять про те, що базове розуміння кіберзагроз необхідно перемістити з професійної областіIT-фахівців в область загального знання. Кожен співробітникповинен мати певне уявлення про сучасні загрози, а тим більшекерівник, який ставить завдання фахівцям з кібербезпеки

1.1.6 Об'єкти кібербезпеки та кіберзахисту

1. Об'єктами кібербезпеки є:

- людина і громадянин, їхні конституційні права і свободи;
- суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;
- держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканість;
- національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави.

2. Об'єктами кіберзахисту є:

- комунікаційні системи державної, комунальної, інших форм власності, в яких оброблюються національні інформресурси та/або які використовуються в інтересах органів державної влади та місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до законів України;
- комунікаційні та технологічні системи критичних інфраструктурних об'єктів;
- комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

3. Об'єкти кіберзахисту у сукупності складають критичну інформаційною інфраструктуру і підлягають внесенню до державного реєстру об'єктів критичної інформаційної інфраструктури. Порядок формування та забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури затверджується Кабінетом Міністрів України.

1.1.7 Аналіз профілей навичок у кібербезпеці

Агентство Європейського Союзу з кібербезпеки ENISA підготувало профілі навичок у кібербезпеці з описами посад, місіями, завданнями, навичками, знаннями та компетенціями, (рис.1.4).

Рисунок 1.4. Профілі навичок у кібербезпеці

1.Головний спеціаліст з інформаційної безпеки (Chiefinformationsecurity officer (CISO))

Керує стратегією кібербезпеки організації та її реалізацією, щоб забезпечити належну безпеку та захист цифрових систем, послуг і активів.

2. Реагувальник на кіберінциденти (Cyber incident responder)

Відстежує стан кібербезпеки організації та обробляє інциденти під час кібератак.

3. Спеціаліст з питань кібер-юриспруденції, політики та відповідності (Cyberlegal, policy&compliance officer)

Керує дотриманням стандартів, пов'язаних із кібербезпекою, законодавчої та нормативної бази на основі стратегії організації та правових вимог.

4. Спеціаліст з розвідки кіберзагроз (Cyber threat intelligence specialist)

Збирає, обробляє, аналізує дані та інформацію для створення дієвих звітів розвідки та розповсюджує їх серед зацікавлених сторін.

5. Архітектор з кібербезпеки (Cybersecurity architect)

Планує та проектує рішення безпеки за проектом (інфраструктури, системи, активи, програмне забезпечення, апаратне забезпечення та послуги) і засоби контролю кібербезпеки.

6. Аудитор з кібербезпеки (Cybersecurity auditor)

Проводить аудит кібербезпеки екосистеми організації. Забезпечення відповідності законодавчій, нормативній, політикам, вимогам безпеки, галузевим стандартам і найкращим практикам.

7. Педагог з кібербезпеки (Cybersecurity educator)

Покращує знання, навички та компетенцію з кібербезпеки у людей.

8. Реалізатор кібербезпеки (Cybersecurityimplementer)

Розробляє, розгортає та керує рішеннями кібербезпеки (системами, активами, програмним забезпеченням, елементами керування та послугами) в інфраструктурі та продуктах.

9. Дослідник кібербезпеки (Cybersecurityresearcher)

Досліджує галузь кібербезпеки та впроваджує результати в рішення з кібербезпеки.

10. Менеджер ризиків кібербезпеки (Cybersecurity risk manager)

Управляє ризиками організації, пов'язаними з кібербезпекою, відповідно до стратегії організації. Розробляє, підтримує та комунікує про процеси та звіти з управління ризиками.

11. Цифровий слідчий-криміналіст (Digital forensics investigator)

Забезпечує розслідування кіберзлочинів, виявляє всі цифрові докази, які підтверджують зловмисну діяльність.

12. Тестер проникнення (Penetrationtester)

Оцінює ефективність засобів контролю безпеки, виявлення та використання вразливостей кібербезпеки, оцінює їх критичність в разі експлатування.

1.1.8 Рейтинг наймогутніших кібердержав світу

Цифровий ландшафт — кіберпростір — це нове поле битви, оскільки держави намагаються протистояти одна одній за допомогою кіберзасобів і збільшувати свою кіберпотужність.

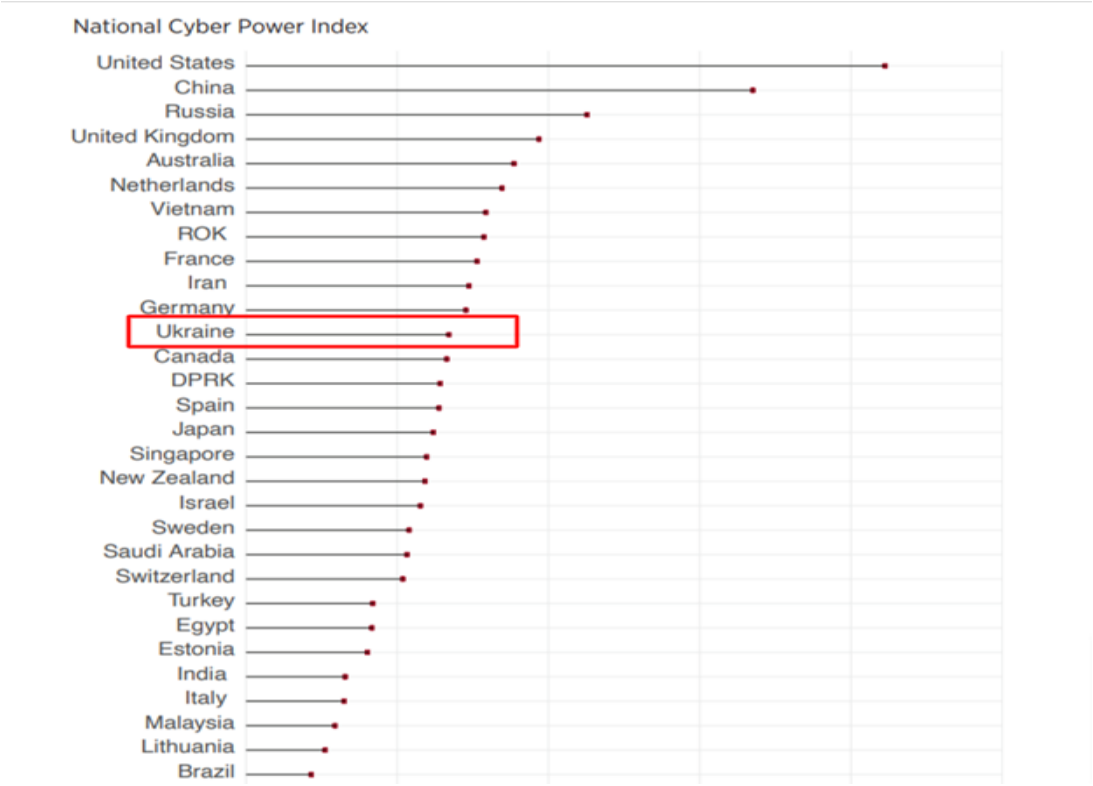


Рисунок 1.5 Топ-30 найпотужніших кібердержав світу

Центр науки та міжнародних відносин Роберта та Рене Бельфера Гарвардського університету опублікував Національний індекс сил

кібербезпеки (NationalCyberPowerIndex, скор. – NCPI), або Національний індекс кіберпотужності за 2022 рік.,(рис.1.5).

Сполучені Штати займаютьперше місце в списку Топ-30. Україна поки не потрапила до Топ-10, посівши 12 місце, але здійснила гігантський стрибок із 29 місця у 2020 році завдяки збільшенню рівня кіберзахисту, розвідки та руйнівної діяльності.

1.2. Роль кібербезпеки в період пандемії covid-19 та воєнного часу

1.2.1 Посилення деструктивної кіберактивності під час карантину

Етап сучасного розвитку Української держави характеризується повною комп'ютеризацією всіх сфер життя. Водночас перенесення багатьох процесів, у тому числі пов'язаних із критичною інфраструктурою, у кіберпростір, маючи позитивні моменти, має й негативні наслідки: вразливість цих процесів до численних кіберзагроз. Пандемія COVID-19, серед іншого, загострила занепокоєння щодо кібербезпеки, оскільки кризи традиційно сприяли ескалації різних хакерських груп. Нижче описані основні фактори, які можуть сприяти посиленню деструктивної (нелегальної) кіберактивності.

Практика запровадження карантинного режиму спонукає роботодавців змінити характер виробничих відносин із працівниками на формат дистанційної роботи. У більшості випадків ці взаємодії відбуваються через Інтернет. Як наслідок, збільшується кількість потенційно вразливих ланок, які можуть скомпрометувати інформацію або саму організацію, її співробітників тощо. Обмеження на поїздки, максимальні обмеження розрахунків готівкою, а також збільшення часу, проведеного громадянами вдома, призводять не лише до збільшення часу користування Інтернетом загалом, а й до збільшення електронних платежів зокрема. В результаті традиційно зростає кількість фішингових атак – зростає кількість фейкових листів (із вбудованим

шкідливим програмним забезпеченням) і фейкових сайтів (для збору особистої та банківської інформації громадян).

Кількість людей, які вперше починають працювати віддалено і не завжди знають, як це зробити, стрімко зростає, тому деякі організації тимчасово спрощують доступ до інформації, надаючи її співробітникам у віддаленому форматі. У той же час ці співробітники часто використовують набагато менш безпечне телекомунікаційне середовище, ніж на робочому місці в офісі. Все це підвищує ризик витоку конфіденційної інформації.

Експерти також відзначають, що джерелом атаки на домашні системи співробітників можуть бути сервіси відеорепетиторів, якими можуть користуватися їхні діти, які також перебувають на карантині (ці сервіси традиційно набагато менш захищені, ніж інші).

1.2.2 Аналіз інцидентів безпеки пов'язаних з корона вірусом

Поширення коронавірусу в Україні посприяло появі значної кількості додатків та ботів, які допомагають користувачам відслідковувати останні новини, пов'язані із COVID-19. В той же час кіберзлочинці, намагаються використати таку "оболонку новин про вірус" для поширення "зараженого" програмного забезпечення на різних ресурсах.

Зокрема, зафіксовані випадки поширення "вірусного" програмного забезпечення під виглядом додатків для відстеження ситуації із коронавірусом, яке незаконно здійснювало збір персональних та банківських даних осіб.

У 2020 році були виявлені онлайн-карти поширення коронавірусу, які показують актуальні дані, але при цьому впроваджують на комп’ютери шкідливе програмне забезпечення. Фахівці безпеки виявили, що хакери використовують ці карти для крадіжки інформації користувачів, включаючи імена користувачів, паролі, номери кредитних карт і інші дані.

Зловмисники розробляли сайти, пов’язані з коронавірусом, щоб запропонувати завантажити додаток, яке повідомляє про зміни ситуації з вірусом. Ця програма не вимагає установки і показує карту поширення COVID-19. Однак зловмисники можуть створити шкідливий файл і встановити його на свій комп’ютер.

Ці веб-сайти є справжні карти для відстеження коронавірусу, але мають іншу URL-адресу або інші деталі з вихідного джерела. В цьому методі використовувалося шкідливе програмне забезпечення, відоме як AZORult, яке було вперше виявлено в 2016 році. Воно призначене для крадіжки даних з вашого комп’ютера і зараження іншими шкідливими програмами. AZORult може вкрасти інформацію з вашого комп’ютера, включаючи паролі і криптовалюти. Він також може завантажувати додаткові шкідливі програми на заражені машини. AZORult зазвичай продається на російських підпільних форумах з метою збору конфіденційних даних з зараженого комп’ютера.

Дослідження показало, що домени, пов’язані з коронавірусом, на 50 відсотків частіше встановлюють шкідливе ПЗ в нашу систему.

Публічно зареєстровані інциденти безпеки (при використанні хмарних технологій) в регіонах - за кількістю порушень представлені на Рисунку 1.6.

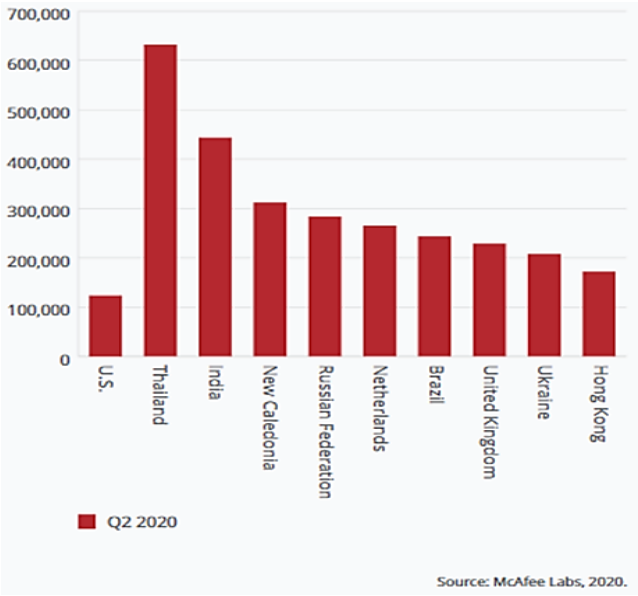


Рисунок 1.6 Інциденти безпеки (при використанні хмарних технологій), що відбулися в регіонах.

Найбільша кількість хмарних інцидентів сталося в Таїланді, менше - в США, Україна - за меншої їх кількості - на третьому місці після США і Гонконгу.

В останньому звіті відомої компанії McAfee® Labs про загрози (за листопад 2020 г.) докладніше розглядаються загрози і інциденти безпеки, які проявилися в умовах COVID-19 у другому кварталі 2020 року і постійно збільшуються в обсязі і масштабі на сьогоднішній день.

Результати дослідженьв порівнянні з попереднім кварталом показують:

- Збільшення загроз в середньому - 419 в хвилину.
- Поява нових шкідливих програм для Office зросла на 103%.
- Кількість нових шкідливих програм DonoffPowerShell збільшилася на 117%.
- Збільшення нових шкідливих програм для Linux на 22%

Зловмисники перенаправили все більш витончені методи в сторону підприємств, урядів, шкіл і співробітників, які продовжують ще стикатися з проблемами, пов'язаними з обмеженнями COVID-19 і потенційними уразливими віддалених пристроїв і безпеки їх смуги пропускання.

У цих умовах для співробітників як і раніше важливо дотримуватися протоколи безпеки і зберігати пильність щодо зловмисників, остерігатися використовувати зовнішні вкладення електронної пошти і неперевірені посилання, фішингові точки входу, через які можуть бути доставлені і ініційовані програми-вимагачіі інші шкідливі програми.

1.2.3 Заходи щодо кібербезпеки в період пандемії

В умовах карантину, коли значна частина населення перейшла на дистанційний режим роботи, перш за все варто подбати про кібербезпеку. Наразі немає переконливих доказів збільшення кібершахрайства, пов’язаного з

пандемією, але все більше експертів радять громадянам і роботодавцям вжити оперативних заходів для мінімізації потенційних негативних наслідків.

До них належать:

- забезпечення належного рівня цифрової гігієни для користувачів та вдосконалення їхніх цифрових навичок;
- використання VPN (особливо в громадських місцях);
- мінімізація використання відкритого (публічного) WiFi;
- підвищена увага до будь-яких незнайомих листів або тих, що містять «емоційні» заголовки з посиланнями;
- використовувати лише офіційну інформацію та дані;
- негайне повідомлення роботодавця у разі втрати/викрадення персонального мобільного пристрою, з якого працівник міг отримати доступ до робочого обладнання;
- постійний контакт між роботодавцями та працівниками щодо кібер-інцидентів.

Основним та й зрештою відомим правилом є заборона переходити за підозрілими посиланнями та заборона завантажувати програми із сумнівних ресурсів. Однак, компанії, які працюють із конфіденційною інформацією повинні передбачити додаткові механізми захисту. Зокрема, усі необхідні файли, які містять конфіденційну інформацію, варто зберігати у хмарному сховищі із надійним паролем та доступом тільки тих осіб, які залучені у проект. Обладнання, яке передається для дистанційної роботи, має бути захищеним від стороннього втручання надійними паролями до самого пристрою, до папок, де зберігається конфіденційна інформація та до програм, які використовуються при роботі із нею.

Також варто проводити із працівниками додаткові тренінги про роботу у дистанційному режимі та звертати увагу на окремі правила кібербезпеки, зокрема такі як: не під'єднувати робочий ноутбук до підозрілих пристроїв чи

мереж, не надавати дозвіл на обробку персональних даних підозрілим сайтам тощо.

1.2.4 Питання кібербезпеки в умовах воєнного часу

З початку війни Україна стала ціллю чисельних кібератак, які охопили державні установи, приватні організації та громадян. Ті підприємства, які є частиною критичної інфраструктури, зокрема енергетичні, телекомунікаційні, медіа та фінансові компанії, також мають бути у режимі підвищеної готовності, оскільки саме ці галузі часто вважаються пріоритетними цілями у період війни. Бізнес має бути готові протидіяти цим викликам – компанії повинні оцінити свою готовність до кіберінцидентів і свою здатність відновити діяльність.

Необхідно провести огляд наявних планів реагування, щоб краще зрозуміти ризики поточних сценаріїв загроз, які з великою ймовірністю можуть відбутися, враховуючи такі фактори, як профіль компанії, її географію тощо.

Що потрібно зробити:

- Переглянути ландшафт потенційних загроз для вашого бізнесу, налагодити зв’язок з організаціями, які надають інформацію щодо загроз кібербезпеки (ThreatIntelligence) аби краще зрозуміти бізнес ризики та заходи, яких необхідно вжити;
- Врахувати можливість призупинення діяльності в регіонах, де вже відбуваються бойові дії або велика імовірність того, що це може відбутися найближчим часом, і те, як мінімізувати ці ризики для бізнесу Наприклад, що роботи в разі недоступності важливих функцій, частково або повністю IT-інфраструктури, телефонного зв’язку тощо;
- За необхідності забезпечити евакуацію або переїзд працівників та їх сімей, офісу, систем; перевести компанію в гібридний/віддалений формат роботи (якщо це не було зроблено під час пандемії), забезпечити роботу

кризового штабу для забезпечення безпеки людей та безперервності/відновлення роботи компанії ;

❖ Переглянути плани реагування на інциденти та плани неперервності, поставити собі наступні запитання: Як часто проводиться тестування планів? Чи спрацюють тестові сценарії під час поточних загроз? Оновити плани реагування на інциденти безпеки та створити конкретні плани реагування у відповідності до основних сценаріїв;

❖ Переконатися, що договори з постачальниками послуг з реагування та стримування атак є актуальними;

❖ Переглянути всі нормативні вимоги щодо необхідності звітування про інциденти кібербезпеки;

❖ Розглянути можливість проактивного налагодження зв'язків з правоохоронними та державними органами, які мають бути залучені у разі масштабного інциденту кібербезпеки;

❖ Подумати про проведення симуляцій реагування на кібератаки, якщо такі вправи не виконувались протягом останніх шести місяців.

1.2.4.1 Заходи кіберзахисту

Необхідно переглянути ключові набори контролів кібербезпеки, які можуть допомогти знизити ймовірність успішності атак, зокрема тих, які допомагають захиститися від загроз від держави-агресора або організованих угруповань, які активізували свою діяльність під час війни.

Що потрібно зробити:

❖ Надати пріоритет задачам з встановлення виправлень (патчів) усіх критичних вразливостей у системах – особливо для тих, які зараз активно використовуються зловмисниками. Агентство з кібербезпеки та безпеки інфраструктури США (CISA) веде базу даних таких вразливостей, а деякі

центри кібербезпеки надають поради щодо того, на які з них слід звернути першочергову увагу;

❖ Переглянути контролі доступу до ключових систем, зосереджуючи увагу на багатофакторній аутентифікації, видаленні облікових записів, що не використовуються або термін дії яких закінчився, а також необхідності ізоляції систем, що мають високий ризик;

❖ Переконатися, що захист від шкідливого ПЗ встановлений, ліцензії актуальні і програми регулярно оновлюються;

❖ Виконати зовнішнє сканування вразливостей для систем, що мають доступ до інтернету, і усунути найбільш важливі недоліки;

❖ Переконатися, що для критичних систем налаштовані процеси резервного копіювання і регулярно створюються офлайн копії важливих бізнес-даних.

1.2.4.2 Моніторинг кібербезпеки

Окрім превентивного захисту ефективний моніторинг безпеки є також важливим з огляду на своєчасне виявлення та реагування на вторгнення. Середній час між початковою компрометацією і запуском деструктивного шкідливого ПЗ тепер вимірюється днями, а не тижнями або місяцями, як було раніше.

Що потрібно зробити:

❖ Зрозуміти поточні можливості з моніторингу кібербезпеки у мережевій інфраструктурі організації, щоб переконатися в існуванні можливостей з виявлення та запобігання інцидентів кібербезпеки та охопленні ними бізнес послуг, систем та даних;

❖ Якщо в компанії є команда з полювання на загрози, доручити їм пошук індикаторів компрометації (IOC), заснованих на тактиках, техніках та процедурах (TTP’s), пов’язаних з групами, що асоціюються з державою-

агресором або її партнерами, або організованими злочинними групами, які залучені до війни на кіберфронті;

❖ Подумати про залучення зовнішніх вендорів, що надають послуги керованого виявлення та реагування, з метою розширення ваших можливостей та отримання кваліфікованої підтримки у разі потреби.

1.2.4.3 Людський фактор кібербезпеки

Підприємствам слід планувати можливу зупинку своєї діяльності в регіонах бойових дій та у деяких випадках організовувати тимчасову кадрову підтримку для забезпечення функціонування своїх критичних сервісів, допоки їхні співробітники не зможуть повернутися до офісу або в країну. Окрім підтримки співробітників та їхніх сімей, організації також мають знати про ризики організованих злочинних груп. Ці групи намагаються скористатися кризою на свою користь, створюючи підроблені веб-сайти, які нібито пропонують допомогу чи корисну інформацію, або приймають пожертвування. Є велика ймовірність фішингових кампаній, орієнтованих на тематику війни в Україні і спрямованих на високопоставлених осіб, які відкрито висловлюють свою позицію стосовно війни.

Що потрібно зробити:

❖ Пересвідчитись, що співробітники мають доступ до надійних та перевірених джерел інформації щодо поточної ситуації і є обізнаними щодо ризиків фішингу і шахрайських веб сайтів з тематики війни в Україні;

❖ Надавати поради з кібербезпеки для співробітників, що знаходяться в місцях потенційного ризику або працюють на високих позиціях;

❖ Надавати психологічну підтримку співробітникам та їх сім’ям, включаючи проведення тренінгів або семінарів щодо дій в непередбачуваних або кризових ситуаціях;

❖ Подумати про термінову додаткову підтримку в управлінні звичайними функціями безпеки, аналізу збільшеного обсягу сповіщень безпеки та реалізації термінових покращень щодо безпеки.

1.2.4.4 Ризики партнерів, вендорів і ланцюгів поставок

На початку пандемії COVID-19, коли підприємства припиняли свою роботу, а співробітників відправили додому, організації швидко зрозуміли, наскільки залежними вони стали від складної екосистеми третіх сторін, що надають критичні системи, послуги та дані. Воєнний стан в Україні знову підкреслює важливість розуміння безпеки та стійкості усіх партнерів у важливих напрямках ланцюгів поставок.

Що потрібно зробити:

❖ Ідентифікувати залежності від вендорів і партнерів, та створити резервний план, якщо раптом за певних умов вони будуть виключені з ланцюгів постачання;

❖ Для критичних постачальників (щонайменше) налаштувати посилений моніторинг вхідного мережевого трафіку, оскільки кіберзлочинність може стати більш витонченою та складною через дії численних хакерських груп, у яких розв’язані руки в поточній ситуації;

❖ Для критичних постачальників (щонайменше), перевірити наявність та актуальність планів реагування на інциденти та планів забезпечення стійкості;

❖ Зрозуміти вплив на вашу організацію потенційних інцидентів у ваших ланцюгах поставок, щоб визначити, де саме зосередити посилений моніторинг та підвищити готовність до реагування.

1.2.4.5 Міграція у хмару

Воєнний стан в Україні викликає занепокоєння компаній також через нові виклики у забезпеченні безперебійної роботи критичних сервісів та систем, які можуть бути пошкоджені або виведені з ладу внаслідок бойових дій. Перенесення IT-інфраструктури в хмару або створення сайтів аварійного відновлення у глобальних хмарних ЦОД (центр опрацювання даних) дозволить гарантувати необхідний рівень доступності.

Що потрібно зробити:

- Проаналізувати наявну IT-архітектуру на предмет можливості та доцільності міграції в хмару, враховуючи технічні (можливість/складність перенесення в хмару), фінансові, регуляторні та питання безпеки;
- Обрати провайдера хмарних сервісів, враховуючи наявні компетенції IT-спеціалістів;
- Визначити черговість та критичність перенесення тих чи інших елементів IT-архітектури в хмару;
- Розглянути та обрати наявні на ринку хмарні сервіси, зокрема для забезпечення віддаленої роботи (проведення відеодзвінків, офісне програмне забезпечення тощо);
- Організувати збереження резервних копій інформації в хмарі;
- Організувати сайти аварійного відновлення в публічній хмарі в Європі або США.

Поточна ситуація залишається непередбачуваною – компаніям та організаціям важливо постійно аналізувати, як ситуація може розвиватися далі, та які сценарії можуть виникнути. Для кожного сценарію у компанії має бути аналіз, як той чи інший сценарій вплине на організацію з огляду на людей, бізнес, ланцюги поставок і технології. При цьому деякі розглянуті рекомендації можна впровадити вже зараз, щоб підготуватися до таких випадків, підвищити

стійкість, зменшити вплив і скоротити тривалість інцидентів, якщо вони відбудуться.

1.3 Аналіз сучасних процесів у кібербезпеці

1.3.1 Реагування на різні види подій у кіберпросторі

Згідно з постановою Кабінету Міністрів України від 4 квітня 2023 р. № 299, про порядок реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі:

1) Цей Порядок визначає процедури реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі (далі - кіберінциденти/кібератаки) та категорії (рівні) їх критичності.

2) У цьому Порядку терміни вживаються у значенні, наведеному в Законі України "Про основні засади забезпечення кібербезпеки України" та постанові Кабінету Міністрів України від 29 грудня 2021 р. № 1426 "Про затвердження Положення про організаційно-технічну модель кіберзахисту" (Офіційний вісник України, 2022 р., № 4, ст. 219).

3) Реагування на кіберінциденти/кібератаки здійснюється суб'єктами забезпечення кібербезпеки шляхом вжиття заходів до кіберзахисту, спрямованих на швидке виявлення та захист від кіберінцидентів/кібератак, належне інформування про них, запобігання негативним наслідкам, їх мінімізації та усунення, виправлення вразливостей, а також відновлення сталості і надійності функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем та інших об'єктів кіберзахисту.

Суб'єкти забезпечення кібербезпеки вживають заходів відповідно до методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджених Адміністрацією Держспецзв'язку.

4) Реагування на кіберінциденти/кібератаки здійснюється суб'єктами забезпечення кібербезпеки послідовно такими етапами, як підготовка, виявлення та аналіз, стримування, усунення, відновлення, аналіз ефективності заходів з реагування на кіберінциденти/кібератаки.

5) Реагування суб'єктами забезпечення кібербезпеки на кіберінциденти/кібератаки розпочинається з етапу підготовки, під час якого здійснюються заходи з вивчення та дослідження сучасних видів кіберінцидентів/кібератак, розроблення методів і механізмів запобігання та протидії можливим кіберінцидентам/кібератакам.

6) На етапі виявлення та аналізу суб'єкти забезпечення кібербезпеки здійснюють виявлення кіберінциденту/кібератаки та визначають їх критичність для забезпечення пропорційності та/або співрозмірності подальших заходів з кіберзахисту реальним та потенційним ризикам.

Суб'єкти забезпечення кібербезпеки визначають критичність кіберінциденту/кібератаки відповідно до методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджених Адміністрацією Держспецзв'язку, за такими категоріями (рівнями):

- ❖ рівень 0, некритичний (білий) - кіберінцидент/кібератака не загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем;
- ❖ рівень 1, низький (зелений) - кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, але не загрожує захищеності (конфіденційності, цілісності і доступності) інформації та даних, що ними обробляються;

❖ рівень 2, середній (жовтий) - кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, внаслідок чого створюються передумови для порушення захищеності (конфіденційності, цілісності і доступності) інформації та даних, що ними обробляються, виникають передумови для припинення виконання функцій та/або надання послуг критичною інфраструктурою;

❖ рівень 3, високий (помаранчевий) - кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що ними обробляються, внаслідок чого виникають потенційні загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг критичною інфраструктурою. Реагування на цьому рівні може потребувати залучення сил та засобів більше ніж одного основного суб'єкта національної системи кібербезпеки;

❖ рівень 4, критичний (червоний) - кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування кількох інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що ними обробляються, внаслідок чого виникають реальні загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг критичною інфраструктурою. Кіберінцидент/кібератака може мати транскордонний вплив.

Реагування на цьому рівні потребує залучення сил та засобів основних суб'єктів національної системи кібербезпеки;

❖ рівень 5, надзвичайний (чорний) - кіберінцидент/кібератака безпосередньо загрожує сталому, надійному та штатному режиму функціонування значної кількості інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, порушується захищеність (конфіденційність, цілісність і доступність) інформації та даних, що ними обробляються, внаслідок чого виникають невідворотні загрози для повноцінного функціонування держави або загроза життю громадян України. Кіберінцидент/кібератака може мати транскордонний вплив. Реагування на цьому рівні потребує максимального залучення сил та засобів основних суб'єктів національної системи кібербезпеки та інших суб'єктів забезпечення кібербезпеки.

7) Під час етапу стримування суб'єктами забезпечення кібербезпеки вживаються заходи до зниження негативного впливу кіберінциденту/кібератаки, запобігання порушенню безпеки, забезпечення сталого, надійного та штатного режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, несанкціонованого втручання в їх роботу, захищеності (конфіденційності, цілісності і доступності) інформації та даних, що ними обробляються.

8) Під час етапу усунення суб'єкти забезпечення кібербезпеки вживають заходів до ліквідації наслідків кіберінциденту/кібератаки для інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем, інформації та даних, що ними обробляються.

9) На етапі відновлення суб'єктами забезпечення кібербезпеки вживаються заходи до відновлення безпеки, сталого, надійного, штатного та захищеного від несанкціонованого втручання в роботу режиму функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних

систем, технологічних систем, захищеності (конфіденційності, цілісності і доступності) інформації та даних, що ними обробляються.

10) За результатами вжиття заходів до кіберзахисту суб'єкти забезпечення кібербезпеки проводять аналіз ефективності реагування на кіберінциденти/кібератаки.

Під час цього етапу забезпечується вивчення задокументованих даних щодо кіберінциденту/кібератаки, інформування керівництва суб'єкта забезпечення кібербезпеки, узагальнення та проведення аналізу досвіду реагування для подальшого підвищення ефективності вжиття заходів до кіберзахисту у разі можливих кіберінцидентів/кібератак у подальшому.

1.3.2Модель взаємодії підсистеми кіберзахисту у складі системи забезпечення кібербезпеки України.

Кіберпростір є середовищем, яке принципово відрізняється від звичайного фізичного світу. Проте він є надзвичайно фізичним середовищем : створений фізичними мережами й системами,що поєднані між собою, та підпорядковуються певним правилам, що проявляються через програмне забезпечення та комунікативні протоколи. Крім того, основа роботи кіберпростору – це суто фізичні закони електромагнетизму та світла. Вони створюють його основну особливість – можливість глобальних комунікацій та передачі масштабних обсягів даних, які здійснюються майже миттєво і передаються на великі відстані, незважаючи на географічні кордони. Саме швидкість і незалежність від фізичних перешкод дає найважливішу перевагу і одночасно створює проблему, оскільки можливості кіберпростору можуть бути використані будь-ким та з будь-якою метою.

Визнаючи кіберпростір одним із середовищ застосування геостратегій та «п'ятим плацдармом» проведення бойових дій, разом із суходолом, морем, повітрям і космосом, дедалі більше уваги приділяється розвитку й захисту

інформаційних ресурсів, а також можливостям впливати на інформаційні ресурси інших країн, що загалом описується як проблема забезпечення кібербезпеки держави.

У Законі України «Про основні засади забезпечення кібербезпеки України» [9] кібербезпека визначається, як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі», а кіберпростір – «середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних». Ці визначення є результатом відповідного компромісу суб'єктів забезпечення кібербезпеки та не відповідають повною мірою визначенням, які запропоновані в міжнародній практиці [10].Очікуються, що в нову редакцію Закону будуть внесені уточнення і врахується як отриманий національний, так і міжнародний досвід.

Кібербезпеку забезпечують суб'єкти кібербезпеки, які здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних, маніпулятивних та інших протиправних і злочинних цілях, виявляють і реагують на кіберінциденти та кібератаки, усунення їх наслідків, провадять інформаційний обмін щодо реалізованих та потенційних кіберзагроз, розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту, забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління, здійснюють інші заходи із забезпечення розвитку та безпеки

кіберпростору. Схематично модель взаємодії підсистеми кіберзахисту у складі системи забезпечення кібербезпеки та іншими її складовими представлена на Рисунку 1.7.

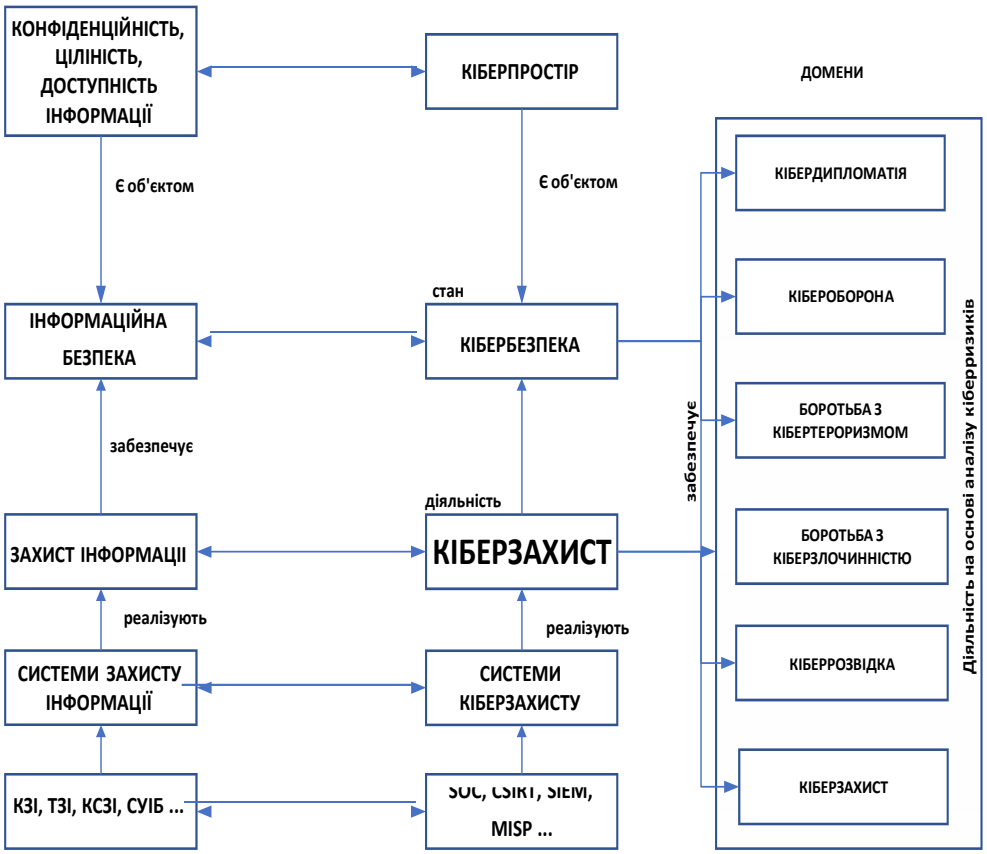


Рисунок 1.7 Місце та роль кіберзахисту у забезпеченні кібербезпеки

Видами діяльності у сфері кібербезпеки є: кібероборона, кіберзахист, протидія кібертероризму, кібершпигунству та кіберзлочинності, кіберрозвідка та кібердипломатія, а також координація діяльності за цими видами. Така діяльність спрямована на нейтралізацію різних видів джерел загроз і на захист людини, суспільства, держави, процесів та інформаційних технологій.

Ці види діяльності розподілені між складовими національної системи кібербезпеки, насамперед її ядра, яке утворюють основні суб'єкти національної системи кібербезпеки.

У законодавстві внаслідок його динамічного розвитку, перманентних структурних і функціональних змін сектору безпеки та оборони чітко не визначено інституалізаційну підсистему кіберзахисту системи кібербезпеки, її елементи, завдання та функції, порядки взаємодії. Винятком є

Держспецзв'язку, підпорядкований йому Державний центр кіберзахисту та Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA. Але ці суб'єкти теж потребують суттєвого коригування своєї структури, повноважень, цілей та пріоритетів діяльності з метою максимального наближення до інституційних вимог ЄС та НАТО, підвищення рівня ефективності та результативності публічної політики й управління у цій сфері.

Відповідно до Закону України [9] Держспецзв'язку забезпечує:

- ❖ формування та реалізацію державної політики щодо захисту в кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах;
- ❖ координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту;
- ❖ забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно- технічної моделі кіберзахисту;
- ❖ здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків;
- ❖ інформує про кіберзагрози та відповідні методи захисту від них;
- ❖ забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації);
- ❖ координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість;
- ❖ забезпечує функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA.

Графічне представлення ролі і місця Держспецзв’язку в загальній системі кібербезпеки представлено на Рисунку 1.8.

Рисунок 1.8 Роль і місце Держспецзв’язку в системі кібербезпеки

1.3.3 Аналіз кіберзагроз та заходи із захисту від них.

Найбільш поширеними способами здійснення кібератак в період карантину та воєнного часу вважається сніфер пакетів та IP-спуфінг, DoS і DDoS атаки, парольні атаки, атаки на рівні додатків типу логічних бомб і троянських коней, вірусні атаки й так звані ін’єкції.

1) Сніфер пакетів — програма, яка використовує мережний інтерфейс, функціонуючи в так званому нерозбірливому (promiscuousmode) режимі. Вона перехоплює мережний трафік, призначений для інших вузлів, та здійснює його подальший аналіз. Застосування програми дає змогу виявити паразитний,

вірусний і закільцьований трафік; виявити в мережі шкідливе та несанкціоноване ПЗ (мережні сканери, флудери, троянські програми тощо); перехопити будь-який призначений для користувача незашифрований, а іноді й зашифрований трафік із метою отримання паролівта іншої інформації; локалізувати несправність мережі або помилку конфігурації мережних агентів.

Щоб знизити загрозу сніфінгу пакетів, доцільно:

- застосовувати такі методи автентифікації, як одноразові паролі типу One-TimePasswords (OTP) і DTP. В інших випадках, наприклад у разі перехоплення електронної пошти, зазначені методи не ефективні;
- створити комутуючу інфраструктуру (у разі використання комутуючого Ethernet-протоколу це дозволить хакерам отримати доступ лише до трафіку, що надходить на порт, до якого вони під'єднані);
- установити антисніфери або ПЗ, яке розпізнає сніфер пакетів, наявний у певній мережі (антисніфери вимірюють час реагування хостів і визначають, чи не доводиться хостам обробляти зайвий трафік);
- створити систему криптографічного захисту. Це найбільш ефективний спосіб боротьби зі сніфером пакетів. Якщо канал зв'язку має криптографічний захист, то хакер перехоплює не повідомлення, а зашифрований текст (тобто незрозумілу послідовність бітів).

2) IP-спуфінг (spoof — обман, містифікація, підроблення) — вид хакерської атаки (рис.1.9), що передбачає використання чужої IP-адреси, тобто введення в оману системи безпеки (зловмисник, який перебуває всередині корпорації/установи або поза нею, видає себе за санкціонованого користувача). Часто застосовується як складова комплексної атаки. Типовий приклад — DDoS атака, для здійснення якої хакер розміщує відповідну програму за чужою IP-адресою, щоб приховати власну.

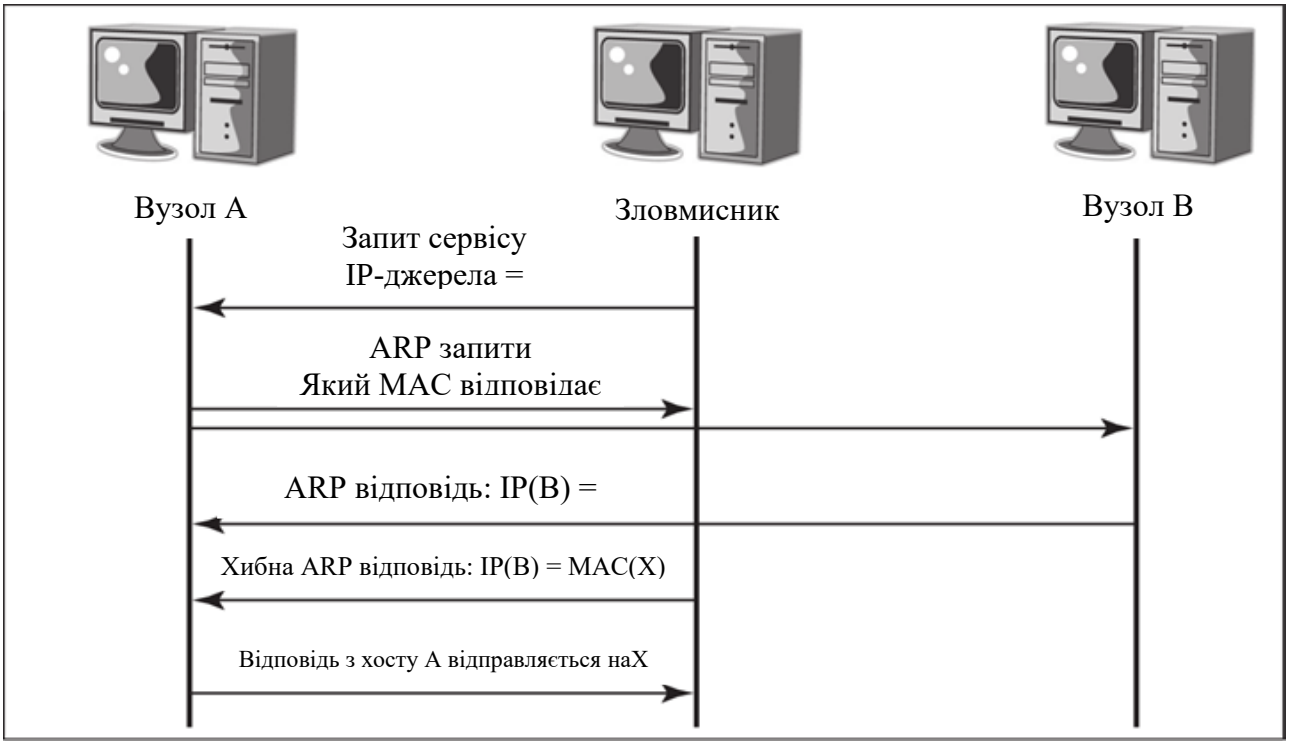


Рисунок 1.9 Застосування IP-спуфінгу для отримання несанкціонованого доступу до ресурсів

Послабити загрозу IP-спуфінгу, а кібератаку перетворити на абсолютно неефективну можна завдяки:

- правильному настроюванню управління доступом (із забороною будь-якого трафіку, що надходить із зовнішньої мережі з вихідною адресою, яка має перебувати всередині власної мережі);
- застосуванню фільтрації RFC 2827 (із забороною будь-якого трафіку, вихідна адреса якого не є однією з IP-адрес певної установи);
- упровадженню додаткових заходів автентифікації, таких як створення системи криптографічного захисту.

3) Відмова в обслуговуванні (DenialofService – DoS) — атака на комп'ютерну систему, що має на меті зробити комп'ютерні ресурси/мережу недоступними для користувачів через перевищення припустимих меж функціонування мережі, операційної системи або додатка; підвищення витрат ресурсів процесора та зменшення пропускної здатності і каналу зв'язку (рис. 1.10). До найвідоміших різновидів DoS атак належать такі: Flood, ICMP flood,

Identification flood, TCP SYN flood, Ping of Death, Tribe Flood Network, Trinco, Stacheldracht, Trinity.

Рисунок 1.10 Схема DoS атаки

На думку фахівців, особливо ефективна атака TCP SYN flood, що полягає в надсиланні надзвичайно великої кількості запитів на ініціалізацію TCP-з'єднань із вузлом-мішенню. Останньому через це доводиться витрачати всі свої ресурси на те, аби відстежувати ці частково відкриті з'єднання. Зазначена атака — найвідоміший спосіб переповнення інформаційного каналу SYN-пакетами, унаслідок якого сервер втрачає здатність відповідати на запити користувачів.

Розглянемо різновиди DoS атак:

Flood («затоплення») та ICMP flood (floodping — «потік пінгів») — це атаки, під час яких система отримує велику кількість ICMP- (найчастіше) або UDP-пакетів, які не несуть корисної інформації, і так званих ехозапитів ICMP (пінг системи). У результаті маємо зменшення перепускної смуги каналу, із завантаженням комп'ютерної системи непродуктивними діями щодо аналізу «сміття», яке надійшло, та генеруванням на нього відповідей (ICMP-пакети не аналізуються системою за замовчуванням, а відповіді на них не займають багато CPU-часу).

Identificationflood (запит ідентифікації системи) — атака, дуже схожа на ICMP flood. Відрізняється від неї тільки тим, що додатковою умовою її

проведенняє запит інформації про комп'ютерну систему (TCP порт 113). Оскільки аналіз цих запитів і генерування на них відповідей потребують більше процесорного часу, ніж у разі здійснення пінгів, то така атака вважається більш ефективною.

Ping ofDeath — атака, що призводить до зависання ОС, включаючи мишу й клавіатуру. Це, як правило, є відповіддю системи на надходження сильно фрагментованого ICMP-пакета великого (64 кбіт) обсягу. Сьогодні майже не використовується.

UDP flood (User DatagramProtocol) і TCP flood — атаки, полягають у відправленні на адресу системи-мішені безлічі пакетів UDP та TCP, що зрештою призводить до «зв'язування» мережних ресурсів. Нині ці атаки вважаються найменш небезпечними, оскільки їх легко виявити завдяки застосуванню при обміні пакетами головного контролера й агентів нешифрованих протоколів TCP і UDP.

Загрозу DoS атак можна послабити за допомогою:

- правильної конфігурації на маршрутизаторах і міжмережних екранах функцій антиспуфінгу (упровадження фільтрації RFC 2827) та функцій, спрямованих проти DoS;
- обмеження обсягу некритичного трафіку (non-criticaltraffic — визначає ймовірність того, що мережа зв'язку відповідає заданому та узгодженому трафіку), який проходить мережею. Типовим прикладом є обмеження обсягів трафіку ICMP, що використовується тільки з діагностичною метою.

4) Розподілена DDoS атака (DistributedDenialofService) — це підтип DoS атаки, здійснюваної одночасно з великої кількості IP-адрес (комп'ютерів) на систему об'єкта атаки, аби зробити мережу недоступною для звичайного використання (рис. 1.11).

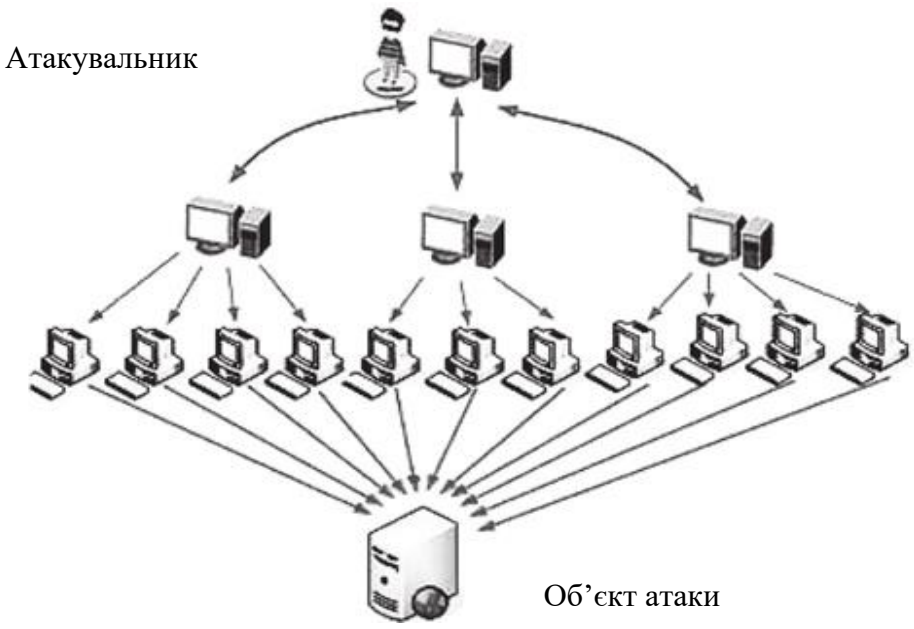


Рисунок 1.11 Схема DDoS атаки

Для цього створюються так звані ботнети (інакше бот-мережі, або зомбі-мережі) із групи заражених шкідливими програмами комп’ютерів, які одночасно надсилають запити до атакованого ресурсу, (рис.1.12). У результаті сервер не справляється з навантаженням, і доступ до атакованого ресурсу ускладнюється або взагалі стає неможливий.

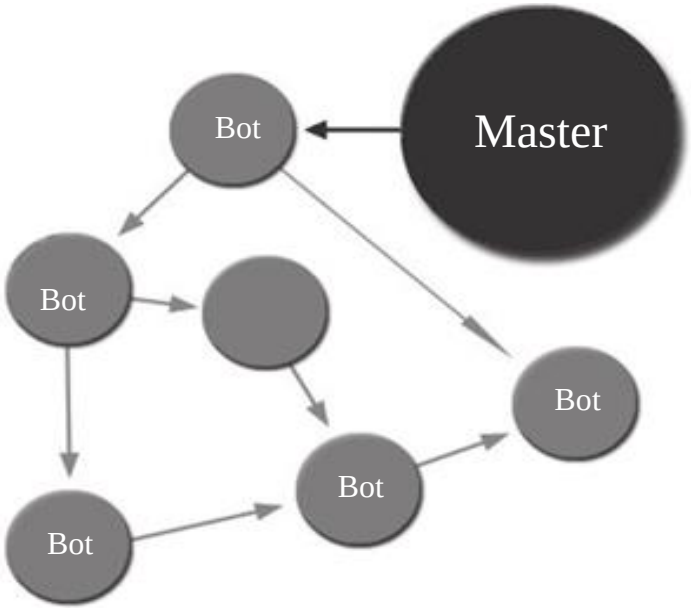


Рисунок 1.12 Загальна схема організації бот-мережі

Найбільш відомі різновиди DDoS атак такі: TCP SYN flood (рис. 1.13), TCP flood (рис. 1.14), SYN flooding, UDP flood, Smurfта ICMP floodатаки. При цьому найнебезпечніші ті програми, що використовують одночасно кілька видів описаних атак, наприклад TFN і TFN2K.

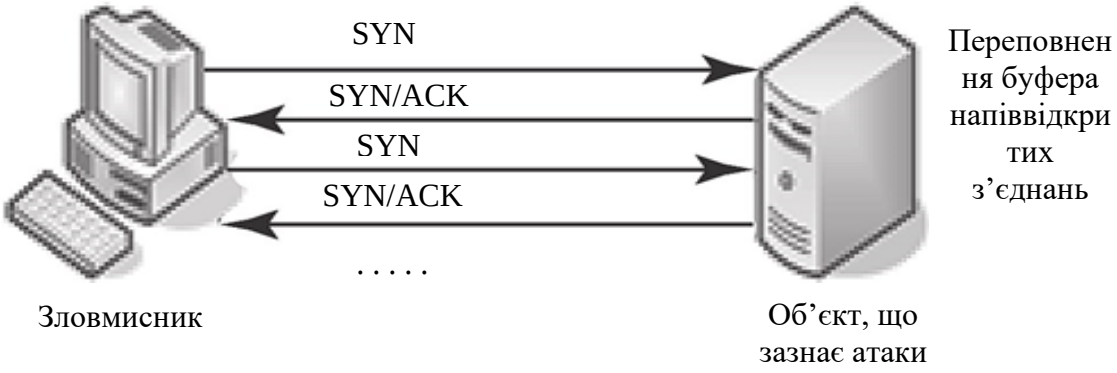


Рисунок 1.13 TCP SYN flood атаки

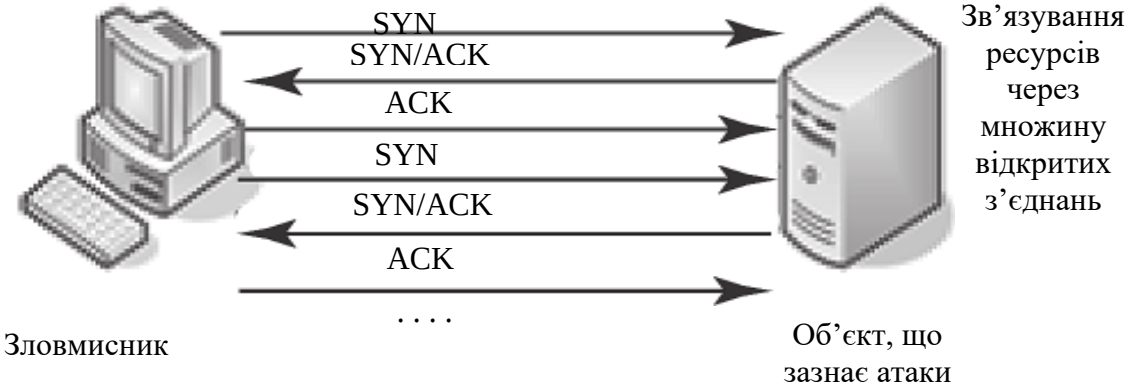


Рисунок 1.14 TCP flood атака

Одна з нових програм для організації DDoS атак — Stacheldracht — дозволяє здійснювати всілякі типи атак і генерувати лавини широкомовних пінгзапитів із шифруванням обміну даними між контролерами й агентами. Із погляду інформаційного захисту саме DDoS атаки становлять одну з найскладніших мережних загроз, а отже, пошук ефективних заходів протидіїїм — складне завдання, особливо, для організацій, діяльність яких безпосередньо пов'язана з інтернетом.

Протидія DDoS атакам передбачає:

❖ профілактику причин, що спонукають тих чи інших осіб організовувати DDoS атаки. Дуже часто атаки здійснюються внаслідок особистої образи або політичних, релігійних розбіжностей;

❖ розосередження або побудову розподілених і резервних систем, які не припинять обслуговувати користувачів, навіть якщо деякі їхні елементи стануть недоступні;

❖ фільтрацію трафіку на маршрутизаторах (міжмережні екрани та спеціалізовані antiflood засоби фільтрації — найбільш ефективний, але й найбільш дорогий метод. По змозі їх установлюють якнайближче до джерела flood. Наприклад, програмний засіб ADoS, який є динамічним фільтром TCP-пакетів, здатний блокувати в реальному часі доступ до web-сервера з IP-адрес, що генерують інтенсивний потік HTTP-запитів);

❖ розміщення (розташування) безпосередньої цілі атаки — доменного імені або IP-адреси подалі від інших ресурсів, які часто зазначають впливу разом із безпосередньою ціллю;

❖ нарощування ресурсів системи (якщо flood спрямований на вичерпання ресурсів, то найпримітивнішим способом протидії цьому є нарощування власних ресурсів, щоб протиборча сторона не змогла їх вичерпати).

1.3.4 Аналіз новітніх технологій кібербезпеки

1.3.4.1 Багатофакторна автентифікація (MFA)

Багатофакторна автентифікація (англ. multi-factorauthentication, MFA) підтверджує особу користувача шляхом використання двох або більше факторів, таких як код, маркер, PIN-код, біометричні дані або їх комбінація, перш ніж надати доступ до даних або системи.Для простої автентифікації потрібна одна частина даних, наприклад пароль. Багатофакторна

автентифікація використовує більше ніж один фактор для доступу до ресурсу для підвищення безпеки.

Враховуючи сучасний веб-світ і зростаючу кількість крадіжок даних, MFA є ключовим компонентом будь-якої системи безпеки для захисту приватної інформації користувача від несанкціонованого доступу.Сьогодні більшість облікових записів в Інтернеті, включаючи банківські облікові записи та облікові записи в соціальних мережах, а також такі гаджети, як телефони та ноутбуки, захищені MFA.

MFA додає додатковий рівень безпеки, вимагаючи доступу до одного з додаткових факторів, навіть якщо пароль користувача було зламано. Це означає, що навіть якщо хтось дізнається пароль користувача, йому все одно знадобиться доступ до одного з додаткових факторів, щоб отримати доступ.

Хакерам значно складніше отримати доступ до облікових записів, якщо використовується більше ніж один фактор автентифікації, оскільки їм потрібно знати багато частин інформації.MFA набирає популярності, особливо тому, що компанії переходять від використання стандартних паролів до більш надійних методів перевірки особи. Багатофакторна автентифікація (MFA) — це потужний інструмент для запобігання незаконному доступу до мереж і даних користувачів за допомогою кількох етапів перевірки особи.

MFA має важливе значення для захисту інформації користувачів у сучасних взаємопов’язаних мережах і зростаючій кількості випадків крадіжки даних. Це допоможе зменшити ризик крадіжки особистих даних, витоку даних та інших кібератак.

Приклад принципу дії MFA відображається на Рисунку 1.15, може застосовуватися у банківських платформах, що використовуюсь послуги MFA.

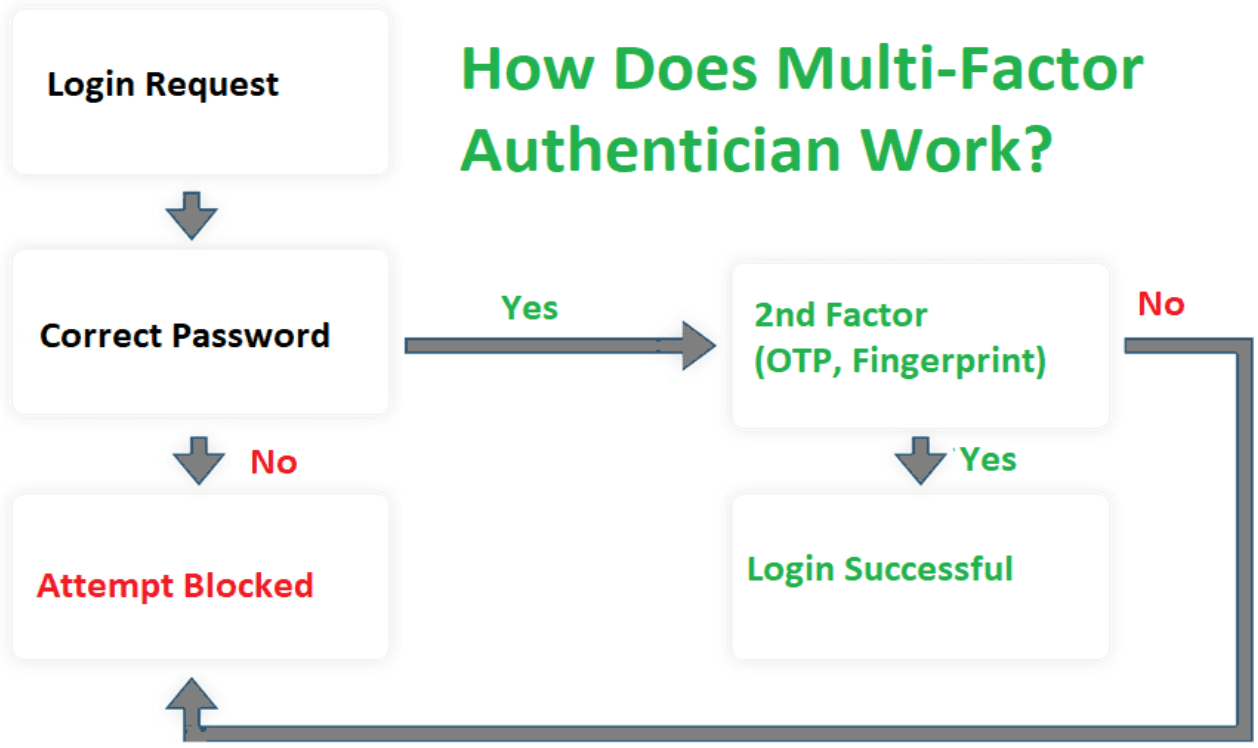


Рисунок 1.15 Приклад принципу дії MFA

Перш ніж надати комусь доступ до системи або облікового запису, захід безпеки під назвою MFA перевіряє особу людини за допомогою різних методів автентифікації. Це має на меті значно ускладнити зловмисникам доступ до конфіденційної інформації чи ресурсів.

MFA поєднує фізичний елемент, наприклад код, який надійшов на ваш телефон, із чимось, що ви знаєте, наприклад паролем. Він також може використовувати біометричні дані, такі як відбитки пальців, для встановлення особи.

Кінцеві користувачі зазвичай вводять своє ім'я користувача та пароль під час входу в обліковий запис за допомогою багатофакторної автентифікації. Після цього їх попросять підтвердити свою особу, зазвичай із кількома додатковими варіантами. Іншими альтернативами є одноразові паролі (OTP), надіслані через SMS, або коди, введені через програми автентифікації.

Також може бути використовувана програма автентифікації, щоб надіслати біометричну інформацію, наприклад відбиток пальця або сканування

обличчя. Деякі корпоративні фірми можуть вимагати від користувачів автентифікації за допомогою фізичного токена, наприклад ключа або картки.

1.3.4.2 Багаторівнева модель безпеки Zero Trust

Останні кілька років сучасний бізнес вийшов за межі офісів. Співробітники компаній отримують віддалені доступи до корпоративної інформації, часто використовують для цього особисті пристрої та працюють там, де є можливість підключатися до Wi-Fi. З одного боку, це розширює географію бізнесу, з іншого – ускладнює організацію комплексної безпеки компанії.

Сьогодні бізнесу потрібна багаторівнева модель безпеки, яка ефективно адаптується до нових умов роботи і забезпечує захист локальних та хмарних ресурсів. Вона вимагає суворої перевірки ідентичності для кожної людини та пристрою, які намагаються отримати доступ до корпоративної мережі.

Для своїх клієнтів Microsoft пропонує модель безпеки, яка базується на стратегії Zero Trust.Zero Trust – це модель безпеки, яка вимагає суворої перевірки ідентичності для кожної людини та пристрою, які намагаються отримати доступ до ресурсів у мережі, незалежно від того, чи знаходяться вони всередині або за межами периметра мережі.

Основний меседж Zero Trust: «Ніколи не довіряти, завжди перевіряти». Ця модель передбачає, що зловмисники є як всередині, так і за межами мережі, тому жодним користувачам чи пристроям не можна автоматично довіряти. Zero Trust перевіряє ідентичність та привілеї користувача, а також ідентифікацію та безпеку пристрою. Ця модель поєднує у собі політики, практики та технологічні інструменти, які працюють разом, щоб забезпечити компаніям більш надійний рівень безпеки, (рис 1.16).

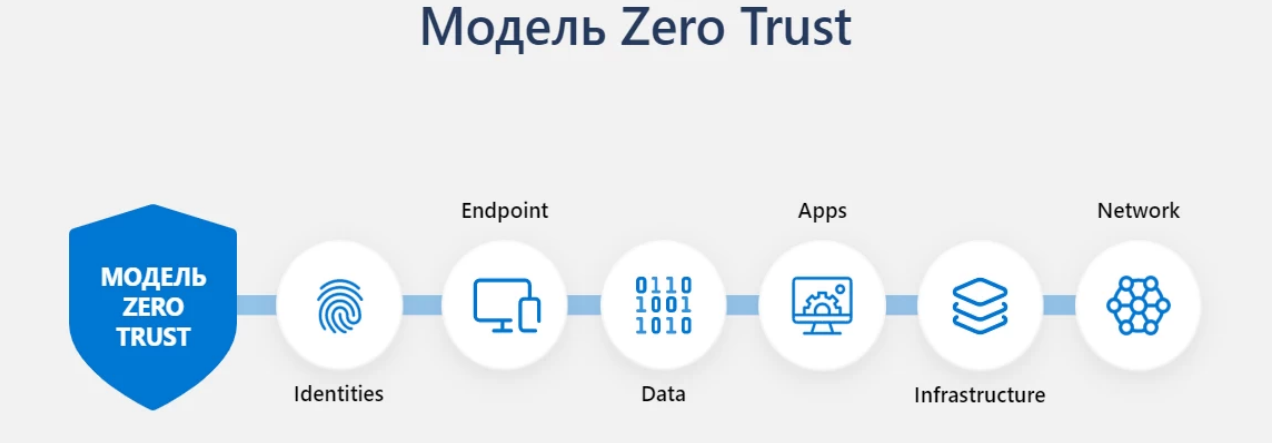


Рисунок 1.16 Модель Zero Trust

Області захисту моделі Zero Trust

- Identity

Організація перевірки та контролю ідентифікаційних даних користувачів із застосуванням суворої автентичності у всьому цифровому середовищі компанії.

- Endpoints

Контроль усіх пристроїв, які звертаються до інфраструктури компанії. Забезпечення перевірки стану та відповідності вимогам перед наданням доступу.

- Data

Перехід із захисту на основі периметра до системи безпеки на основі даних. Використання аналітики для класифікації та маркування даних. Організація шифрування та обмежень доступу з урахуванням політик компанії.

- Apps

Пошук тіньових IT у своєму середовищі, контроль прав та привілеїв усередині додатків, організація доступів на основі аналітики в режимі реального часу, відстеження та контролю прав користувачів.

- Infostructure

Використання засобів телеметрії, щоб виявляти атаки або аномалії та автоматичне блокування та маркування небезпечних дій; організація доступів з урахуванням мінімальних необхідних привілеїв.

- Network

Недовіра до пристроїв та користувачів на підставі того, що вони знаходяться всередині мережі компанії. Організація шифрування всіх каналів обміну даними та обмеження доступу на основі політик компанії.

Кожен із цих рівнів – важлива ланка в моделі нульової довіри. І кожен із них зловмисники або самі користувачі можуть використати як точки входу чи канали для витоку корпоративної інформації.

1.3.5 Розробка моделі кібербезпеки

Сучасні інформаційно-комунікаційні розробки привели людство в епоху цифрового кіберпростору. Плодами такої технологічної еволюції стали, як цифрові апаратні засоби, так і сервіси і додатки, що нам полюбилися. Комп'ютерні системи та портативні гаджети стали незамінною частиною нашого життя та принесли людству повсякденну користь. Їх застосування у різних сферах відкриває нові грані, але й таїть безліч небезпек. З'являється все більше інформації про фінансову шкоду компаній в секторі IT. Причиною проблем, що виникають, можуть стати системні помилки, людський фактор і навіть злочинна діяльність зловмисників. Політика підприємства щодо управління ризиками, відбиває надійність її і стійкість до різноманітних загроз. Співробітники або сторонні організації, які займаються сектором управління ризиками компанії, повинні правильно оцінювати загрози з розрахунку методів і засобів боротьби з ними, що є в наявності. Прозорість ситуації в усвідомленні своїх кібер-уразливостей може вплинути і на спільну роботу з іншими компаніями. Адже контролюючі органи та бізнес-партнери мають право вимагати інформацію про кібер-уразливості та пов'язані з ними ризики. Кібер-ризик зазвичай комплексна проблема, що включає не тільки IT складову бізнесу, а й організаційно-технічні аспекти виробництва. Ефективне управління ризиками у сфері інформаційних технологій має на увазі облік

кібер-ризиків ще на початковому етапі розробки бізнес-стратегії компанії і тому є фундаментальною ланкою будь-якого бізнес-проекту. Отже, фахівці з ризиків необхідні у всіх видах організацій будь-якої спрямованості. Їхнє завдання забезпечити безпеку корпоративних даних, контролювати кібер-загрози та ефективно боротися з результатами їх втілення в життя.

Кібер-загроза – це потенційно небезпечна подія, у разі реалізації якої порушується одна або кілька складових інформаційної безпеки (цілісність, доступність, конфіденційність), що може призвести до різнобічного збитку різного ступеня для об'єкта, що постраждав від події.

Реалізація подібної небезпечної події можлива в результаті:

- Умисних дій злочинців у напрямку складових інформаційної безпеки з метою отримання доступу до конфіденційних/критичних даних та подальшого використання цих даних у своїх цілях.
- Ненавмисних дій персоналу або техногенних причин, які можуть призвести до порушень складових інформаційної безпеки.

У процесі усвідомлення фундаментальних механізмів мінімізації ризиків слід звернути увагу, що людський чинник є основною причиною виникнення загроз. З іншого боку, не слід забувати, що співробітники є основним ресурсом трудової діяльності організації. Отже, робота з персоналом стає найважливішим пунктом у реалізації політики управління ризиками. Його можна розділити на сектор навчання та організаційні заходи щодо управління ризиками. Фінансові вкладення підвищення кваліфікації персоналу з питань кібер-ризиків може бути дуже корисними, оскільки в процесі навчання колективу, будуть впроваджуватися ази кібергігієни на робочому місці. В результаті навчений персонал буде ефективно інтегрований у стратегію управління ризиками компанії. Такий підхід до профілактики кіберпростору, що використовується, дозволяє організувати більш ефективну систему мінімізації кібер-ризиків підприємства.

Варто зазначити, що стандартні заходи безпеки, актуальні за будь-якого рівня підготовки персоналу, адже базові елементи захисту інформації підвладні навіть найдосвідченішим користувачам. Наприклад, копіювання важливих даних та хмарне зберігання інформації або встановлення антивірусної програми може підвищити кіберстійкість комп'ютерної системи. Необхідно розуміти, що від ступеня важливості інформації залежать заходи захисту. Організаційні заходи щодо управління ризиками визначають ступінь важливості інформаційних активів на кожному рівні доступу персоналу до корпоративних даних. Працівник кожної ланки на підприємстві повинен мати чітке уявлення про цінність даних, до яких має доступ. В результаті такого підходу більшість кіберпорушень можна буде припинити завдяки базовим заходам безпеки для різних рівнів доступу. Аналіз ризиків, пов'язаних із критичними даними підприємства, визначить додаткові заходи безпеки для максимального контролю уразливих систем.

Немає сумніву в користі базових заходів безпеки, проте завжди залишається ймовірність реалізації кібер-ризику у вигляді інциденту, що відбувся, чи це навмисні або випадкові подія. У разі вдалої кібератаки або витоку даних з іншої причини, в силу має набути протокол реагування на інциденти, завданням якого є мінімізація наслідків кіберінциденту. Відповідальні за управління ризиками компанії повинні бути впевнені, що їхні протоколи зможуть ефективно реагувати на інциденти з метою підтримки іміджу підприємства, а також мінімізації інтелектуальних та фінансових втрат як для клієнтів, так і для самого підприємства. Модель системи управління ризиками підприємства представлена на Рисунку 1.17.

Рисунок 1.17 Модель кібербезпеки

Кіберзагрози стали реаліями роботи будь-якої компанії і не лише у сфері ІТ. Вони вторглися в наше життя разом із технологічними благами, виступаючи в ролі ложки дьогтю в бочці меду. Невеликі підприємства та великі корпорації вже давно ведуть свій бізнес з огляду на кібер-ризики та їх можливі наслідки. Питання кібербезпеки вийшли на міжнародний рівень, наприклад ще 2013 року, було розроблено стратегію кібербезпеки Європейського Союзу. Отже всім підприємствам необхідно ретельно оцінювати свої кібер-ризики. За правильної стратегії планування підприємства можуть за допомогою простих елементів управління, убезпечити себе від більшості загроз, мінімізувати наслідки кібератак і використовувати технологічні блага без особливих побоювань за долю свого бізнесу.

1.3.6 Тренди кібербезпеки

Тенденції останніх років такі, що ефективну систему кібербезпеки на підприємстві неможливо побудувати без активного залучення до процесу не тільки керівника відділу IT-безпеки (ChiefInformationSecurityOfficer, CISO), (див.1.7) або директора з інформаційних технологій (ChiefInformationOfficer, CIO), а також без керівників різних IT-відділів, оскільки інформаційні технології проходять через всі сфери діяльності будь-якої сучасної компанії. При цьому основну відповідальність за забезпечення кіберзахисту несе, як правило, головний виконавчий директор (CEO), у підпорядкуванні якого вже знаходиться CISO, який керує ризиками та приймає рішення для їх запобігання.

Окреме тонке питання пов'язане з розрахунком бюджету на IT-безпеку. У кожному випадку результат буде дуже індивідуальним, але для орієнтування можна взяти міжнародні дані – як показує глобальна статистика, наприклад, підприємства групи G2000 інвестують у IT-безпеку близько 2,8% загального річного прибутку.

Зазначимо, що у кожному регіоні є свої особливості, пов'язані зі специфічними вимогами щодо забезпечення інформаційної безпеки. Так, в ЄС одним із головних трендів є прагнення до дотримання Загального регламенту захисту даних (GeneralDataProtectionRegulation, GDPR), що відбивається на загальній політиці роботи з даними.

Що стосується технологічної сторони питання, то сьогодні великі надії щодо підвищення ефективності боротьби з кіберзагрозами покладають на системи захисту зі штучним інтелектом (щоправда, цю ж ідею прагнуть використати і злочинці).

Окрема нова галузь – це інтернет речей. Тут ще багато потрібно зробити в плані вироблення загальних стандартів та підходів до забезпечення IT-

безпеки (яких сьогодні фактично немає). Але великі галузеві організації, усвідомлюючи нагальну необхідність, активно працюють у цьому напрямі.

Ще однією важливою тенденцією є дедалі більша складність кіберзахисту, тому все частіше це завдання делегується профільним компаніям за принципом аутсорсингу.

3 ОХОРОНА ПРАЦІ

Закон України «Про охорону праці» визначає основні положення по охороні праці і регулює взаємини між працівниками і адміністрацією. В Україні законодавство по охороні праці складається із Закона України «Про охорону праці», Кодексу законів про працю і інших нормативних актів.

Широке впровадження комп'ютерної техніки, що дозволяє автоматизувати багато рутинних операцій, дістати доступ до численних джерел інформації істотно підвищує продуктивність праці користувачів відеотерміналу електронно-обчислювальної машини (ВДТ ЕОМ).

В дипломному проекті проводиться дослідження аналізу новітніх технологій кібербезпеки в період пандемії covid-19 та воєнного часу. Тому даному розділі дипломного проекту розглядається питання охорони праці програміста.

1.Аналіз небезпечних і шкідливих факторів, що впливають на програміста при розробці даного програмного комплексу

Програміст як і користувач персонального комп’ютера випробовує значне навантаження, як фізичне (сидяче положення, навантаження на очі), так і розумове, що приводить до зниження його працездатності до кінця робочого дня.

На робочому місці під час роботи програміст піддається впливу наступних несприятливих факторів:

- недостатнє освітлення;
- шум від працюючих машин;
- електромагнітне випромінювання;
- виділення надлишків теплоти.

Тому необхідно розробити засоби захисту від цих шкідливих факторів

2 Гігієнічні вимоги до виробничого середовища.

2.1 Вимоги до приміщення

Приміщення в яких планується установка та подальша робота з комп'ютером, повинні відповідати проектній документації будинку, погодженій з державними органами. Крім того, роботодавець повинен враховувати санітарні нормативи.

Об'ємно-планувальні рішення будівель та приміщень для роботи з ВДТ мають відповідати вимогам ДСанПІН 3.3.2.007-98. Розміщення робочих місць з ВДТ ЕОМ і ПЕОМ у підвальних приміщеннях, на цокольних поверхах заборонено. Для уникнення можливих аварій та замикань, поряд з приміщеннями, де вестиметься робота з комп'ютером (над чи під ними), також не дозволяється проведення робіт, що потребують здійснення надмірно вологих технологічних процесів. Приміщення укомплектоване системами центрального опалення Площа на одне робоче місце становить не менше 6,0 $м^2$, а об'єм – не менше ніж 20,0 $м^3$. У приміщеннях слід щоденно робити вологе прибирання. Вони повинні бути оснащені аптечками першої медичної допомоги.

2.2 Мікроклімат

У наслідок досліджень про взаємодію користувачів комп'ютерів з мікрокліматичними умовами на робочих місцях, а вірніше з повітряним середовищем виробничих приміщень, спостерігається низка фізичних відхилень організму, це пов'язано з наступними небезпечними факторами:

1. Збільшення концентрації: позитивних іонів, аерозолів, мікробних тіл в повітрі приміщень з ВДТ.

2. Перевищення температури повітря що спричиняє висихання слизових оболонок, їх пересихання і розтріскування;

3. забруднень хвороботворними мікробами на комп'ютеризованих робочих місцях в теплий період року, що спричиняє до зміни терморегуляції робітників і зниження працездатності.

4. Відносна вологість повітря часто є нижче за встановлені норми.

Для забезпечення оптимальних мікрокліматичних умов в будь-який період року для приміщень в яких розташовані комп'ютеризовані робочі місця повинно бути виконано:опалювання і приміщеннях, кондиціонування повітря (найпоширеніші способи нормалізації мікроклімату) ;

- раціоналізація режимів праці і відпочинку (досягається скороченням тривалості робочого часу за рахунок додаткових перерв, створенням умов для ефективного відпочинку в приміщеннях з нормальними метеорологічними умовами);
- теплоізоляція обладнання і захисних екранів (як теплоізоляційні матеріали широко використовують: азбест, азбоцемент, мінеральну вату, склотканина , керамзит, пінопласт);
- для підтримки допустимих значень мікроклімату і концентрації позитивних і негативних іонів необхідно передбачити установки або прилади зволоження та / або штучної іонізації, кондиціонування повітря.

У виробничих приміщеннях на робочих місцях мають забезпечуватись оптимальні значення параметрів мікроклімату: температури, відносної вологості й рухливості повітря – ГОСТ 12.1.005-88, СН 4088-86.

Параметри мікроклімату	Значення параметрі	значення параметрі
	Взимку	влітку
Температура, C^0	22-24	23-25
Відносна вологість, %	40-60	40-60
Швидкість руху повітря, м/с	0,1	0,1-0,2

2.3 Освітлення

Щоб програміст легко виконував поставлені перед ним завдання, важливо, щоб на його місце попадало досить світла. При слабкій освітленості

очі втомлюються швидше, увага слабшає. Якщо освітлення занадто яскраве, воно буде зліпити і провокувати різь в очах, стане причиною дратівливості.

Освітлення приміщення має природне та штучне походження. Природне освітлення подається через віконні прорізі, бокове. Для штучного освітлення у приміщенні використовуються люмінесцентні лампи, які в порівнянні з лампами розжарювання мають ряд істотних переваг. Так за спектральним складом світла вони близькі до природного світла, мають підвищену світлову віддачу, триваліший термін служби. Норма освітленості на робочих місцях складає 300-500лк.

2.4 Вимоги до організації робочого місця працівника

Основний меблями робочого місця програміста є крісло і стіл. У крісла повинна бути трохи увігнута поверхня і незначний нахил спинки назад. Його висота повинна бути змінена, а вся конструкція не повинна заважати свободі рухів корпусу і рук. Бажано, щоб у крісла були підлокітники.

Стіл повинен мати відповідну для конкретної людини висоту, а його нижня частина повинна бути такої конструкції, щоб не вимагалося підтискати ноги. На поверхні столу не повинні з’являтися відблиски, які завадять нормально бачити інформацію на дисплеї. Оптимальні розміри столу – це довжина 1300 мм і ширина 650 мм, а також висота 710 мм і глибина мінімум 400 мм.

2.5 Електробезпека

Ураження струмом може виникнути при роботі під напругою і при несправному стані електроустановок, а саме при дотику до оголених проводів, незаземлених металевих корпусах електричного обладнання, при відкритих рубильниках і других струмоведучих частинах.

Для захисту працюючих від ураження електричним струмом передбачені наступні заходи:

- недоступність струмоведучих частин;
- захисне заземлення (занулення) корпусів електрообладнання;

- передбачені рубильники закритого типу;
- блокіровка, надписи, плакати, засоби індивідуального захисту (калоші і боти діелектричні (ГОСТ 13385-78), рукавиці резинові діелектричні, коврики резинові діелектричні (ГОСТ 4997-75).

Заземлені конструкції, що знаходяться в приміщеннях, де розміщені робочі місця операторів (батареї опалення, водопровідні труби, кабелі із заземленим відкритим екраном) мають бути надійно захищені діелектричними щитками або сітками з метою недопущення потрапляння працівника під напругу.

У приміщенні, де одночасно експлуатуються понад п’ять ЕОМ, на помітному та доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітленнянедоступність струмоведучих частин;

3 Пожежна безпека

Протипожежний захист приміщення забезпечується застосуванням автоматичної установки пожежної сигналізації, наявністю засобів пожежогасіння, застосуванням основних будівельних конструкцій будинку з регламентованими межами вогнестійкості, організацією своєчасної евакуації людей.

Для ліквідації пожеж використовують первинні засоби пожежогасіння, які призначенні для гасіння пожеж у початковій стадії їх розвитку. Вони є у всіх виробничих приміщеннях, цехах.

Необхідну кількість первинних засобів пожежогасіння визначають окремо для кожного поверху та приміщення. Якщо в одному приміщенні знаходяться декілька різних за пожежною небезпекою виробництв, не відділених одне від одного протипожежними стінами, усі ці приміщення забезпечують вогнегасниками, пожежним інвентарем та іншими видами засобів пожежогасіння за нормами найбільш небезпечного виробництва.

Пожежні щити (стенди) встановлюють на території об’єкта з розрахунку один щит (стенд) на площу 5000м^2. До комплекту засобів пожежогасіння, які розміщуються на ньому, слід включати: вогнегасники – 3шт., ящик з піском – 1шт., покривало з негорючого теплоізоляційного матеріалу або повсті розміром 2м х 2м– 1шт., гаки – 3шт., лопати – 2шт., ломи – 2шт., сокири – 2шт.

Ящики для піску повинні мати місткість 0.5, 1.0 або 3.0м^2 та бути укомплектованими совковою лопатою. Вмістилище для піску, що є елементом конструкції пожежного стенду, повинні бути місткістю не менше 0.1м^3. Конструкція ящика (вмістилище) повинна забезпечувати зручність діставання піску та усування попадання опадів.

ВИСНОВКИ

Війна в Україні викликає зростання занепокоєння щодо інцидентів кібербезпеки та стійкості критичних бізнес функцій та послуг. Хоча ситуація сьогодні доволі непередбачувана, потрібно постійно аналізувати, як вона може розвиватися далі, та які сценарії можуть виникнути. Для кожного сценарію потрібно оцініть вплив на організацію з огляду на людей, бізнес, ланцюги поставок і технології.

До 2025 року глобальні збитки від кіберзлочинності досягнуть 10,5 трильйона доларів на рік. Якби сума була порівнянна з економікою країни, то кіберзлочинність, яка, за прогнозами, завдасть збитків на загальну суму 8 трильйонів доларів у 2023 році, була б третьою за величиною економікою у світі після США та Китаю. Програми-здирники щільно влаштувалися в заголовках новин. Частка спричинених ними порушень минулого року зросла на 41%. Програмам-вимагачам потрібно було в середньому 277 днів – близько 9 місяців – для виявлення та стримування порушення. Середня вартість шкідливої програми зросла до 4,54 мільйонів доларів. 32% жертв платять викуп, але отримують лише 65% своїх даних назад. Лише 57% компаній успішно відновлюють дані за допомогою резервних копій. Очікується, що загальне глобальне сховище даних перевищить 200 зеттабайт до 2025 року. Це включає дані, що зберігаються на приватних і публічних IT-інфраструктурах, в приватних і публічних хмарних центрах обробки даних, на персональних обчислювальних пристроях - ПК, ноутбуках, планшетах і смартфонах - і на пристроях IoT (Інтернет речей). Рідко суб'єкти загроз чекають на новий рік, щоб раптово розкрити новий вид атаки, кардинально змінити тактику або змінити свої цілі. Загрози розвиваються повільно і адаптуються до контролю безпеки, що постійно покращується. Але ми можемо робити деякі висновки, ґрунтуючись на статистиці та спостерігаючи за розвитком нових шкідливих програм та методів хакерських угруповань.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Шемчук В. В. Основні напрямки міжнародного співробітництва у сфері кібербезпеки. Вчені записки. Серія : Юридичні науки. Кримінальне право та кримінологія ; кримінально-виконавче право. 2018. Т. 29(68) № 2. С. 125–129.

2. Дешко Л. М., Бонарєва К. Д. Кібербезпека в Україні і Національна стратегія та міжнародне співробітництво. Порівняльно-аналітичне право. 2018. № 2. URL : http://pap.in.ua/2_2018/112.pdf.

3. Піскорська Г. А., Яковенко Н. Л. Сучасні виклики і загрози в кіберпросторі : формування механізму міжнародної інформаційноїбезпеки. International relations, part «Political science». No 18–19(2). URL : https://cutt.ly/GQCBYfV.

4. Доронін І. М. Організація звітування суб'єктів кібербезпеки. Актуальні проблеми управління інформаційною безпекою держави : зб. тез наук. доп. наук.-практ. конф. Київ : Нац. акад. СБУ, 2019. URL : https://cutt.ly/5QCBPIq.

5. Забара І. М. Кібернетична безпека держави в умовах розвитку штучного інтелекту : до питання визначення напрямків міжнародно-правового регулювання. Актуальні проблеми управління інформаційною безпекою держави : зб. тез наук. доп. наук.-практ. конф. Київ : Нац. акад. СБУ, 2019. URL : http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf.

6. Кравець В. М. Порівняльний аналіз міжнародних індексів кібербезпеки. Актуальні проблеми управління інформаційною безпекою держави : зб. тез наук. доп. наук.-практ. конф. Київ : Нац. акад. СБУ, 2019. URL : http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf.

7. Нікітіна Є. О., Тимофєєв Д. С. Інструменти проактивного аналізу кіберзагроз. Актуальні проблеми управління інформаційною безпекою держави

: зб. тез наук. доп. наук.-практ. конф. Київ : Нац. акад. СБУ, 2019. URL : http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf.

8. Вдовенко С. Г., Даник Ю Г., Пермяков О. Ю, Досвід розвитку систем кібербезпеки та кібероборони провідних країн світу. Modern Information Technologies in the Sphere of Security and Defence. 2019. № 3(36) URL : http://sit.nuou.org.ua/article/view/202623/202526.

9. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163. URL : https://zakon.rada.gov.ua/laws/show/2163- 19.

10. Мохор В. В., Богданов А. М., Килевой А. С. Наставления по кибербезопасности. Киев : Три-К, 2013. 63 с.

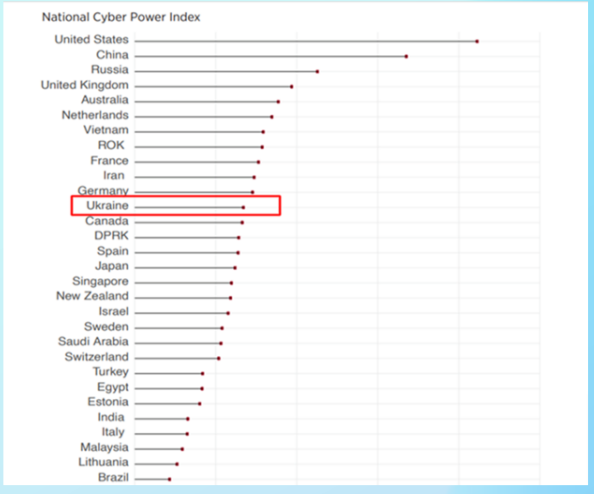
ДОДАТОК Б

Слайди мультимедійної презентації

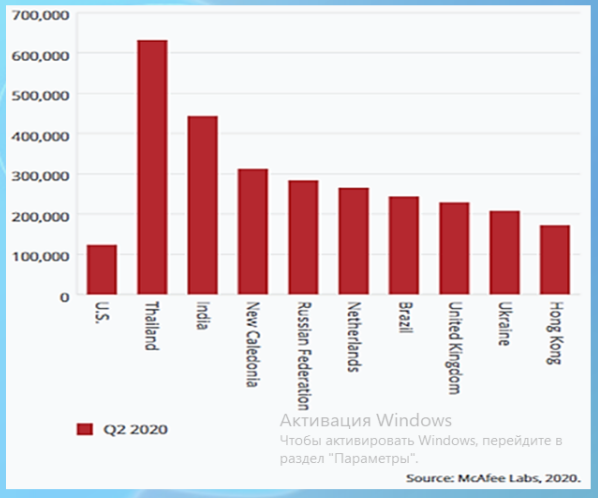
Профілі навичок у кібербезпеці

Головний спеціаліст з інформаційної безпеки
Реагувальник на кіберінциденти
Спеціаліст з питань кібер-юриспруденції, політики та відповідності
Спеціаліст з розвідки кіберзагроз
Архітектор з кібербезпеки
Аудитор з кібербезпеки
Реалізатор кібербезпеки
Дослідник кібербезпеки
Менеджер ризиків кібербезпеки
Цифровий слідчий-криміналіст
Тестер проникнення

Топ-30 найпотужніших кібердержав світу



Інциденти безпеки



Роль і місце Держспецзв'язку в системі кібербезпеки

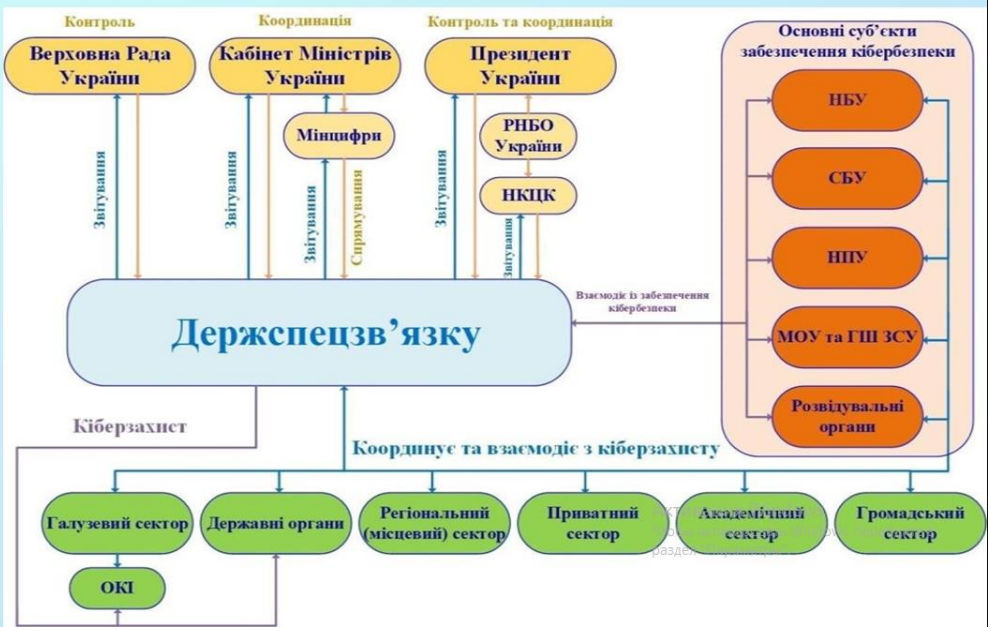
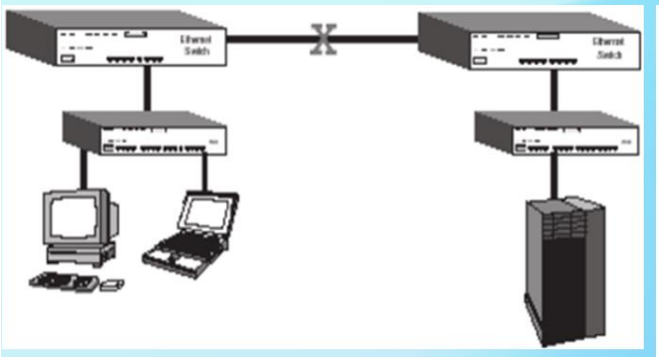
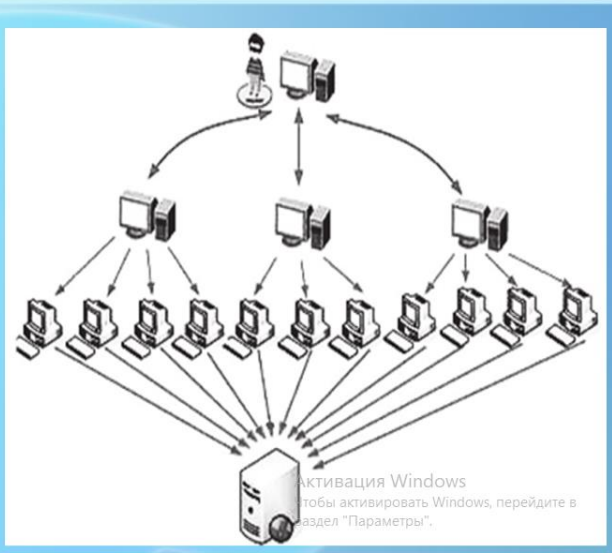
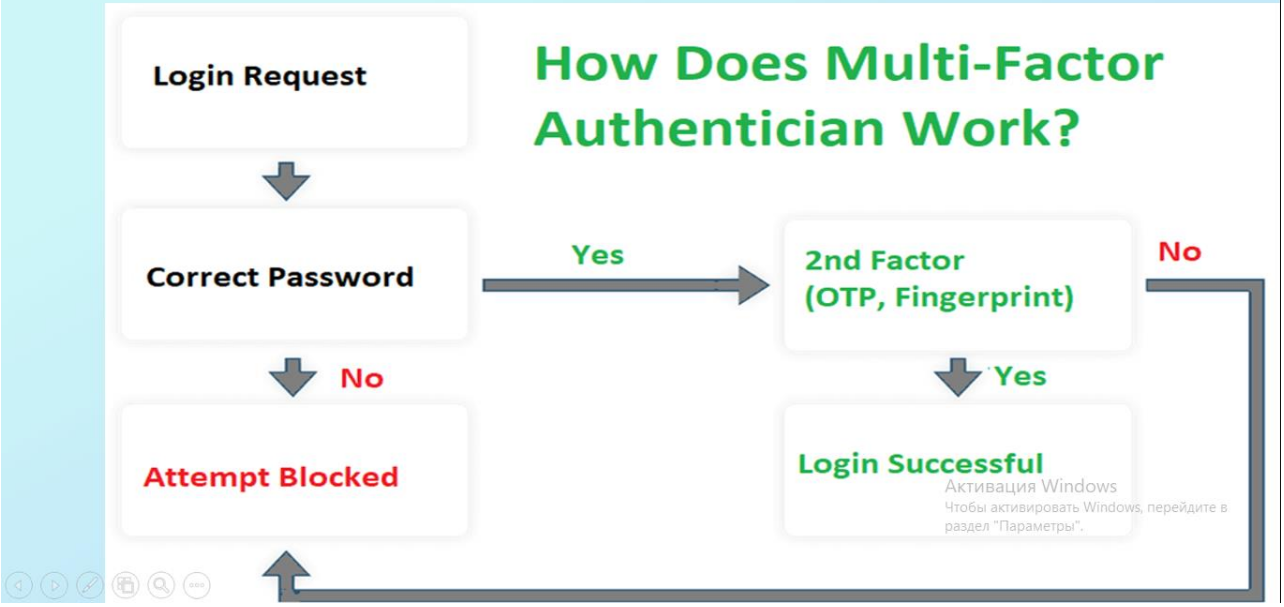


Схема DoS та DDoS атаки

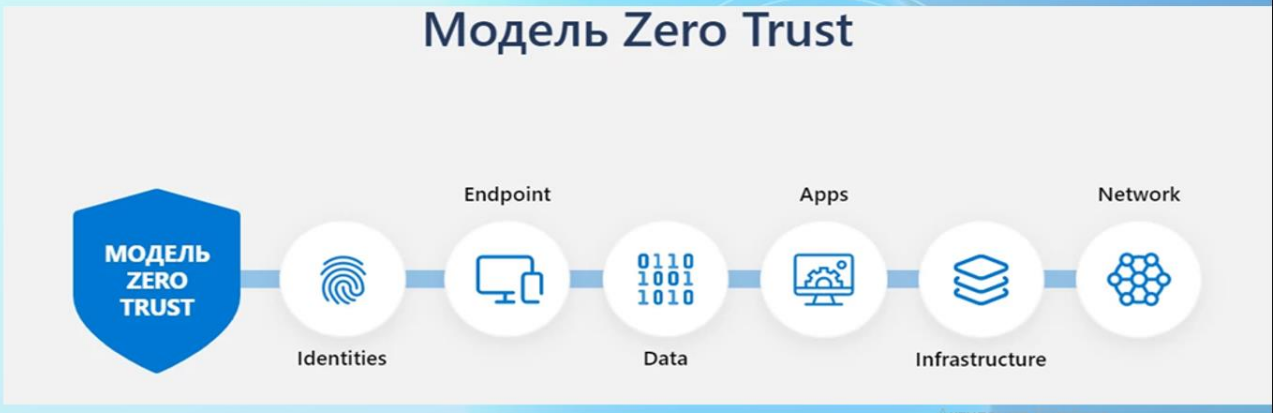




Багатофакторна автентифікація (MFA)



Багаторівнева модель безпеки Zero Trust



Модель кібербезпеки підприємства

UNICHECK

Ім'я користувача:
Наталія Вікторівна Копусь

ID перевірки:
1015591776

Дата перевірки:
13.06.2023 21:05:45 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
13.06.2023 21:06:37 EEST

ID користувача:
100011688

Назва документа: 2БКС-27 Аверін В.М

Кількість сторінок: 47 Кількість слів: 8041 Кількість символів: 63588 Розмір файлу: 1,009.56 KB ID файлу: 1015240935

45.5%
Схожість

Найбільша схожість: 14.2% з Інтернет-джерелом (https://kpmg.com/ua/uk/blogs/home/posts/2022/4/pytannya-kiberbe...

45.5% Джерела з Інтернету | 570 ..... Сторінка 49

Не знайдено джерел з Бібліотеки

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи | 3

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на випускну роботу бакалавра здобувача освіти

відділення комп'ютерних систем

Аверіна Володимира Михайловича

(прізвище, ім`я та по батькові)

Спеціальність **123 «Комп'ютерна інженерія»**

Освітня програма **Обслуговування комп'ютерних систем та мереж**

Керівник дипломного проекту (роботи) **Шевцов Юрій Сергійович**

(прізвище, ім`я та по батькові)

Тема дипломного проекту (роботи)

Аналіз новітніх технологій кібербезпеки в період пандемії covid-19 та воєнного часу

Обсяг розрахунково-пояснювальної записки 72 сторінок

Обсяг графічної (презентаційної) частини 12 аркушів (слайдів)

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ (РОБОТИ)

а) заключення про ступінь відповідності виконаного дипломного проекту (роботи) завданню

Дипломний проект повністю відповідає завданню до дипломного проектування. Графічна частина складається з окремих слайдів, оформлених у вигляді презентації, передбачених технічним завданням. Якість виконання пояснювальної записки та слайдів добра.

б) характеристика виконання кожного розділу дипломного проекту (роботи)

Пояснювальна записка дипломного проекту виконана якісно, у повному обсязі. В дипломному проекті здобувачем проаналізовано новітні технологій кібербезпеки в період пандемії covid-19 та воєнного часу. Розроблено модель кібербезпеки. В дипломному проекті в останніх розділах проаналізовано економічні показники та питання охорони праці.

в) оцінка якості виконання пояснювальної записки та графічної частини дипломного проекту (роботи) _____

Презентаційні матеріали виконані якісно, демонстративно та відповідають вмісту теоретичного матеріалу

г) перелік позитивних якостей дипломного проекту (роботи)_____

Здобувачем проаналізовані новітні технологій кібербезпеки в період пандемії covid-19 та воєнного часу, що є дуже актуальною тематикою в наш час. Розроблено модель кібербезпеки згідно до завдання на випускну роботу.

д) основні недоліки дипломного проекту (роботи) _____

Присутні помилки оформлення і орфографічні помилки в тексті пояснювальної записки;
Наведено багато зайвої теоретичної інформації

Оцінка розрахункової частини _____ *Добре*

Оцінка графічної частини _____ *Добре*

Загальна оцінка _____ *Добре*

Прізвище, ім'я, по батькові рецензента _____ *Василіу Євген Вікторович*

Місце роботи і посада рецензента *Державний університет інтелектуальних технологій і зв'язку, д.т.н., проф. кафедри КБ та ТЗІ, декан факультету інформаційних технологій та кібербезпеки*

Підпис: _____

«16» 06 2023 р.

ПІДПИС ПОСВІДЧУЮ
НАЧАЛЬНИК ВІДДІЛУ КАДРІВ ДУІТЗ _____ Котіка

ВІДДІЛ КАДРІВ

ВСП «Одеський технічний фаховий коледж ОНТУ»

ВІДГУК

керівника про випускну роботу бакалавра

Аверіна Володимира Михайловича

(прізвище, ім`я та по батькові)

Спеціальність 123 "Комп'ютерна інженерія"

Тема випускної роботи Аналіз новітніх технологій кібербезпеки в період пандемії covid-19 та воєнного часу

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ (РОБОТИ)

а) Обсяг і якість виконання роботи (графічного матеріалу і розрахунково-пояснювальної записки) Випускна робота виконана відповідно технічному завданню. Пояснювальна записка до випускної роботи містить 72 сторінки. У пояснювальній записці зроблено аналіз новітніх технологій кібербезпеки в період пандемії covid-19 та воєнного часу. Розроблено модель кібербезпеки. Графічна частина складається з 12 слайдів, оформлених у вигляді презентації, передбачених технічним завданням. Якість виконання пояснювальної записки та слайдів добра, розробку виконано у повному обсязі.

б) Самостійність роботи

Протягом виконання випускної бакалаврської роботи Аверін В. М. поступово та послідовно виконував всі етапи, проявив ініціативу у створенні загальної концепції та реалізації випускної роботи. Всі роботи він виконував самостійно, з оглядом на рекомендації керівника.

в) Теоретична підготовка здобувача освіти

Аверін В. М. під час роботи над випускною бакалаврською роботою вивчив достатню кількість літературних джерел за даною тематикою.

Вважаю, що теоретична підготовка здобувача освіти добра і він готовий до захисту роботи.

г) Вміння розв`язувати виробничі і конструкторські питання на базі останніх досліджень науки і техніки, передових методів виробництва

Під час виконання роботи Аверін В. М. мав змогу самостійно приймати окремі рішення з виконання програмної частини роботи та показав вміння організовано працювати над поставленою задачею, користуючись сучасними комп'ютерними програмними засобами.

Оцінка розрахункової частини Добре

Оцінка графічної частини Відмінно

Загальна оцінка Відмінно

Прізвище, ім`я, по батькові Харченко Роман Юрійович к.т.н.

Місце роботи і посада керівника роботи

доцент каф. "Морського радіозв'язку" НУ «Одеська Морська академія»

Підпис

«12» 06 2023 р.

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Аверін Володимир Михайлович,
здобувач освіти гр. 4ФКГ-06, та

Харченко Роман Юрійович,
керівник дипломного проекту,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до випускної кваліфікаційної роботи бакалавра на тему:

«Аналіз новітніх технологій кібербезпеки в період пандемії covid-19 та воєнного часу»
(автор роботи – Аверін В. М., керівник роботи – Харченко Р.Ю.)

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2023 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи, і даємо згоду на обробку персональних даних.

Виконавець _____ / Аверін В. М./

Керівник _____ / Харченко Р.Ю./

« 12 » _____06_____ 2023 р.