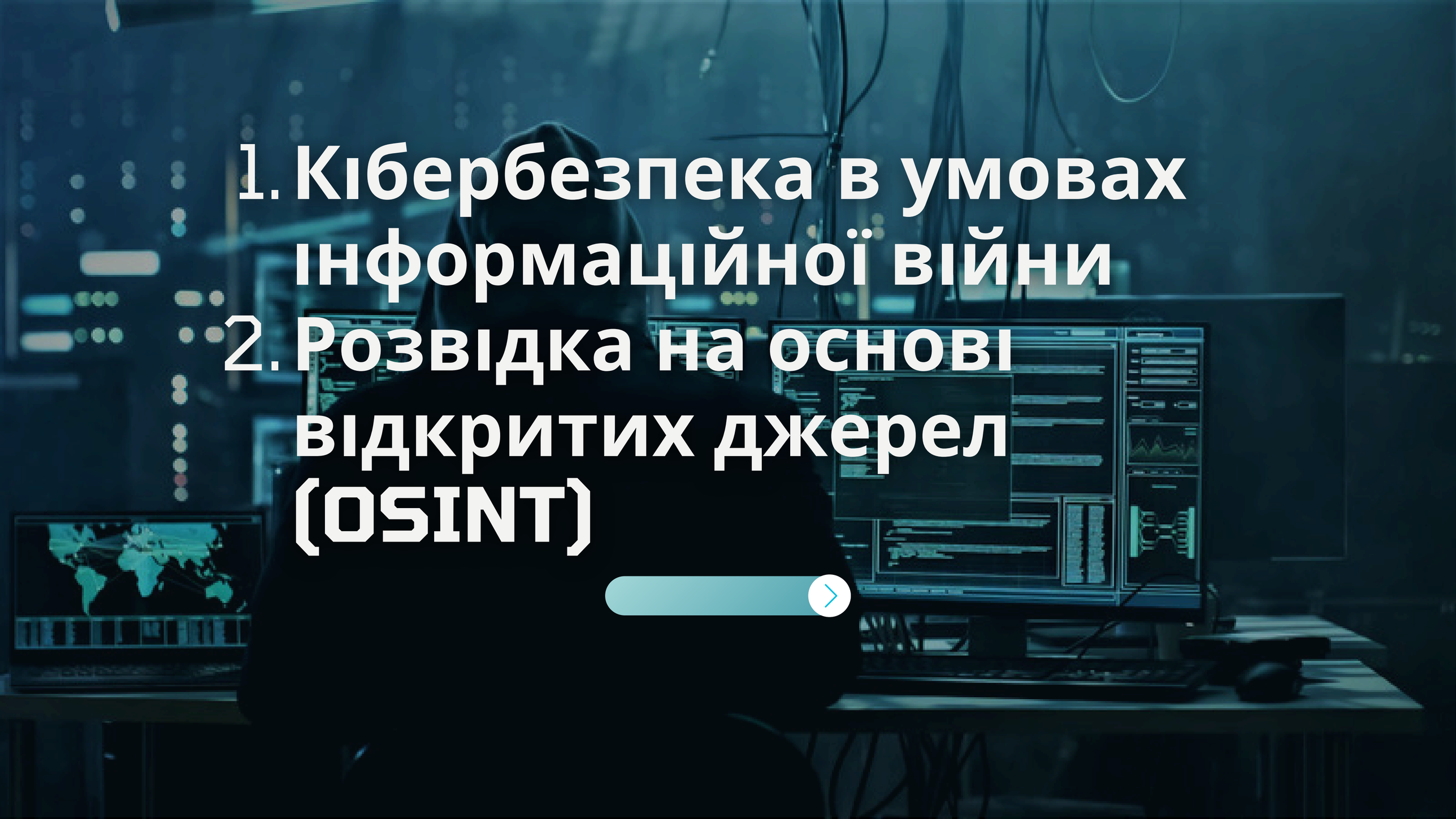


1. Кібербезпека в умовах інформаційної війни
2. Розвідка на основі відкритих джерел (OSINT)

Мета заняття:

ознайомитись з поняттям кібербезпека та основними засадами кібергігієни.

дізнатися про можливості кібератак, цілі та завдання кібервоєн

вивчити приклади успішних кібератак між країнами

ознайомитися з головними подіями історії протистоянь в кіберпросторі України і росії

вивчити головні поради для захисту приватних облікових записів від кібершахрайства

План

1. Кібербезпека людини та держави
2. Ефективність кібервтручання в діяльність систем супротивника
3. російсько-українська кібервійна
4. Основні рекомендації для кібергігієни

Сьогодні людство повністю залежить від інформаційних технологій. Напружені війни проводяться в кіберпросторі як державами, так і окремими групами, що створює великий прибуток для ініціаторів кібератак.

Головна умова для нападу – це цілковита анонімність агресора.

Для війн такого роду визначальною є

- технічна перевага
- розвиток технологій (де-)шифрування
- рівень комп'ютерних спеціалістів.

Через кібератаки та боротьбу з їхніми наслідками бізнес щорічно втрачає 400 мільярдів доларів.

1 Кібербезпека людини та держави

Кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору. Це стан захищеності систем передавання, опрацювання та зберігання даних, у якому забезпечено конфіденційність, доступність і цілісність даних.

Кіберзахист – це постійний процес захисту *даних* від знищення, копіювання, зміни, використання; а також *приладів і систем* – від будь-якого стороннього впливу, тому неможливо створити систему, захист якої не можна буде зламати.
Головне завдання: створення такого механізму захисту, вартість зламу якого буде дорожчою за інформацію, яку можна отримати.

Цілі кібервійни не відрізняються від цілей традиційних протистоянь:

- здійснення впливу на об’єкт
- зміна поведінки супротивника та
- встановлення над ним своєї влади.

Різниця лише у ***методах***

Окрім того, кібервійна має свої особливості:

1

1. Впливає на інформаційні потоки, на техніку, на системи.
Вона може спрямовувати, фальсифікувати або перешкоджати потокам інформації для впливу на думку суспільства, державних чиновників або військових.

2

2. Атаки на критичну інфраструктуру (електроенергетичні мережі, транспортні системи, фінансові установи, зв’язок тощо).
Це призводить або до паралізування управління державою, або впливає на життя громадян і може змусити виконувати вимоги агресора.

3

Включає кібершпигунство та кібершантаж. Збір конфіденційної (зокрема, економічної) інформації про супротивника та подальший шантаж.

4

4. Проведення дестабілізації та психологічного тиску. Суспільство настільки залежне від комп’ютерних інформаційних технологій, що їх порушення створює небезпеку для життя та здоров’я, створює справжній хаос.

Безпосередніми цілями атак зловмисників та ворогів стають:

комунікаційні системи, в яких обробляються національні інформаційні ресурси та які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань

комунікаційні системи, які використовуються для забезпечення суспільних потреб та реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу (енергетика, зв’язок, залізниця, банківська система тощо)

об’єкти критичної інформаційної інфраструктури

«***Кіберзброя»,*** яка застосовується в атаках − це відповідні інструменти, технології або методи, які використовуються в кіберпросторі для здійснення кібератак, кібервійськових операцій або впливу на інформаційні системи та мережі.

Її призначення разом з розвідкою, руйнуваннями, шпигунством − впливати на суспільну думку або завдавати шкоди ворогові.

Прикладами кіберзброї є:

1

Віруси та програми-шпигуни — збір конфіденційної інформації або виконання певних дій на комп'ютері без дозволу користувача.

2

Віруси-троянці ховаються у вигляді корисної програми або файлу і виконують шкідливі дії під час активації.

3

Комп'ютерні черви здатні самостійно розповсюджуватися через комп'ютерні мережі і використовують вразливості у програмному забезпеченні.

4

DDoS-атаки (Distributed Denial of Service) спрямовані на перевантаження вебсерверів або мережевих інфраструктур шляхом надмірного надходження запитів або трафіку

5

Фішинг — один із видів соціально-інженерної атаки – маскування зловмисника як легальної особи або організації для отримання конфіденційної інформації. Т**ехнічний фішинг** – маскування комп'ютерної системи як легальної. Згідно з даними дослідження Deloitte, 91% всіх кібератак починається з фішингового листа, а 32% всіх успішних проникнень у системи передбачає використання інструментів фішингу.

6

Кіберзброя на основі штучного інтелекту використовується для виявлення вразливостей, розвідки, аналізу великих даних та розробки нових методів атак.

Всі ці варіанти застосовуються за допомогою соціальної інженерії, щоб знайти вразливу точку.
Соціальна інженерія – це спосіб «зламу», в якому використовуються психологічні методи для обману людини.

Очікувані наслідки кібератак:

1. Втрата функціональності об’єкта, зупинка роботи його систем або неправильна робота. Наприклад, зупинка роботи важливих систем керування або призупинення роботи критичних інфраструктурних об’єктів.
2. Знищення, пошкодження чи зміна даних. Це може мати серйозні наслідки для діяльності об’єкта та його здатності виконувати свої функції.
3. Порушення конфіденційності інформації, несанкціонований доступ до секретної інформації об’єкта.
4. Зміна або викривлення інформації, що призводить до помилкових рішень чи спричиняє втрату довіри до об’єкта
5. Підрив робочих процесів, порушення діяльності об’єкта, зменшення продуктивності або збої в роботі систем та процесів.
6. Психологічний тиск та деморалізація. Кібератаки можуть викликати психологічний тиск на персонал об’єкта, призвести до деморалізації та зниження ефективності роботи.

2 Ефективність кібервтручання в діяльність систем супротивника.

Приклади кібервтручання не завжди стають відомими, оскільки об’єкт атаки намагається не повідомляти про свою вразливість. Але відомими стають деякі особливі факти.

У розпал холодної війни, у ***червні 1982 року***, американський супутник раннього попередження виявив великий вибух у Сибіру. Це був вибух на радянському газопроводі. Причиною цього була несправність системи управління комп’ютером, яку радянські шпигуни викрали у фірми в Канаді. Вони не знали, що спеціалісти ЦРУ втручались у програмне забезпечення і зробили так, що воно через певний інтервал часу перестало працювати, скидало оберти насосу та налаштування клапанів. Це спричинило створення надмірного тиску для з’єднань зварних швів трубопроводів. Отримані збитки були значними на той час.

У ***2000***-их роках Китай проводив низку кібероперацій для промислового шпигунства у США та країнах Європи.

У ***2008 р.*** під час проведення операції «Олива» сирійські ППО та радіоелектронна розвідка були заблоковані методами кібервійни.

У ***2010 р.*** спеціально розроблений вірус Stuxnet втрутився в роботу автоматизованої системи, що забезпечувала технологічний ланцюжок атомної промисловості в Ірані. Внаслідок цього центрифуги, на яких збагачувався уран для створення атомної зброї, розігналися до недопустимих швидкостей і зламалися. Це гарантовано призупинило ядерну програму Ірану на декілька років.

2 Ефективність кібервтручання в діяльність систем супротивника.

З ***2011*** року в Північній Кореї із найкращих програмістів набирають групи хакерів, яким надають заробіток і нормальне харчування (для Північної Кореї це розкіш). Ціль їхніх кібератак – криптобіржі у всьому світі; мова про вкрадені мільярди доларів

У ***2012*** році співробітники британської МІ6 зламали сайт Аль-Каїди і замінили інструкцію з виготовлення саморобної бомби рецептом приготування кексів.

2015 р. у шведському центрі управління польотами цивільної авіації вимкнулися комп’ютери, зокрема диспетчерів. Тоді причиною несправності офіційно був названий потужний сонячний шторм. Проте у ***квітні 2016*** року ЗМІ повідомили, що насправді шведська влада направила термінові повідомлення до НАТО про потужну кібератаку на інформаційну систему управління польотами разом із застосуванням засобів радіоелектронного придушення радарів з боку російських військових. Також іншою жертвою кібератаки з боку російських спецслужб була інформаційна система енергетичної компанії Vattenfall.

Кіберпротистояння є настільки важливим, що країни вже давно вводять відповідні підрозділи до складу своїх армій та/або залучають групи цивільних хакерів

3 російсько-українська кібервійна

2013-2014 рр..Під час Революції Гідності було зафіксовано посилення втручання груп нетботів й атаки на телефони лідерів опозиції з метою заблокувати зв'язок з ними, проте це був дуже спрощений рівень.

Під час дострокових Президентських виборів в Україні ***2014*** фахівцями Ситуаційного центру забезпечення кібербезпеки СБУ було знешкоджено атаки на автоматизовану систему «Вибори». За декілька днів до проведення виборів ця система була повністю виведена з ладу. Завдяки залученню фахівців приватної компанії "Датагруп" роботу системи відновили, але залишили один з виявлених «сюрпризів», попередньо його знешкодивши. І ця пастка для російських спецслужб спрацювала – росіяни повірили даним і подали інформацію про нібито виграш Дмитра Яроша на «президентських перегонах».

У ***2015 р***. відбулася атака на «Прикарпаттяобленерго». Було вимкнено близько 30 підстанцій у 3 областях, близько 230 тисяч мешканців залишились без світла від однієї до шести годин.

У ***2016*** році внаслідок атаки на «Київобленерго» було відключено 30 вузлових підстанцій, від яких живилася низка стратегічних об'єктів, понад 80 тисяч споживачів були без електрики протягом однієї-трьох годин.

3 російсько-українська кібервійна

29 грудня 2016 року, на засіданні РНБО України, Президент України Петро Порошенко заявив, що тільки за останні два місяці в Україні було зафіксовано 2,5 тисяч кібератак.

У ***2017 році*** росія провела масову атаку на різні установи вірусом Petya, який розшифрував і знищував усі дані.

Згодом, після обрання нового Президента, Міністр цифрової трансформації України Михайло Федоров злегковажив питання кібербезпеки і свою думку озвучив привселюдно. Ці слова стали свідченням зміщення фокусу уваги в цифровому просторі України. Напередодні та з початком повномасштабної фази війни Україна зазнала відчутних кіберударів, а інтенсивність тільки зростала, тому довелося не тільки посилювати захист, але й розробляти дії у відповідь

З того часу успішною масштабною кібердією росії стала атака на оператора зв'язку «Київстар» у ***грудні 2023 року***. Для побутових споживачів вона була відчутною, оскільки поєднувалася із відключеннями електроенергії внаслідок ракетних обстрілів електростанцій. Натомість українці зламували провайдерів і запускали українські трансляції у різних регіонах, блокували банківські системи та органи влади, викрадали та після цього знищували великі обсяги інформації російських установ і компаній.

4 Основні рекомендації для кібергігієни

Індивідуальний захист громадян важливий, оскільки масові проблеми (злами і втрати облікових записів), крім особистих труднощів для жертв атаки, неминуче вплинуть на інформаційне поле держави.

Щоб зменшити ризик стати ціллю шахраїв у соцмережах, ***кілька порад:***

1

Вимкніть передачу геолокації в метаданих фотографій на вашому смартфоні. Під час відправлення фото можуть передаватися й дані про місце зйомки. Це одна з причин, чому також важливо не фотографувати й не розповсюджувати світлини з місця прильотів.

2

Налаштуйте двофакторну аутентифікацію. Завдяки їй зловмисникам буде набагато важче отримати доступ до вашого акаунту.

3

Для конфіденційних розмов доцільно використовувати тільки програми із найвищим рівнем шифрування. Найкраща серед таких — ***Signal.***

4

Обмежте видимість у соцмережах свого номера телефону, персональних даних і профілю, щоб ці дані були доступні лише вашим контактам.

5

Вимкніть автоматичне завантаження файлів, щоб уникнути контакту з потенційно небезпечними програмами.

6

Не передавайте свої дані незнайомим контактам або сумнівним сервісам. Звертайте увагу на повідомлення про підозрілий вхід чи спробу входу з невідомого пристрою

7

Уникайте переходу за підозрілими посиланнями і не приймайте викликів від незнайомців. Це знизить ризик фішингових атак.

8

Не використовуйте телеграм, вайбер чи фейсбук для авторизації на сторонніх сайтах або сервісах. Це зменшить ризик передачі акаунту зловмисникам.

9

За можливості, користуйтеся вебверсіями месенджерів, оскільки в них легше контролювати доступ до мікрофона, камери, геолокації та телефонної книги.

Дані рекомендації повинні бути дотримані військовослужбовцями вже як обов’язкові до виконання. Це не тільки посилить особисту безпеку, але й безпеку всіх військовослужбовців підрозділу.

РЕКОМЕНДАЦІЇ НА БАЗІ CERT-UA З ОСНОВ КІБІЕРГІГІЄНИ НАСТУПНІ:

1

Використовуйте ліцензійні/легалізовані операційні системи, інші програмні продукти, своєчасно й систематично їх оновлюйте.

2

Користуйтеся антивірусним програмним забезпеченням з технологією евристичного аналізу.

3

Використовуйте програмний міжмережевий екран (брандмауер) та штатні засоби захисту від шкідливого програмного забезпечення.

4

Здійснюйте регулярне резервне копіювання даних, зберігайте резервні копії на зовнішніх носіях інформації (SSD, HDD тощо) та налаштуйте функцію «відновлення системи».

5

Не підключайте флешки та зовнішні диски, не вставляйте CD та DVD тощо у ваш комп’ютер, якщо ви не довіряєте повністю їх джерелу.

6

Не зберігайте автентифікаційні дані в легкодоступних місцях (наприклад, на робочому столі). Використовуйте для зберігання паролів спеціальні програмні засоби (наприклад, KeePass). Використовуйте стійкі, складні та окремі для кожного акаунту паролі

7

Уникайте використання інтернет-банкінгу, електронних платіжних систем, введення автентифікаційних даних під час доступу до інтернету через загальнодоступні (незахищені) безпроводові мережі (в кафе, барах, аеропортах та інших публічних місцях).

8

Будьте особливо обережними з відкриттям вкладень до електронної пошти від невідомих. Найактуальнішим засобом розсилання шкідливого програмного забезпечення є електронна пошта.

9

Іноді, особливо під тиском часу, буває важко відрізнити шкідливі файли від легітимних. Користуйтеся сервісом VirusTotal для перевірки підозрілих файлів шляхом їх одночасного сканування більш ніж 50 антивірусами; але це теж не виключає того, що файл може бути шкідливим.

10

Під час користування інтернет-ресурсами (інтернет-банкінгом, соціальними мережами, системами обміну повідомленнями, новинами,онлайн-іграми) не відкривайте підозрілі посилання (URL), особливо ті, що вказують на вебсайти, які ви зазвичай не відвідуєте.

11

Будьте уважним до проявів інтернет-шахрайства. Найпоширенішим засобом уведення в оману в мережі “Інтернет” є ***фішинг.*** Особливу увагу варто звертати на доменне ім’я інтернет-ресурсу, що запитує автентифікаційні дані, перш ніж натиснути на посилання: зловмисники можуть замаскувати доменне ім’я, щоб воно виглядало знайомим (facelook.com, goooogle.com тощо) або мати вигляд, схожий на справжню.

12

Використовуйте VirusTotal для перевірки підозрілих і скорочених посилань так само, як для сканування файлів.

13

Будьте обережні щодо спливаючих вікон та повідомлень.

14

Під час використання віддаленного доступу необхідно обмежити доступ за допомогою «білого списку» (IP whitelisting).

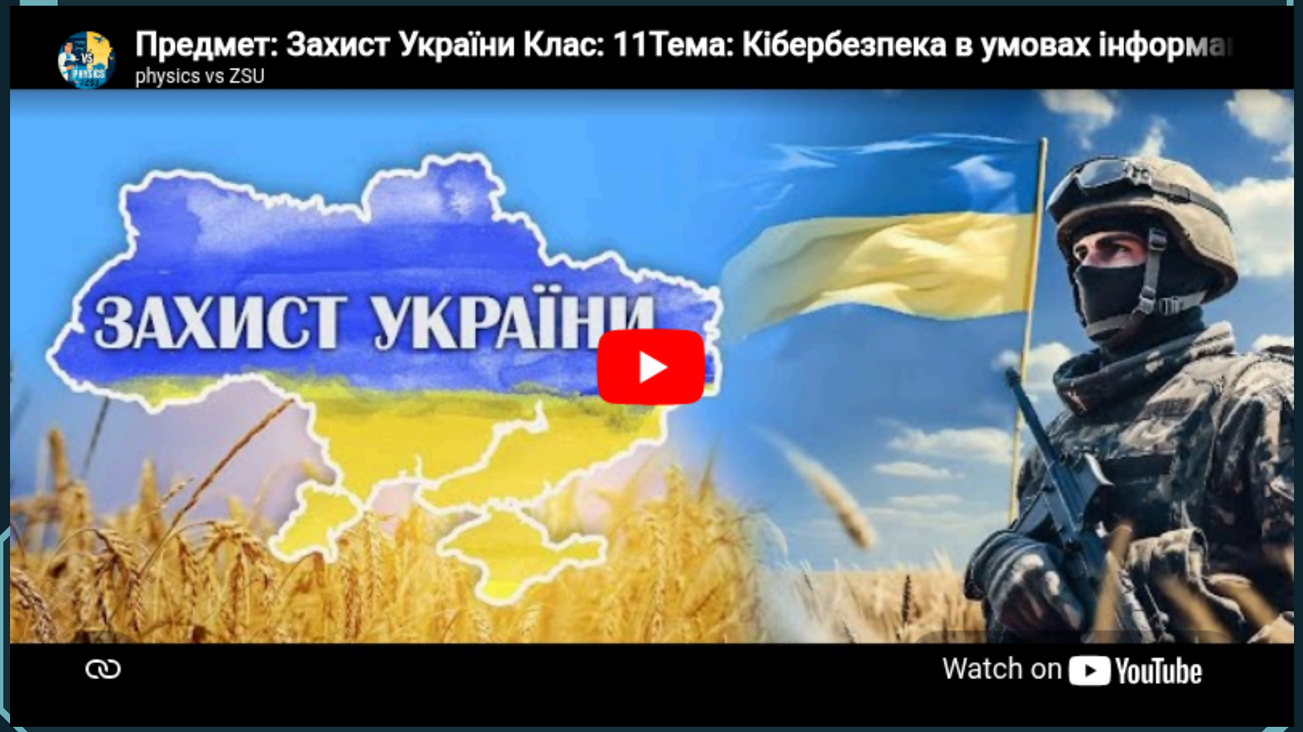
15

Установіть обмеження кількості введення помилкових логінів/паролів.

Дотримання вимог кібергігієни значно зменшує ризик втрати даних!

Висновки

- Кібербезпека є надзвичайно важливою складовою національної безпеки в умовах сучасної інформаційної війни.
- Основними загрозами в кіберпросторі залишаються атаки на державні ресурси, інфраструктуру, банківську систему, а також поширення фейкової інформації через хакерські зломи.
- Особиста цифрова гігієна – це перша лінія захисту кожного користувача. Вона включає безпечне користування паролями, перевірку джерел інформації, обачність у використанні пристроїв і програм.
- Розвиток кіберкультури та освіти з кібербезпеки є запорукою стійкості держави до інформаційно-кібернетичних загроз.


Предмет: Захист України Клас: 11Тема: Кібербезпека в умовах інформа
physics vs ZSU
ЗАХИСТ УКРАЇНИ
Watch on YouTube

Домашнє завдання

ЗАХИСТ УКРАЇНИ 11

Тема Інформаційна війна

11 клас

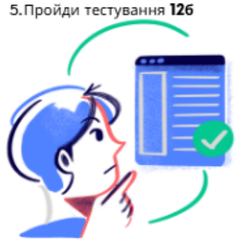


Завдання

1. Повтори матеріал заняття
   - "Кібербезпека в умовах інформаційної війни"
   - (OSINT)
2. Опрацюй самостійно тему і зроби презентацію для демонстрації на наступному занятті. **6-8б**

Цілі та завдання OSINT. Інструменти та методи OSINT.

3. Подивись відео
4. Проведи «OSINT-самоаудит» — спробуй знайти інформацію про себе, використовуючи власне ім'я, фото та ніки в соціальних мережах.. **4б**
5. Пройди тестування **12б**





ДЯКУЮ ЗА УВАГУ!