# КІБЕРБЕЗПЕКА.

## Основи кібергігієни для медичного персоналу.

## КІБЕРГІГІЄНА

# АКТУАЛЬНІСТЬ

Галузь охорони здоров’я є однією із основною цілей кіберзлочинців, але з моменту появи COVID-19, організації зазнали зростання інцидентів і атак, пов’язаних з кібербезпекою. Так, у період з лютого по червень 2020 року організації повідомили про 192 великомасштабних витоки даних з Управління з цивільних прав МОЗ і соціальних служб США – більш ніж в два рази більше, ніж було зареєстровано за той же період в 2019 році, цьому сприяв швидкий перехід до віддаленої роботи, розширення телемедицини та додаткове навантаження на комп’ютерні ресурси.

Наприклад, в останні місяці деякі медичні організації, тимчасово послабили безпеку операційної системи Windows, щоб полегшити додаткові можливості роботи з дому, скоротили кількість постачальників або уклали нові контракти, щоб швидко розгорнути або розширити можливості телемедицини.

***Чому знання кібербезпеки важливо для лікарів:***

**- Медичні дані є конфіденційною інформацією, і їх розголошення може призвести до правових та етичних наслідків.**

**- Злами систем можуть зупинити роботу лікарні, що ставить під загрозу життя пацієнтів оскільки потрібно безперервно надавати медичні послуги .**

**- Втрата даних може негативно вплинути на довіру пацієнтів та суспільства до установи, страждає репутація медичного закладу, лікаря.**

**Отже, кіберзлочинці націлені на органи охорони здоров'я, фармацевтичні компанії, наукові співтовариства, медичні дослідні організації та місцеві органи влади, а також на інших осіб, які беруть участь в охороні здоров'я, оскільки медичні установи є особливо привабливими для кібератак через високу цінність медичних даних. Зловмисники можуть використовувати ці дані для шантажу, продажу на чорному ринку або зламу систем для вимагання викупу.**

***Саме тому, кібербезпека в медицині виходить на більш важливе місце.***

# Мета лекції:

- **формування у слухачів знань з інформаційної безпеки (кібербезпеки);**
- **розвиток цифрової грамотност;**
- **вивчення питань інформаційної безпеки;**
- **формування та розвиток професійних компетенцій, що дозволяють застосовувати сучасні технології захисту інформації, вибирати засоби та інструменти захисту інформації, які мінімізують загрози несанкціонованого доступу до даних.**

1. **Поняття кібербезпеки, кібератаки. Конфіденційність, цілісність та доступність даних**
2. **Типи загроз. Способи захисту інформації від загроз**
3. **Онлайн (online) та офлайн (offline)-ідентифікація. Захист особистих даних**
4. **Захист організації**

# Поняття кібербезпеки, кібератаки. Конфіденційність, цілісність та доступність даних

## Cyber Security - забезпечення захисту даних

*Електронна інформаційна мережа використовується для збору, обробки, зберігання та обміну великою кількістю цифрової інформації.*

**Кібербезпека** – це сукупність технічних і соціальних засобів, стратегій, принципів для забезпечення захисту суспільства від загроз і впливів з небажаними наслідками, що походять від інтернет-середовища.

***Кібербезпека*** - це набір заходів для захисту систем, мереж і програм від цифрових атак. Лікарі працюють із чутливими даними пацієнтів, тому повинні бути особливо уважні до кібербезпеки.

*З початку 2022 року число виявлених кіберзагроз зросло на 20%, зокрема збільшилась кількість шпигунських програм та спам-листів!*

## *Основні загрози кібербезпеки в медицині*

1. **Шкідливе програмне забезпечення (віруси, трояни):**

- Може пошкодити медичне обладнання або систему керування медичними записами.
- Викрадення медичних даних з метою шантажу або продажу на чорному ринку.

2. **Фішинг та соціальна інженерія:**

- Лікарі можуть отримати електронні листи чи повідомлення з підробленими посиланнями або документами, які можуть здаватися легітимними, але призначені для викрадення даних.

# *Основні загрози кібербезпеки в медицині*

3. **Атаки на медичне обладнання:**

- Багато сучасних медичних пристроїв підключені до Інтернету (напр., інсулінові помпи, кардіостимулятори). Зловмисники можуть зламати ці пристрої та втрутитися в їх роботу, що може загрожувати життю пацієнтів.

4. **Ransomware (віруси-вимагачі):**

- Один з найбільш небезпечних типів атак у сфері охорони здоров'я. Атака типу ransomware блокує доступ до медичних систем, вимагаючи викуп для їх відновлення. Це може паралізувати роботу лікарень і медичних закладів.

5. **Злам електронних медичних записів (EMR):**

- Електронні медичні записи зберігають велику кількість чутливої інформації. Злам цих систем може призвести до витоку особистих даних пацієнтів, що порушує медичну етику та законодавство.

# Поняття кібербезпеки, кібератаки. Конфіденційність, цілісність та доступність даних

## Фундаментальні поняття (CIA)

- ***confidentiality*** секретні дані будуть доступні дозволеним користувачам

Конфедецій-ність

- ***integrity*** гарантія збереження даними правильних

цілісність

- ***availability*** авторизовані користувачі завжди будуть отримувати

доступність

# Поняття кібербезпеки, кібератаки. Конфіденційність, цілісність та доступність даних

## Безпека інформаційної системи

*безпека комп'ютера*

*мережева безпека*

*Кібербезпека є необхідною умовою розвитку інформаційного суспільства*

# Поняття кібербезпеки, кібератаки. Конфіденційність, цілісність та доступність даних

## *Безпека комп'ютера*

*(захист даних, що зберігаються і обробляються комп'ютером)*

засоби операційних систем та програм

замкнути на замок клавіатуру

зняти жорсткий накопичув

# Поняття кібербезпеки, кібератаки. Конфіденційність, цілісність та доступність даних

## *Мережева безпека*

захист даних у момент їх передачі по лініях зв’язку

захист від несанкціоно-ваного віддаленого доступу в мережу

чітко визначені права кожного користувача

# Поняття кібербезпеки, кібератаки. Конфіденційність, цілісність та доступність даних

**Безпечна інформаційна система** – це система, яка, по-перше, захищає дані від несанкціонованого доступу, по-друге, завжди готова надати їх своїм користувачам, а по-третє, надійно зберігає інформацію і гарантує незмінність даних.

**Безпечна інформаційна система**

- **Конфіденційність**
  - Несанкціоноване ознайомлення з інформацією становить загрози конфідиційності
- **Доступність**
  - Порушення можливості використання комп'ютерних систем або оброблювальної інформації становить загрозу доступності
- **Цілісність**
  - Несанкціонована модифікація інформації становить загрозу цілісності

# Поняття кібербезпеки, кібератаки. Конфіденційність, цілісність та доступність даних

**Конфіденційність** – це основний компонент InfoSec, який полягає в тому, що доступ до інформації можуть отримувати лише авторизовані користувачі.

Шифрування даних

Багатофакторна автентифікація

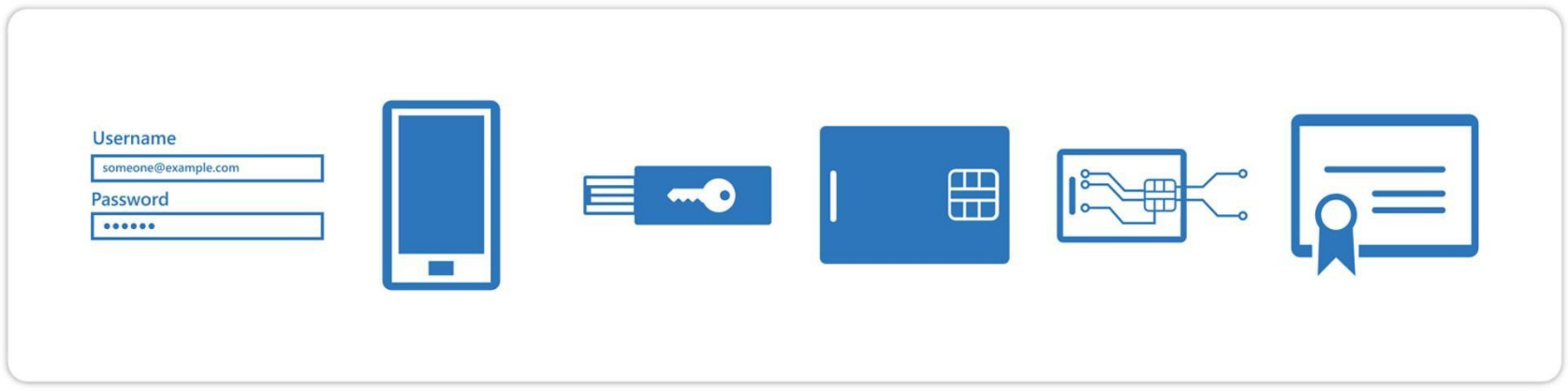
Захист від втрати даних

*приклади інструментів для забезпечення конфіденційності*

# Поняття кібербезпеки, кібератаки. Конфіденційність, цілісність та доступність даних

*Що таке багатофакторна автентифікація (БФА)?*

**Багатофакторна автентифікація (БФА)** додає ще один рівень захисту під час входу. Під час доступу до облікових записів або програм користувачі проходять додаткову перевірку ідентичності, наприклад сканують відбиток пальця чи вводять код із телефона




Багатофакторна автентифікація (БФА) за допомогою хмарної служби *Azure Active Directory (Azure AD)* допомагає *захистити доступ до даних і програм*, не ускладнюючи роботу для користувачів.

# Поняття кібербезпеки, кібератаки. Конфіденційність, цілісність та доступність даних

*Поняття конфіденційності, доступності та цілісності можуть бути визначені не тільки по відношенню до інформації, але і до інших ресурсів обчислювальної мережі, наприклад зовнішніх пристроїв або додатків.*

| | |
|---|---|
| Конфіденційність | • доступ до пристрою мають користувачі, яким цей доступ дозволений |
| Доступність | • готовність до використання кожного разу, коли в цьому виникає необхідність |
| Цілісність | • незмінності параметрів налаштування цього пристрою |

**Незаконне використання мережевих пристроїв завдає матеріальної шкоди організації, а також є порушенням безпеки системи.**

*Необмежений доступ до пристрою друку дозволяє зловмисникові отримувати копії, роздруковувати документи, змінювати параметри налаштування, що може призвести до зміни черговості робіт і навіть до виведення пристрою з ладу.*

# Типи загроз. Способи захисту інформації від загроз

*Наскільки ваш комп'ютер або веб-сайт захищений від хакерської атаки – це саме і є питання кібербезпеки.*

**Кібератака** – це спроба реалізації загрози. Тобто, це дії кіберзловмисників або шкідливих програм, які спрямовані на захоплення інформаційних даних віддаленого комп'ютера, отримання повного контролю над ресурсами комп'ютера або на виведення системи з ладу.

**Кібератака**

- Порушення цілості систем і даних, що зберігаються всередині
- Несанкціонований доступ до конфіденційної інформації
- Порушення нормального функціонування організації
- Використання атак для шифрування даних і вилучення грошей у жертви

# Типи загроз. Способи захисту інформації від загроз

**Віруси вимагачі (Ransomware - англ. ransom — викуп і software — програмне забезпечення).** Це шкідливе програмне забезпечення, яке блокує пристрій або шифрує його вміст, вимагаючи гроші у жертв.

Оператори програм-вимагачів використовують багато різних технік інфікування:

- **Шифрування диску** та блокування доступу користувача до операційної системи.
- **Блокування екрану** користувача.
- **Шифрування даних** на диску жертви.
- Блокування пристроїв Android шляхом **зміни коду доступу** для заблокування пристрою користувача.

# Типи загроз. Способи захисту інформації від загроз

*Як працює програма-вимагач?*

Після завантаження на комп'ютер шкідлива програма активується і блокує всю операційну систему, після чого запустить попередження із загрозою і з зазначенням суми викупу, яку треба заплатити за «порятунок» всієї інформації.

*Щоб додатково налякати жертву, іноді додається IP-адрес, назви Вашого Інтернет-провайдера або навіть фотографія, перехоплена з Вашої веб-камери.*

# Типи загроз. Способи захисту інформації від загроз

***Як захиститися від атак-вимагачів?***

– Регулярне оновлення компонентів операційної системи.

– Тримати програмне забезпечення на комп'ютері в актуальному стані оновлюючи його.

– Не відкривати спам-повідомлення електронної пошти та не відвідувати підозрілі веб-сайти.

– Тримати увімкненим мережевий екран.

– Використовувати відомі антивіруси для захисту від шкідливих програм та оновлювати антивірусні бази.

– Перед першим запуском нових програм перевіряти їх антивірусом.

– Періодично виконувати резервне копіювання важливих даних.

# Типи загроз. Способи захисту інформації від загроз

**Ботнет** — це мережа комп'ютерів, інфікована шкідливим програмним забезпеченням. Кіберзлочинці використовують ботнет-мережі, які складаються з великої кількості комп'ютерів для різних зловмисних дій без відома користувачів.

## Атака ботнетів

- Розподілені атаки типу «відмова в обслуговуванні»
- Розповсюдження спам-листів
- Крадіжка конфіденційних даних
- Встановлення шпигунських програм

# Типи загроз. Способи захисту інформації від загроз

*Комп'ютер може потрапити в мережу ботнету через встановлення певного програмного забезпечення, без відома користувача.*

Трапляється це зазвичай через:

– Інфікування комп'ютера вірусом через вразливість в ПЗ (помилки в браузерах, поштових клієнтах, програмах перегляду документів, зображень, відео).
– Недосвідченість або неуважність користувача — шкідливе ПЗ маскується під «корисне програмне забезпечення».
– Використання санкціонованого доступу до комп'ютера (рідко).
– Підбір адміністративного пароля до мережевих ресурсів зі спільним доступом (наприклад, до $ADMIN, що дозволяє віддалено виконати програму) — переважно в локальних мережах.

*У 2016 році ботнет був використаний для створення найбільшої DDoS-атаки в історії, яка спричинила збої у роботі таких сайтів як Twitter, Amazon та Netflix*

# Типи загроз. Способи захисту інформації від загроз

***Щоб не стати частиною ботнету, важливо дотримуватися таких правил безпеки:***

- Виконувати регулярне оновлення програмного забезпечення та виправлення помилок.
- Необхідно бути обережним, завантажуючи файли або програми та відкриваючи вкладення.

– Використовувати рішення для забезпечення безпеки в Інтернеті, до яких входить захист від ботнет-атак. Такі рішення виявляють та блокують загрози та використовують брандмауер.

**Брандмауер (Brandmauer)** – це комп'ютерна програма, метою якої є захист комп'ютера від вірусів і хакерських атак) для фільтрації зв'язку між комп'ютером та Інтернетом.

# Типи загроз. Способи захисту інформації від загроз

**Соціальна інженерія** — низка не технічних прийомів маніпулювання користувачами, які використовуються кіберзлочинцями під час атак. Це мистецтво маніпулювання людьми через виконання дій або розголошення конфіденційної інформації.

*Більшість методів соціальної інженерії не вимагають особливих технічних знань з боку зловмисників, а отже використовувати ці методи може будь-хто — від дрібних злодіїв до досвідчених кіберзлочинців.*

Існує багато методик, які підпадають під загальний термін соціальної інженерії в галузі кібербезпеки. Серед найвідоміших методик — **спам та фішинг.**

# Типи загроз. Способи захисту інформації від загроз

**Спам** — це масове розсилання небажаних листів. Найчастіше спам — це лист електронної пошти, який надсилається одразу на велику кількість адрес, але він також може бути доставлений через миттєві повідомлення, SMS та соціальні мережі.

*Власне, спам не є соціальною інженерією, однак в деяких кампаніях використовуються його види*

Фішинг

Цілеспрямо-ваний фішинг (spearphishing)

Вішинг (vishing)

Смішинг (smishing)

Шкідливі вкладення або посилання

# Типи загроз. Способи захисту інформації від загроз

**Фішинг** — це форма кібератаки, під час якої злочинець намагається завойовувати довіру жертви для виманювання конфіденційної інформації.

Для отримання даних зловмисники також створюють відчуття терміновості або застосовують тактику залякування. Варто зазначити, що фішингові кампанії можуть бути націлені на велику кількість випадкових користувачів або конкретну особу чи групу.

**Цілеспрямований фішинг** — це форма фішингу, під час якої зловмисник надсилає повідомлення, спрямовані на конкретну групу людей, або навіть просто окрему особу з метою викрадення даних або маніпулювання ними в зловмисних цілях.

# Типи загроз. Способи захисту інформації від загроз

**Вішинг** — це методи соціальної інженерії, подібні до фішингу, але здійснюються не через електронну пошту, а реалізовується через шахрайські телефонні дзвінки.

***Яскравий приклад:*** *дзвінок нібито з банку*. Зловмисники, вдаючи із себе співробітників банку, вигадують різні приводи для виманювання даних. Наприклад, кажуть, що відбулося блокування карти, і служба безпеки банку проводить звіряння особистих даних клієнтів для убезпечення їх від шахрайства.

***Інший приклад:*** *«Ваш родич потрапив в аварію чи поліцію».* Найчастіше зловмисники здійснюють такого роду дзвінки вночі або рано вранці, коли людина сонна, погано міркує.

# Типи загроз. Способи захисту інформації від загроз

**SMS-фішинг (смішинг)** — різновид фішингу, який здійснюється через SMS-розсилки.

Одним із яскравих прикладів є SMS-повідомлення нібито про ***виграш великої суми грошей або автомобіля***. Однак, щоб отримати виграш, потрібно внести 10% за «оформлення» необхідної документації тощо. Також SMS-шахрайством є повідомлення від «банків».

# Типи загроз. Способи захисту інформації від загроз

**«Дорожнє яблуко» («road apple»), або «Троянський кінь»** — різновид фішингу, який здійснюється через SMS-розсилки.

Носій може мати логотип компанії чи надпис, що зацікавить співробітника, наприклад, «Список на звільнення», «Заробітна плата. Жовтень» тощо.

Щойно співробітник вставить такий носій у комп'ютер, він запустить шкідливий код, який надасть хакеру віддалений доступ до мережі.

# Типи загроз. Способи захисту інформації від загроз

**«Зворотна соціальна інженерія»** — це вид соціальної інженерії, за якої особа сама звертається до шахрая та повідомляє свої конфіденційні дані.

Зловмисник підсовує жертві оголошення виду «*Якщо виникли неполадки з комп'ютером, зателефонуйте за таким-то номером*»

Цілком імовірно, що через певний час хтось із співробітників зателефонує і шахрай зможе вивідати інформацію, яка його цікавить

# Типи загроз. Способи захисту інформації від загроз

**Складна атака через проміжну ціль («Supply chain attack»)** — це кількаступенева атака, в ході якої хакер атакує не напряму організацію, яка його цікавить, а менш захищену проміжну організацію чи установу, а вже через неї компрометує ту ціль, яка від самого початку його цікавила.

***Наприклад***, хакер обрав своєю ціллю заклад освіт, однак після його вивчення зрозумів, що установа має високий рівень захисту і просто так її не скомпрометувати.

У такому разі хакер може сфокусуватися на атаці компанії, яка розробляє або обслуговує сайт. Невеликі компанії зазвичай менш захищені, а тому скомпрометувати їх набагато простіше.

***Висновок:*** *пам'ятайте, справжньою ціллю хакера можете бути не Ви, а Ваш керівник чи установа, де Ви працюєте, а Ви – це лише інструмент у досягненні цілі!*

# Типи загроз. Способи захисту інформації від загроз

***Як здійснюються атаки з використанням соціальної інженерії?***

- Граматика і лексика
- Адреса відправника
- Почуття терміновості
- Запит на конфіденційну інформацію
- Щось звучить занадто добре, щоб бути правдою

# Типи загроз. Способи захисту інформації від загроз

***Способи захисту від атак з використанням соціальної інженерії:***

1. Регулярне навчання з кібербезпеки усіх працівників.

2. Здійснювати сканування на наявність слабких паролів. Крім того, створіть додатковий рівень захисту за допомогою двофакторної аутентифікації.

3. Впровадження рішення для захисту, які попереджають про можливі випадки шахрайства, а також повідомляють про виявлення спаму та фішингу.

4. Створення політики безпеки з чітким планом дій, які потрібно буде виконати працівникам, якщо вони стикнуться з проявами соціальної інженерії.

5. Використовувати рішення для централізованого управління корпоративною мережею, наприклад, ESET Security Management Center, щоб забезпечити повний огляд мережі, усіх рішень з безпеки та подій для виявлення та знешкодження потенційних загроз.

# Онлайн (online) та офлайн (offline)-ідентифікація. Захист особистих даних

*Чим більше часу ви проводите в Інтернеті, тим сильніше на ваше життя може вплинути ваша ідентичність як в Інтернеті, так і в офлайні.*

**Офлайн-ідентичність** — це ви самі, особа, з якою ваші друзі та сім'я взаємодіють щодня вдома або на роботі.

**Онлайн-ідентичність** — це те, як ви представляєте себе іншим в Інтернеті.

Ім'я користувача не повинно містити жодної особистої інформації. Це має бути щось доречне і прийнятне.

Ім'я користувача не повинно давати привід стороннім людям подумати, що ви є легкою ціллю для кіберзлочинців або хочете привернути небажану увагу.

# Онлайн (online) та офлайн (offline)-ідентифікація. Захист особистих даних

*У віртуальному світі Інтернету ми постійно стикаємося з проблемою* ***ПРИВАТНОСТІ***

Згідно зі ст. 8 Європейської конвенції з прав людини, приватність закріплюється як окремий аспект приватного життя. Ніхто не має права збирати та поширювати інформацію про наше приватне життя. Особиста інформація, якою ми не хочемо ділитися, має залишатися конфіденційною, не підлягати розголосові.

Питання збереження приватності в мережі Інтернет є актуальним, оскільки віртуальне спілкування практично ніколи не буває приватним.

Користувачі Інтернету самі несуть відповідальність за захист відомостей про своє життя.

**СТАТТЯ 8**

**Право на повагу до приватного і сімейного життя**

1. Кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції.

2. Органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб.

# Онлайн (online) та офлайн (offline)-ідентифікація. Захист особистих даних

*Відповідно до Закону України «Про захист персональних даних»:*

**Персональні дані** — відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

*Незаконне отримання та оприлюднення (поширення) чужої особистої інформації є злочином.*

***Важливо!*** За порушення недоторканості приватного життя, а саме за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації винна особа притягується до кримінальної відповідальності (*стаття 182 Кримінального кодексу України*)

# Онлайн (online) та офлайн (offline)-ідентифікація. Захист особистих даних

## Способи захисту особистих даних:

### *1. Створення складних паролів*

Довший пароль забезпечує більший рівень безпеки. Використовуйте **щонайменше вісім символів**. Це можуть бути **комбінації літер, цифр і символів.**

- **Не використовуйте поширені слова**
- **Не використовуйте особисту інформацію**
- **Поєднуйте різні типи символів**

Використовуйте комбінації буквено-цифрових символів і знаків.

- Великі літери. Наприклад, A, E, T
- Малі літери. Наприклад, a, e, т
- Цифри. Наприклад, 2, 6, 7
- Спеціальні символи. Наприклад, ! @ & *

# Онлайн (online) та офлайн (offline)-ідентифікація. Захист особистих даних

## Способи захисту особистих даних:

### 2. *Використання двофакторної аутентифікації*

Крім імені користувача та пароля, або особистого ідентифікаційного номера (PIN) чи шаблону, для двофакторної аутентифікації іноді потрібен додатковий токен безпеки, такий як:

– Фізичний об'єкт - кредитна картка, телефон або ключ-брелок.

– Біометричне сканування - відбиток пальця, відбиток долоні, розпізнавання обличчя або голосу.

*Навіть якщо використовується двофакторна аутентифікація хакери можуть отримати доступ до ваших облікових записів в Інтернеті через такі атаки, як фішинг, зловмисне програмне забезпечення та соціальна інженерія.*

# Онлайн (online) та офлайн (offline)-ідентифікація. Захист особистих даних

## Способи захисту особистих даних:

### 3. *Шифрування повідомлень*

**Шифрування** — це процес перетворення інформації у форму, в якій неавторизована сторона не зможе її прочитати.

Більшість месенджерів вже використовують шифрування.

*Наприклад*, WhatsApp пропонує шифрування з 2016 року. Це означає, що ніхто не зможе побачити ваше повідомлення, окрім отримувача.

Крім того – в месенджерах є секретні чати. Але експерти більше довіряють Telegram. А найзахищеніший і зовсім непопулярний в нас месенджер – Signal.

# Онлайн (online) та офлайн (offline)-ідентифікація. Захист особистих даних

## Способи захисту особистих даних:

### 4. *Не підключатися до громадського WiFi.*

Громадські мережі не завжди захищені паролем. Підключатись до відкритого WiFi – погана ідея. Хакери можуть створити мережу – двійника із такою ж назвою та перехопити дані.

Публічні Wi-Fi точки доступу (hot spot) дають змогу отримувати доступ до особистої онлайн-інформації та мандрувати Інтернетом. Тим не менш, краще не підключитися і не надсилати будь-яку важливу особисту інформацію через загальнодоступну бездротову мережу.

# Онлайн (online) та офлайн (offline)-ідентифікація. Захист особистих даних

## Способи захисту особистих даних:

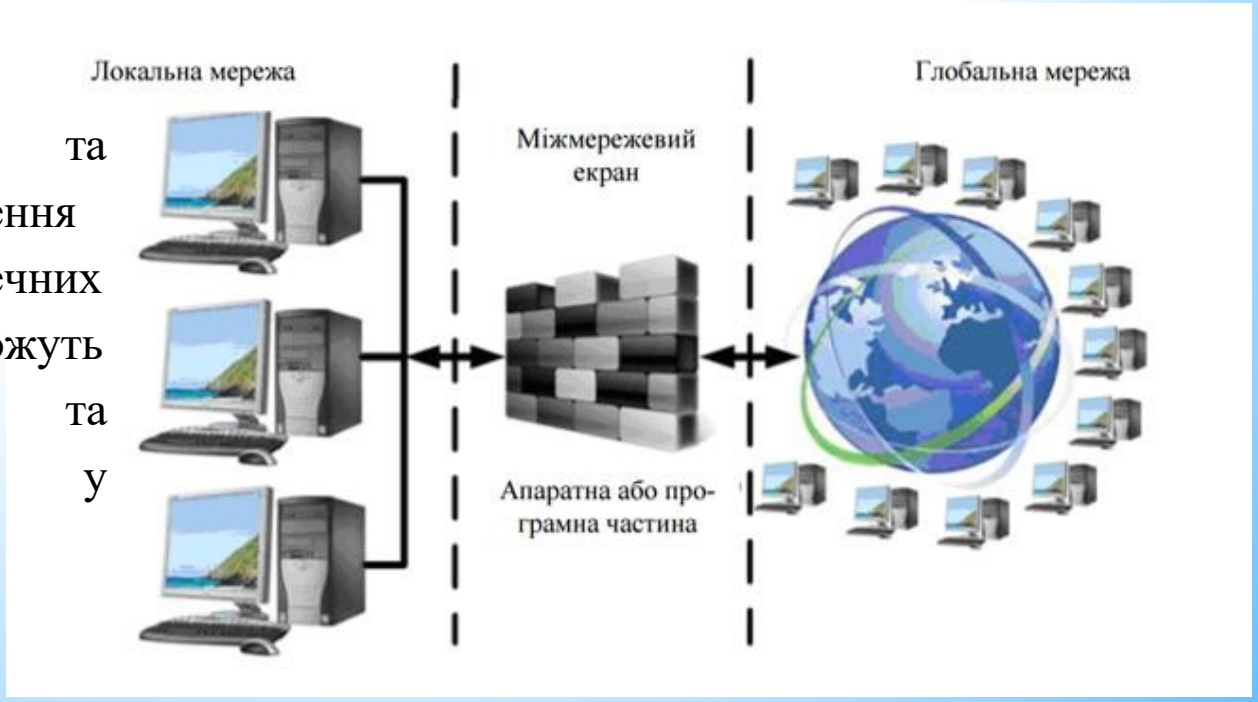
### *5. Використання протоколу HTTPS*

Цей протокол більш безпечний, ніж HTTP, він шифрує всю інформацію та захищає від атак. Необхідно слідкувати, аби HTTPS обов'язково був в адресному рядку сайтів, де ми залишаємо дані банківської карти.

# Захист організації

**Міжмережний екран (фаєрвол, брандмаурер)** — це стіна або перегородка, яка призначена для запобігання поширенню вогню з однієї частини будівлі в іншу.

Захищають мережі та пристрої від вторгнення потенційно небезпечних кіберзлочинців, які можуть інфікувати пристрої та використовувати їх у зловмисних цілях.



# Захист організації

*Головна функція брандмауера —*
фільтрація шкідливого та потенційно небезпечного контенту та з'єднань

***Мережевий екран (брандмауер) призначений:***

- для контролю вхідного і вихідного трафіку на комп'ютері або в локальній мережі,
- дає змогу припиняти практично всі види мережевих атак, вирізати рекламу, відключати банери, рекламні скрипти, спливаючі вікна та інше,
- не надсилати іншим «чужим» серверам інформацію про ваш комп'ютер,
- робить даремною роботу програм-троянів і засобів віддаленого адміністрування.

# Захист організації

**Брандмауери:**

**Апаратні брандмауери** (їх ще називають мережними) розміщені при вході в локальну мережу і фільтрують весь трафік, що надходить у мережу з різних хостів (серверів, комп'ютерів).

**Програмні брандмауери** розміщені на індивідуальному комп'ютері всередині мережі. Такі брандмауери використовується при підключенні нашого особистого комп'ютера прямо до Інтернету, працює на окремому комп'ютері і фільтрує весь вхідний / вихідний трафік даної машини

# Захист організації

Отже, ***кібербезпека*** — це важлива галузь, що впливає на кожного з нас у цифровому світі. Знання основ кібербезпеки допоможуть вам захистити свої дані та уникнути багатьох небезпек. Завжди пам'ятайте, що найслабшим місцем у будь-якій системі є людський фактор, тому ваша уважність і освіченість — найкраща зброя проти кіберзагроз.

Якщо кібератака все ж таки сталася, важливо **швидко реагувати:**

**- Негайно повідомити відповідальні служби (якщо такі є в медичному закладі) або кіберполіцію.**

**- Ізолювати уражені системи від загальної мережі, щоб запобігти поширенню загрози.**

**- Зберегти докази для подальшого розслідування.**

**- Повідомити пацієнтів, якщо їхні дані могли бути скомпрометовані.**

# Захист організації

## Основні проблеми з брандмауерами:

Найпоширенішою проблемою є те, що крім шкідливих програм, брандмауер часто блокує нормальний, потрібний нам трафік. Деякі веб-сайти можуть мати обмежений доступ або не відкривається, оскільки вони були неправильно ідентифіковані.

Досить часто, виникають проблеми з мережевими іграми, оскільки фаєрвол, розпізнає подібний трафік, як шкідливий та блокує роботу програм. Виходячи з цього, слід зазначити, що хоч брандмауер штука вельми корисна, але, його потрібно вірно налаштовувати, щоб він не псував життя своїми заборонами.

# Основні принципи кібергігієни

## *Що таке кібергігієна?*

***Кібергігієна*** - це набір практик, правил спрямованих на підтримку інформаційної безпеки. Особливо важливо для лікарів, які працюють з чутливими даними пацієнтів.

Чому це важливо для лікарів?

1. Медична інформація є конфіденційною і особливо цінною для зловмисників.
2. Захист пацієнтів і їхніх даних - це частина професійної відповідальності.
3. Уникнення потенційних юридичних наслідків.

# Основні принципи кібергігієни

1. **Не використовувати незахищені Wi-Fi мережі для доступу до медичних даних.**
2. **Резервне копіювання важливої інформації.**
3. **Навчання персоналу з кібербезпеки.**
4. **Використовувати складні паролі і їх регулярно оновлювати.**
5. **Застосовувати двофакторну аутентифікацію.**
6. **Захищати пристрої за допомогою антивірусного ПЗ.**
7. **Оновлювати програмне забезпечення.**
8. **Зберігати обережність під час відкриття електронних листів і файлів.**

***Дотримання основ кібергігієни є ключовим для безпеки пацієнтів та лікарів. Застосування цих простих правил допоможе уникнути ризиків у кіберпросторі.***

# Дякую за увагу!