МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ПРИВАТНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД «МЕДИКО-ПРИРОДНИЧИЙ УНІВЕРСИТЕТ»

Кафедра Медсестринства і громадського здоров’я

НАВЧАЛЬНА ДИСЦИПЛІНА

ІНФОРМАТИКА ТА КОМП'ЮТЕРНА ТЕХНІКА ЗА ПРОФЕСІЙНИМ СПРЯМУВАННЯМ

Лекція 4: Інформаційна безпека та конфіденційність даних у охороні здоров'ї

План лекції

1. Вступ
   - Значення інформаційної безпеки у охороні здоров'я.
   - Поняття конфіденційності медичних даних.
   - Мета лекції.
2. Основи інформаційної безпеки в охороні здоров'я
   - Ключові принципи захисту даних.
   - Загрози інформаційній безпеці: хакерські атаки, фішинг, віруси.
   - Основні методи захисту даних: шифрування, аутентифікація, резервне копіювання.
3. Конфіденційність медичних даних
   - Що таке персональні дані і чому вони важливі для охорони здоров'я.
   - Законодавче регулювання: Закон України "Про захист персональних даних", GDPR у Європі.
   - Права пацієнтів та обов'язки медичних працівників щодо збереження конфіденційності.
4. Захист електронних медичних записів (ЕМЗ) та інформаційних систем
   - Способи захисту ЕМЗ: шифрування даних, двофакторна аутентифікація.
   - Приклади порушень безпеки в медичних закладах та їх наслідки.
   - Роль ІТ-відділів у забезпеченні захисту медичних систем.
5. Роль кібербезпеки в умовах пандемії
   - Підвищення загроз кібербезпеці під час пандемії COVID-19.

- Використання телемедицини та загрози безпеці під час її впровадження.

- Як захищати дані пацієнтів під час віддалених консультацій.

6. Підсумки та обговорення

- Основні висновки щодо захисту інформації у охороні здоров'я.

- Відповіді на питання студентів.

1. Вступ

1.1. Значення інформаційної безпеки у охороні здоров'ї

У сфері охорони здоров'я медичні дані є надзвичайно важливими і водночас дуже чутливими. Інформація про здоров'я пацієнтів має бути надійно захищена, оскільки її витік може мати серйозні наслідки як для окремих осіб, так і для охорони здоров'я в цілому. Оскільки електронні медичні записи (ЕМЗ) стали основним інструментом для обміну інформацією між лікарями та медичними установами, питання кібербезпеки стали ще більш актуальними.

1.2. Поняття конфіденційності медичних даних

Конфіденційність медичних даних — це захист інформації про здоров'я пацієнтів від несанкціонованого доступу. Кожен пацієнт має право на захист своїх даних, а медичні працівники зобов'язані забезпечити конфіденційність цих даних на кожному етапі їх обробки.

1.3. Мета лекції

Ця лекція має на меті ознайомити вас із основними принципами інформаційної безпеки, методами захисту медичних даних та нормативно-правовими вимогами, що регулюють обробку конфіденційної інформації в охороні здоров'я.

2. Основи інформаційної безпеки в охороні здоров'я

2.1. Ключові принципи захисту даних

- Конфіденційність: Дані мають бути доступні тільки уповноваженим особам.

- Цілісність: Дані повинні залишатися точними і незмінними під час обробки.

- Доступність: Дані повинні бути доступними для обробки вчасно і при необхідності.

2.2. Загрози інформаційній безпеці

- Хакерські атаки: Неавторизований доступ до медичних систем.

- Фішинг: Шахрайські спроби отримати конфіденційну інформацію.

- Віруси і зловмисне ПЗ: Програми, які можуть викрасти або пошкодити медичні дані.

2.3. Основні методи захисту даних

- Шифрування: Захист даних шляхом їх кодування, що ускладнює несанкціонований доступ.

- Аутентифікація: Використання складних паролів та двофакторної аутентифікації для доступу до системи.

- Резервне копіювання: Регулярне збереження копій даних для відновлення у разі втрати або пошкодження інформації.

3. Конфіденційність медичних даних

3.1. Що таке персональні дані і чому вони важливі?

Персональні дані — це будь-яка інформація, що стосується особистості пацієнта (ім'я, дата народження, медичні записи, результати аналізів). Захист таких даних є основою безпеки у сфері охорони здоров’я, оскільки розголошення цієї інформації може призвести до серйозних наслідків для пацієнта.

3.2. Законодавче регулювання

- Закон України "Про захист персональних даних" регулює збирання, обробку та захист особистих даних пацієнтів.

- GDPR (Загальний регламент захисту даних ЄС) встановлює жорсткі вимоги до обробки та зберігання даних у Європейському Союзі, що є актуальним для українських медичних закладів, які співпрацюють з європейськими організаціями.

3.3. Права пацієнтів та обов'язки медичних працівників

Пацієнти мають право на доступ до своїх медичних даних, а також на їх виправлення або видалення. Медичні працівники повинні забезпечувати конфіденційність цієї інформації та гарантувати її захист.

4. Захист електронних медичних записів (ЕМЗ) та інформаційних систем

4.1. Способи захисту ЕМЗ

- Шифрування даних: Шифрування захищає дані в ЕМЗ, роблячи їх непридатними для прочитання без спеціального ключа.

- Двофакторна аутентифікація: Для доступу до електронних медичних записів медичні працівники повинні використовувати не тільки пароль, але й другий фактор, наприклад, смс-код або біометрію.

4.2. Приклади порушень безпеки

Одним із найвідоміших випадків порушення кібербезпеки в медичних установах була атака вірусу-здирника WannaCry у 2017 році, яка вразила системи охорони здоров’я по

всьому світу, включаючи лікарні у Великобританії. Цей випадок продемонстрував важливість регулярного оновлення систем безпеки та підвищення кіберстійкості медичних закладів.

4.3. Роль IT-відділів у забезпеченні захисту

IT-відділи грають ключову роль у забезпеченні безпеки медичних даних. Вони повинні регулярно оновлювати програмне забезпечення, моніторити мережі на

4. Захист електронних медичних записів (ЕМЗ) та інформаційних систем (доповнення)

4.1 Способи захисту ЕМЗ (доповнення)

Ще один важливий метод захисту даних пацієнтів — аудит доступу. Це означає, що кожен раз, коли будь-який медичний працівник отримує доступ до електронної медичної карти, система реєструє цей доступ. Це дозволяє відстежити всі зміни в записах пацієнта та виявити несанкціоновані дії. Такий аудит забезпечує прозорість у роботі з медичними даними та дозволяє швидко реагувати у випадку порушення безпеки.

4.2 Приклади порушень безпеки (доповнення)

Ще один приклад порушення кібербезпеки в медичних установах — атака на MedStar Health у 2016 році, де в результаті кібератаки було заблоковано доступ до медичних записів пацієнтів, що змусило лікарів тимчасово перейти на паперові записи. Цей випадок продемонстрував, як важливо для медичних установ мати не лише кібербезпеку, але й резервні системи для доступу до даних.

4.3 Роль IT-відділів у забезпеченні захисту (доповнення)

IT-відділи також відповідають за освіту персоналу щодо безпеки даних. Регулярні тренінги з кібербезпеки для медичних працівників допомагають уникати поширених загроз, таких як фішинг та небезпечні програми. Медичний персонал повинен знати, як правильно обробляти персональні дані пацієнтів і як уникати несанкціонованого розголошення інформації.

5. Роль кібербезпеки в умовах пандемії

5.1 Підвищення загроз кібербезпеці під час пандемії COVID-19

Пандемія COVID-19 створила нові виклики для систем охорони здоров'я в усьому світі, включаючи зростання кіберзагроз. Підвищення кількості дистанційних консультацій і збільшення обміну медичними даними через Інтернет зробили медичні установи вразливішими для хакерських атак. Відомі випадки, коли під час пандемії медичні заклади ставали жертвами атак вірусів-здирників, що паралізувало їхню роботу.

5.2 Використання телемедицини та загрози безпеці під час її впровадження

Телемедицина стала важливою частиною системи охорони здоров'я під час пандемії, але вона також принесла нові загрози. Віддалені консультації через незахищені

платформи можуть призвести до витоку конфіденційних даних. Для забезпечення безпеки телемедицини необхідно використовувати захищені платформи та шифрування під час відео- та аудіоконсультацій.

5.3 Як захищати дані пацієнтів під час віддалених консультацій

Забезпечення безпеки віддалених консультацій включає кілька етапів:

1. Використання тільки захищених медичних платформ для телемедицини.

2. Використання двофакторної аутентифікації для входу в системи.

3. Шифрування даних під час консультації, щоб уникнути перехоплення інформації третіми особами.

6. Підсумки та обговорення

6.1 Основні висновки щодо захисту інформації у охороні здоров'я

Інформаційна безпека в охороні здоров'я є критично важливою для захисту конфіденційних даних пацієнтів. Медичні установи повинні використовувати сучасні технології захисту, такі як шифрування, двофакторна аутентифікація та аудит доступу до даних. Безпека даних повинна бути забезпечена на всіх етапах — від збору інформації до її зберігання та передачі.

6.2 Завдання

- Які загрози для безпеки медичних даних, на вашу думку, є найбільш небезпечними?

- Як медичні заклади можуть підвищити кібербезпеку?

- Які методи захисту ЕМЗ ви вважаєте найбільш ефективними?

Ця лекція допоможе студентам зрозуміти важливість інформаційної безпеки у сфері охорони здоров'я та навчитися використовувати ефективні методи захисту даних пацієнтів.

Розробив

Старший викладач кафедри загальних дисциплін Павло КІЧУЛА