Розділ №6. Захист інформації в інформаційно-комунікаційних системах та робота з персональними даними у закладі охорони здоров'я

Тема 6.1 Основи кібербезпеки

6.1.1 Вступ

Інформаційна революція XX сторіччя та подальший невпинний розвиток інновацій в сучасному світі не залишає жодної сфери діяльності людства поза межами впливу новітніх інформаційних технологій. Сфера охорони здоров'я не є виключенням. Водночас разом з перевагами і новими можливостями від цифровізації сфера охорони здоров'я стикається зі значними викликами. Приватність та достовірність персональних даних пацієнтів є однією з важливих складових проблематики цифровізації галузі.

З одного боку, сфера охорони здоров'я має порівняно низький рівень уваги до проблематики захисту інформації в цифровому вигляді, а з іншого – галузь покладається на технології й інформаційний цифровий простір, який є спільним з іншими секторами економіки, включаючи фінансовий сектор та сферу державного регулювання. Це так само означає, що сфері охорони здоров'я треба за стислий термін пройти ті ж стадії еволюції в області безпеки інформації, що проходили й фінансовий сектор та державні органи протягом останніх п'ятдесяти років. Для розкриття базових понять безпеки інформації важливо спиратися на наступні терміни та визначення.

Визначення: ***Інформація***
Будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді (стаття 1 Закон України "Про інформацію").

Визначення: ***Захист інформації***
Сукупність правових, адміністративних, організаційних, технічних й інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Поняття захисту не обмежується цифровою формою інформації і як сфера знань виникла задовго до появи першого комп'ютера. Водночас саме загрози інформації в цифровому просторі є найбільш актуальними і масштабними. Відповідно, це вимагає від організацій сучасних підходів і заходів захисту інформації. Сталим терміном для захисту інформації в цифрових (комп'ютерних) технологіях є «кібербезпека».

Визначення: ***Кібербезпека***
Стан захищеності даних в електронному вигляді від їх несанкціонованого використання або кримінальних дій з цими даними, а також, набір заходів для досягнення такого стану захищеності даних.

В спрощеній інтерпретації, кібербезпека – це захист комп'ютерів, комп'ютерних мереж і програмного забезпечення від потенційних загроз, які можуть виникнути в процесі ведення діяльності.

Заклади охорони здоров'я (далі – ЗОЗ) в сучасному світі широко застосовують цифрові системи, щоб ефективно надавати медичну допомогу. Подібно до того, як захищаються фізичні об'єкти, необхідно захищати «цифрові» активи, тобто інформацію в електронному вигляді.

ЗОЗ відповідно до законодавчих і нормативних вимог несуть відповідальність за забезпечення безпеки даних пацієнтів для збереження їхньої довіри. Окрім того, ЗОЗ

повинні захищати свої цифрові активи та системи з метою забезпечення безперервності надання медичної допомоги пацієнтам та сталого функціонування важливих робочих процесів.

Навмисне втручання в роботу комп'ютерних систем, мереж або отримання несанкціонованого доступу до систем та даних визначено терміном «кібератака». Успішно виконана кібератака може призвести до розкриття, викрадення, видалення або зміни конфіденційних даних.

З огляду на це заклади і установи повинні впроваджувати політики та правила кібербезпеки, що допоможе знизити до мінімуму результати кібератак. Наслідками кібератаки можуть бути шкода репутації організації і погіршення фінансового становища. ЗОЗ повинні дотримуватись нормативних вимог для захисту конфіденційних даних пацієнтів, а також відповідати певним міжнародним вимогам, таким як Загальний регламент захисту даних (GDPR). Даний регламент вимагає від організацій, які володіють, обробляють та зберігають персональні дані громадян держав-учасниць ЄС вжити ряд заходів з кібербезпеки.

В області кібербезпеки фундаментальною задачею є розуміння, яка саме інформація обробляється і зберігається в організації, та від яких негативних факторів її необхідно захищати. Визначення цих критеріїв називається моделюванням загроз.

Типові загрози безпеці інформації – це загрози викрадення, пошкодження, змінення або знищення інформації. Крім того, цифрові медичні пристрої можуть бути зламані і це може завдати прямої шкоди пацієнтам.

Стан захищеності інформації визначають через наступні параметри – конфіденційність, цілісність та доступність інформації.

6.1.2 Конфіденційність, цілісність і доступність інформації

Отже, до складових кібербезпеки входить гарантування конфіденційності, цілісності та доступності цифрових активів.

Визначення: ***Конфіденційність інформації***
Властивість, яка гарантує те, що доступ до інформації можуть одержати тільки авторизовані особи або процеси.

Конфіденційна інформація передається від однієї людини до іншої під час ведення службових справ. Особа, яка отримала конфіденційну інформацію, повинна забезпечити її зберігання та обробку відповідно до умов, встановлених особою, яка надала згоду на передачу конфіденційної інформації (наприклад, обробку персональних даних) або вимог керівних документів стосовно захисту інформації, якщо конфіденційна інформація складає державну таємницю. Детальніше дане питання розглянуто у 6.4.1 Вступ.

Працівники ЗОЗ повинні знати про чутливий характер медичних і персональних даних, що отримує ЗОЗ у ході свого функціонування, розуміти та дотримуватись правил роботи з конфіденційною інформацією; утримуватись від розголошення таких даних. Для досягнення цієї мети слід проводити регулярні навчання всього персоналу, щонайменше раз на рік.

Визначення: ***Цілісність інформації***
Властивість, яка гарантує те, що інформація не містить помилок, є актуальною, вичерпною, будь-які зміни інформації здійснюються авторизованими особами або процесами.

Наряду з конфіденційністю, важливою властивістю медичної інформації пацієнта є цілісність, адже спотворені дані можуть призвести до лікарських помилок у лікуванні пацієнтів з дуже серйозними та навіть тяжкими наслідками.

Ще однією властивістю інформації, яку повинна забезпечувати кібербезпека, є доступність.

Визначення: ***Доступність інформації***
Властивість, яка гарантує те, що забезпечується своєчасний доступ авторизованих осіб і/або процесів до інформації, а також відсутні простої в процесі її обробки (тобто коли інформація знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і у той час, коли вона йому необхідна). У випадку втрати інформації існує можливість своєчасного її відновлення.

На практиці це означає, що лікар повинен мати можливість отримати доступ до цифрової медичної картки пацієнта або до медичної інформаційної системи, з правами доступу в межах своїх повноважень, саме тоді, коли йому це потрібно.

Доступність інформації забезпечується шляхом використання системи контролю доступу. Зазначена система повинна ідентифікувати кожного користувача відповідно до його ідентифікатора і запобігати доступу та використанню інформаційних ресурсів ЗОЗ неавторизованими користувачами. Система контролю доступу включає як внутрішні засоби захисту (паролі, шифрування даних, таблиці контролю доступу, налаштування інтерфейсів користувача тощо), так і зовнішні (пристрої захисту портів, брандмауери, автентифікацію на основі хоста тощо).

Для можливості відновлення даних пацієнтів, що зберігаються у ЗОЗ запроваджується система резервного копіювання. У разі створення резервних копій, ЗОЗ слід обов'язково проводити їх регулярну перевірку на предмет функціональності процедури відновлення даних з резервних копій.

Таким чином, забезпечення конфіденційності, цілісності та доступності інформації є першим базовим принципом кібербезпеки.

У травні 2017 року програмне забезпечення-вимагач WannaCry зашифрувало дані і файли на 230 000 комп'ютерах у 150 країнах, й порушило роботу Національної служби охорони здоров'я (NHS) Великобританії. Ключові системи були заблоковані, що перешкоджало доступу персоналу до даних пацієнтів і критичних послуг. Хоча атака WannaCry не була спрямована безпосередньо на NHS, постраждали й інші великі організації, зокрема Telefonica, FedEx, Nissan, та Банк Китаю. Проте найбільший негативний ефект від кібератаки відчула саме NHS.

Під час спостереження за системами охорони здоров'я в усьому світі стало очевидно, наскільки ця сфера вразлива до будь-якої кіберзагрози. Отже, кібербезпека ЗОЗ стає дуже актуальним питанням в період цифрової трансформації сфери охорони здоров'я України.

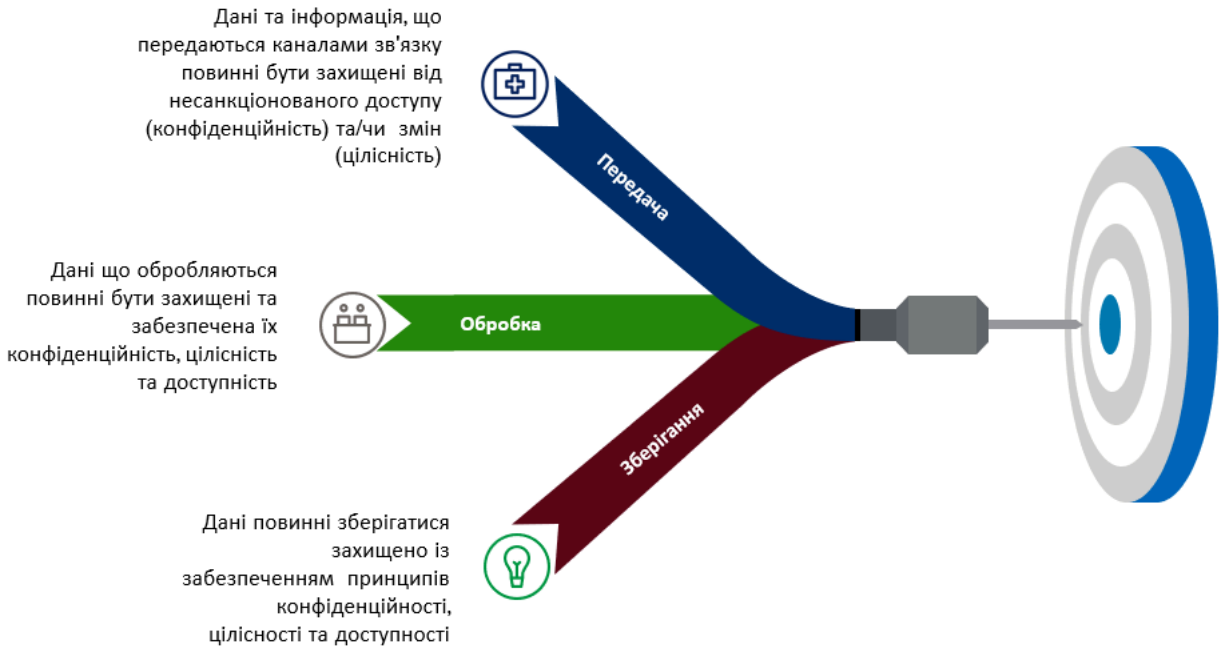
Відповідно до законодавчих і нормативних вимог керівництво ЗОЗ несуть повну відповідальність за підтримання належного рівня інформаційної безпеки ЗОЗ.

Визначення: ***Належний рівень інформаційної безпеки***
Стан фізичного, інформаційного середовища і сфери користувачів інформаційних та цифрових активів, який гарантує конфіденційність, доступність, цілісність інформації та спостережність і контрольованість систем/підсистем, в яких ця інформація циркулює.

У ЗОЗ необхідно впроваджувати і підтримувати організаційні та технологічні заходи для підтвердження того, що медичні дані пацієнтів та інша конфіденційна інформація не були змінені або знищені несанкціонованим чином. ЗОЗ повинен підтримувати впровадження автоматизованих систем та програмного забезпечення для автоматичної перевірки наявності людських помилок під час введення та обробки даних пацієнтів.

6.1.3 Захист інформації при передачі, зберіганні та обробці

Виходячи з визначення належного рівня інформаційної безпеки, а саме такого стану, який гарантує конфіденційність, доступність, цілісність інформації в організації необхідно зазначити, що є й інші важливі складові кібербезпеки. Для належного рівня кіберзахисту необхідно забезпечити спостережність і контрольованість систем та підсистем, в яких циркулює інформація. Це означає, що інформація повинна бути спостережна і захищена не тільки при її збережені, а також при передачі чи обробці (див. малюнок 1).



Малюнок 1. Спостережність та контрольованість інформаційних систем

Дані й інформація, що передаються каналами зв'язку повинні бути захищені від несанкціонованого доступу (забезпечена конфіденційність) та/чи змін (цілісність). Крім того, повинна бути забезпечена їхня доступність абонентам, які передають та отримують інформацію.

Дані й інформація, що обробляються, повинні бути захищені при обробці таким чином, щоб була забезпечена їх конфіденційність, цілісність та доступність.

Дані й інформація повинні зберігатися захищено, і у такий спосіб, щоб було забезпечено виконання принципів інформаційної безпеки із забезпечення конфіденційності, цілісності та доступності.

Спостережність – це властивість інформації бути захищеною весь час і на всіх етапах обробки. Отже, забезпечення захисту інформації на етапах передачі, обробки чи зберігання

є другим базовим принципом кібербезпеки. Він досягається за рахунок вмілого використання комплексу апаратних, програмних і технічних засобів, а також організаційних заходів, спрямованих на забезпечення захищеності інформації на всіх етапах обробки, передачі та зберіганні.

Зберігання і передача конфіденційної інформації має здійснюватися в зашифрованому вигляді. До конфіденційної інформації відноситься будь-яка інформація, яка може бути використана для ідентифікації особи та медичні дані пацієнта. Алгоритми і засоби, які використовуються для шифрування, мають відповідати вимогам, що встановлені Державною службою спеціального зв'язку та захисту інформації України.

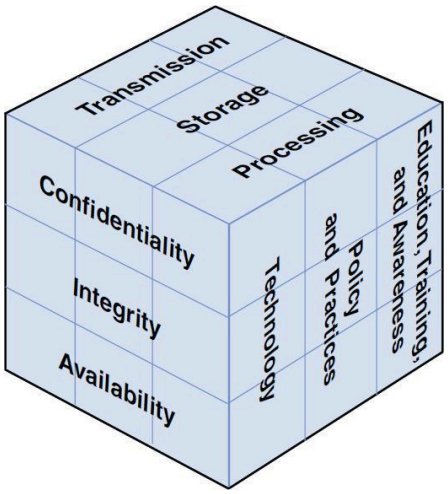
За сутністю заходи захисту інформації при передачі, обробці і зберіганні можна поділити на організаційні, фізичні, апаратні, програмні та апаратно-програмні, а також криптографічні. Ці заходи потребують використання певних засобів і технологій інформаційної безпеки, але в першу чергу, необхідно забезпечити правильну організацію та вміле застосування інформації користувачами. Отже, третя базова складова кібербезпеки – люди, процеси та технології.

Три принципи кіберзахисту (конфіденційність, цілісність, доступність) не існують ізольовано і впливають один на одного. Управління системою кібербезпеки включатиме пошук ефективного балансу цих факторів. Балансування різних факторів завжди пов'язано з управлінням.

Для управління системою кібербезпеки необхідно призначити відповідальну посадову особу. За належний рівень кібербезпеки організації відповідає керівник цієї організації, проте він/вона не зможе приділяти достатньо часу даному процесу, який потребує значної залученості, обізнаності та відповідної підготовки. Тому, в тих ЗОЗ, де визначено багато інформаційних активів та систем, що потребують захисту, керівник призначає окремого відповідального за кібербезпеку/інформаційну безпеку.

У кібербезпеці застосовується багатогранний комплексний підхід до запровадження і застосування методів та засобів кібербезпеки, який ще називається кубом кібербезпеки або кубом МакКамбера, що візуалізує комплексний підхід із забезпечення інформаційної безпеки та є широко відомим і зрозумілим у спільноті фахівців з кібербезпеки.

Куб МакКамбера — це спосіб оцінки системи безпеки з огляду на всі її аспекти, який був детально описаний у 2004 році Джоном МакКамбером у книзі «Оцінка та управління ризиками безпеки в IT-системах: структурована методологія». Куб кібербезпеки виглядає як тривимірна геометрична фігура, де однією з трьох видимих поверхонь є цілі кібербезпеки — конфіденційність, цілісність і доступність. Іншою спостережною поверхнею є стани інформації при передачі, обробці та збережені. Третя видима поверхня цього кубу відноситься до складових, пов’язаних з управлінням людьми, процесами і технологіями (див. малюнок 2).



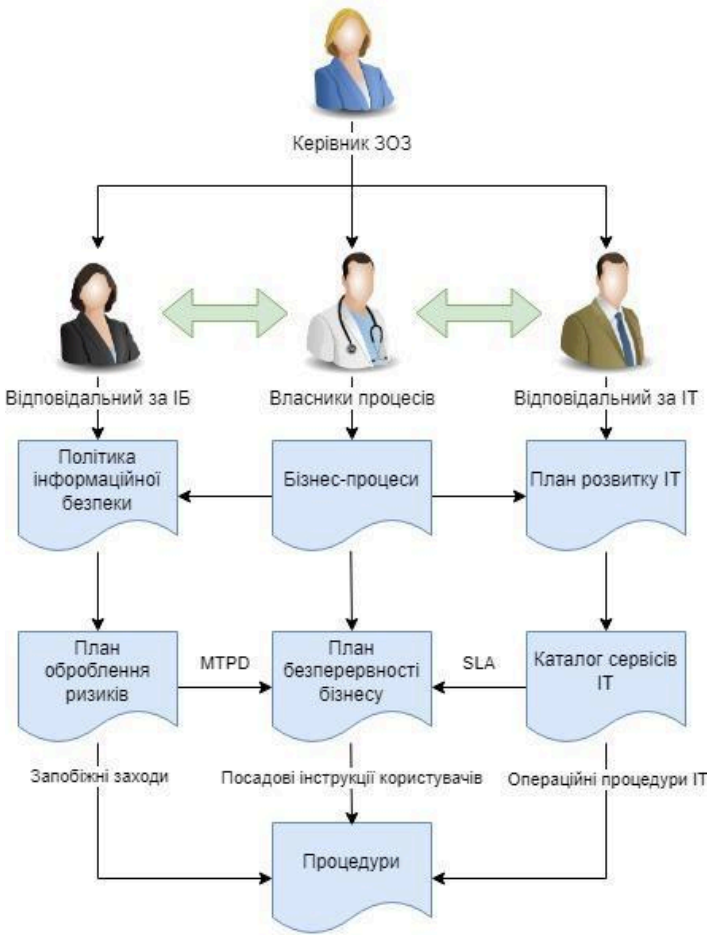
Малюнок 2. Куб кібербезпеки або куб МакКамбера

6.1.3.1 Люди

Визначення: ***Відповідальний за інформаційну безпеку (ВІБ) закладу охорони здоров'я***
Призначена посадова особа зі складу персоналу закладу, який/яка відповідає за дотримання належного рівня інформаційної безпеки ЗОЗ.

Зазначена посадова особа контролює всю поточну діяльність, пов'язану з розробкою, впровадженням та підтримкою політики інформаційної безпеки ЗОЗ, забезпечує дотримання належного рівня кіберзахисту, оптимізує методи цифрового захисту та ефективно використовує наявні ресурси.

Рекомендується, щоб відповідальний за інформаційну безпеку (далі – ВІБ) був заступник керівника ЗОЗ. Отже, така посадова особа буде мати достатньо повноважень для виконання функціональних обов'язків, пов'язаних із забезпеченням кібербезпеки. Зазвичай ВІБ та відповідальний за ІТ – це різні посадові особи (див. малюнок 3). Це пов'язано з різницею у завданнях. У відповідального за ІТ основним завданням є підтримання надання ІТ-сервісів та служб на відповідному рівні, який зазвичай визначається керівником або відповідним договором, який має назву Service-Level-Agreement (SLA).



Малюнок 3. Можливий розподіл відповідальності та повноважень щодо інформаційної безпеки між посадовими особами ЗОЗ

Зі свого боку ВІБ несе відповідальність перед керівництвом за безпеку інформаційних систем та цифрових активів (даних) ЗОЗ. У певний момент часу може скластися ситуація, коли з міркувань безпеки треба припинити надавати окремі ІТ-сервіси, щоб запобігти ризикам інформаційної безпеки. Саме таке протиріччя краще всього вирішується розподіленням повноважень та ескалацією прийняття відповідного управлінського рішення безпосередньо керівнику ЗОЗ.

ВІБ повинен надати керівнику відповідну інформацію про «Максимально допустимий період збою/відключення ІТ-системи» (англ. Maximum Tolerable Period of Disruption – MTPD). Він визначається, як максимально допустимий час, протягом якого ключові сервіси/послуги можуть не надаватися до того часу, поки це не призведе до неприйнятних наслідків.

Безумовно, обмежитись лише одним ВІБ для забезпечення кіберзахисту ЗОЗ неможливо. Щонайменше повинна бути сформована група реагування на інциденти інформаційної безпеки. Якщо ЗОЗ невеликий, з обмеженою кількістю інформаційних систем і цифрових активів, група може складатися з персоналу, який окрім виконання штатних обов'язків залучається до реалізації завдань з підтримання рівня інформаційної безпеки на належному рівні. Якщо ЗОЗ великий, з досить розвиненою ІТ-інфраструктурою, доцільно створювати штатну команду фахівців з кібербезпеки.

Забезпечення інформаційної безпеки ЗОЗ на належному рівні залежить від рівня обізнаності та підготовки персоналу ЗОЗ протистояти загрозам кібербезпеці. Більшість працівників ЗОЗ не освічені щодо сучасних загроз й існуючих рекомендацій з безпеки для захисту пристроїв, мереж та даних. Навчання працівників ЗОЗ принципам кібербезпеки дозволяє знизити ризики порушень політики інформаційної безпеки, що призводять до негативних наслідків. Відповідальність за організацію і проведення навчання персоналу покладається на функціональні обов'язки ВІБ.

6.1.3.2 Процеси

Підвищення обізнаності і навчання працівників принципам кібербезпеки – один з багатьох напрямів роботи ВІБ. Проте головним завданням ВІБ є побудова ефективної системи кіберзахисту. Це комплексне завдання, яке потребує багато знань і навичок у сфері кібербезпеки. Для практичної реалізації зазначеного завдання існують стандарти з кібербезпеки. Одним з таких загальноприйнятих стандартів з кібербезпеки є NIST Cybersecurity Framework («Рамкова модель кібербезпеки NIST»). Відповідно до стандарту кібербезпеку організації потрібно забезпечувати циклічно, виконуючи певні процеси (див. малюнок 4):

Малюнок 4. Забезпечення кібербезпеки відповідно до NIST Cybersecurity Framework

Ідентифікація. Відноситься до управління системами, людьми, активами, даними і ризиками. Цей процес поділяється на шість підпроцесів: управління активами, управління бізнес-середовищем, загальне управління процесами кібербезпеки, оцінка ризиків, управління ризиками і управління ризиками ланцюгів постачання.

Захист. Стосується насамперед захисту послуг і бізнес-процесів. Підпроцеси включають наступні категорії: керування ідентифікацією, автентифікація та контроль доступу, інформування і навчання, безпека даних, захист інформації та пов’язані з цим процедури, обслуговування й технології захисту.

Виявлення. Відноситься до подій інформаційної безпеки та ідентифікацію інцидентів. Цей процес включає моніторинг і виявлення загроз, пов’язаних з будь-якими нехарактерними діями чи аномаліями. Процес виявлення інцидентів і подій інформаційної безпеки складається з наступних етапів: забезпечення спостережності інформаційних систем і мереж, ідентифікація аномальних подій, моніторинг безпеки та покращення процесу виявлення.

Реагування. Це заходи, які вживаються при виявленні інциденту чи кібератаці. Цей процес розподіляється на п’ять підпроцесів, які слід враховувати при реагуванні на інцидент кібербезпеки: планування реагування, комунікації при реагуванні, аналіз інциденту, пом‘якшення наслідків і покращення процесу реагування.

Відновлення. Стосується роботи організації над тим, щоб зберігати стійкість під час атаки, а також відновити послуги, які зазнали впливу від події інформаційної безпеки. Відповідні заходи і план відновлення важливих бізнес-процесів мають бути підготовлені завчасно та повинні включати: планування відновлення, комунікації й процедури покращення.

Для того, щоб ці процеси запровадити, розподілити обов’язки і відповідальність між учасниками і користувачами інформаційних систем ЗОЗ, ВІБ розробляє та затверджує у керівника ЗОЗ Політику інформаційної безпеки.

Визначення: ***Політика інформаційної безпеки***
Визначає основні засади забезпечення інформаційної безпеки ЗОЗ, служить центральним програмним документом з інформаційної безпеки, який встановлює відповідні процедури і правила запровадження та виконання головного процесу побудови й підтримки на належному рівні системи управління інформаційною безпекою.

Головний процес забезпечення інформаційної безпеки організації складається із організації трьох рівнів захисту: фізичного, адміністративного та технологічного.

Фізичний рівень передбачає різні фізичні елементи, які запобігають вторгненню, — це охоронці, камери відеоспостереження, замкнені двері, системи біометричної перевірки тощо.

Адміністративний рівень включає всі політики, процедури, аудити, стандарти та протоколи, які зменшують ризики інформаційної безпеки. Політика паролів організації, багатофакторна автентифікація, дії працівників і регулярне навчання – усі ці заходи відносяться до забезпечення адміністративного рівня.

Нижче розглянуто **технологічний рівень** кіберзахисту і саме технології, які забезпечують цей рівень.

6.1.3.3 Технології

Технологічна складова кіберзахисту включає всі комп‘ютерні і програмні ресурси, які використовуються для забезпечення спостережності інформаційних систем та зменшення ризиків інформаційної безпеки.

Технічними компонентами технологічної складової є: антивірусне програмне забезпечення; системи управління доступом; засоби шифрування; сканери вразливостей; інструменти моніторингу і журнали подій; сегментація та зонування мережі; системи виявлення вторгнень; пісочниці; інструменти аудиту; брандмауери; інструменти глибокої перевірки пакетів; системи запобігання витоку інформації; засоби захисту від зловмисних програм; інструменти перевірки цілісності даних; інструменти аналізу поведінки; інструменти керування виправленнями та змінами.

Серед вищезазначених технічних компонентів деякі займають особливо важливі позиції у забезпеченні кіберзахисту ЗОЗ, тому потребують окремої уваги.

Антивірусний захист здійснюється за допомогою відповідного антивірусного програмного забезпечення (Антивірусне ПЗ), яке встановлюється на всьому робочому обладнанні і серверах ЗОЗ та періодично оновлюється. Антивірусне ПЗ повинно мати підтримку з боку розробника, можливості щодо передачі підозрілих файлів на аналіз відповідним фахівцям і мати можливості евристичного аналізу.

Контроль доступу до інформації та даних ЗОЗ здійснюється за допомогою відповідної системи. **Система контролю доступу** повинна визначати кожного користувача відповідно до його ідентифікатора і запобігати доступу та використанню інформаційних ресурсів ЗОЗ неавторизованими користувачами. Система контролю доступу включає як внутрішні засоби захисту (паролі, шифрування даних, таблиці контролю доступу, налаштування інтерфейсів користувача тощо), так і зовнішні (пристрої захисту портів, брандмауери, автентифікацію на кінцевому пристрою тощо).

Система резервного копіювання та відновлення або бекап система (англ. backup) – призначена для відновлення даних та програмного забезпечення у разі пошкодження або видалення. Створення резервної копії даних надає можливість виконати відновлення інформації/даних при втраті оригіналу, з якого було створено резервну копію, який ще називається об’єктом копіювання. Під втратою треба розуміти настання події, що призвела не тільки до знищення даних, а також неавторизованої зміни, після чого дані втратили цінність або цілісність.

Системи резервного копіювання поділяються на системи повного резервування (Full Backup - L0), які роблять повну копію об’єкту копіювання, та диференційного резервного копіювання (Differential Backup або L1), які здійснюють копіювання змін, що були зроблені після створення останньої повної резервної копії. Також можуть використовуватися додаткові резервні системи копіювання (Incremental Backup або L2) для копіювання змін, що відбулися з часу повного чи диференційного копіювання, якщо такі зміни важливі для забезпечення сталого функціонування системи.

Програмне забезпечення є одночасно і об’єктом захисту й інструментом, який застосовується для забезпечення інформаційної безпеки. Спеціалізоване програмне забезпечення використовується для моніторингу стану інформаційних систем, виявлення інцидентів, протидії вторгненню та витоку даних, а також для аналізу поведінки користувачів.

Існують певні загальні правила кібербезпеки щодо встановлення та використання програмного забезпечення. На внутрішніх комп'ютерах і мережах ЗОЗ має використовуватися лише дозволене до використання програмне забезпечення. Встановлення програмного забезпечення має відбуватись лише уповноваженою особою (адміністратором). Усе програмне забезпечення перед встановленням має пройти перевірку та отримати дозвіл від керівника ЗОЗ або ВІБ. Усі файли і програми, які були передані в електронному вигляді на комп'ютери або мережу ЗОЗ з іншого місця, повинні бути перевірені на віруси відразу після отримання. Програмне забезпечення, яке є критичним для підтримання безперервності бізнес-процесів підлягає резервному копіюванню.

Тема 6.2 Принципи запровадження кіберкультури

6.2.1 Вступ

Побудова системи кібербезпеки в організації передбачає ряд організаційних та технічних заходів. В тому числі, навчання і підвищення обізнаності серед широкого кола працівників організації. Саме недостатня обізнаність працівників і низький рівень загальної цифрової

грамотності стає «слабким місцем» в системі кібербезпеки організації. Про це добре відомо зловмисникам, які «професійно» спеціалізуються на комп'ютерних злочинах. З іншого боку, проінформований персонал створює перший ешелон захисту за допомогою дотримання простих повсякденних правил поведінки з інформацією в цифровому вигляді. Наявність спільного розуміння потреби в захисті інформації та знання простих правил для його підтримки – це ключові складові культури кібербезпеки в організації.

Визначення: ***Культура кібербезпеки***
Це набір припущень, уявлень, ставлення до предметної області, моделей поведінки та робочих звичок, які підсилюють кібербезпеку організації.

6.2.2 Поняття кібергігієни

Набір правил для повсякденної підтримки кібербезпеки для широкого кола працівників прийнято називати кібергігієною.

Визначення: ***Кібергігієна***
Сукупність практик і підходів, які користувачі комп'ютерних систем застосовують для підтримки "здоров'я" та безпеки інформації в таких системах.

На рівні широкого кола користувачів наступні правила кібергігієни виділяють як найбільш важливі:

- правило чистого столу та екрану;
- правила роботи з паролями;
- правила безпечної роботи з електронною поштою;
- правила безпечної роботи з мережею Інтернет;
- правила використання флеш-накопичувачів та інших змінних носіїв інформації.

6.2.3 Правила роботи з паролями

Користування паролями є важливою складовою роботи з будь-яким програмним забезпеченням. Водночас паролі є невід'ємною частиною інформаційної безпеки. Вони забезпечують захист облікових записів користувачів, користувацьких даних і доступу до них. Використання слабкого пароля на робочому місці може призвести до того, що сторонні особи отримають доступ до даних пацієнтів або іншої важливої службової інформації.

6.2.3.1 Вимоги щодо створення паролів

З метою створення надійних паролів, які складно підібрати, слід ознайомитися з наступними вимогами.

Варто уникати паролей з однією або декількома ознаками, що наведені нижче.

Пароль вважається не надійним, якщо:

- для створення паролю використана інформація, яка прямо асоціюється з користувачем (власником паролю);
- в якості паролю обрано день народження, власний номер телефону або іншу персональну інформацію, яку можна порівняно легко дізнатися (наприклад, знайшовши інформацію в довідниках або в соціальних мережах, резюме, персональних оголошеннях тощо);
- в якості паролю обрано ім'я та/чи прізвище іншої людини (родича або знаменитості);
- в якості паролю обрано ім'я казкового персонажу;
- в якості паролю обрано кличку тварини, яка є популярною/розповсюдженою;
- паролем є назва юридичної особи, торгової марки, спортивного клубу чи музичного

гурту;
- паролем є найменування сайту, апаратного або програмного забезпечення;
- пароль складається з одного словникового слова, яке застосовано без змін (написання слова відповідає написанню в словнику);
- пароль є регулярною послідовністю символів і цифр. Наприклад, 111111, abcde, qwerty;
- варіація перерахованих вище опцій, написаних у зворотному порядку;
- варіація перерахованих вище опцій, написаних із додаванням однієї цифри на початку або в кінці;
- варіація перерахованих вище опцій, написаних із додаванням одного знаку пунктуації;
- кількість символів в паролі недостатньо довга – сучасні дослідження доводять слабкість паролей довжиною меншою за 12 символів.

Примітка: Вимоги з вибору довжини паролю не менше 12 символів обумовлена наступними чинниками. В переважній більшості випадків для спроби підібрати пароль до облікового запису користувача, зловмиснику не потрібно знаходитися фізично біля робочого місця користувача. Також, зловмисники використовують високу ступінь автоматизації при підборі паролю. Спеціальне програмне забезпечення імітує дії користувача, перебираючи один можливий пароль за іншим на протязі днів, тижнів тощо. Окремі дослідження стверджують, що сучасні технології дозволяють порівняно швидко підібрати пароль, який має меншу довжину за 12 символів. Навіть, якщо всі інші рекомендації по вибору паролю враховано.

6.2.3.2 Поради по запам'ятовуванню складних паролів

Стійкий до підбору пароль має такі ознаки:

- містить як великі, так і малі літери;
- включає в себе декілька цифр;
- містить символи пунктуації або спеціалізовані символи (наприклад, % $ §* / &)
- має загальну довжину не менше 12 символів;
- не має ознак слабкого паролю, які було перераховано вище.

Хорошою практикою є вибір паролю, який одночасно є стійким до підбору і який можливо запам'ятати.

Одна з популярних технік для цього полягає в наступному. Пароль базується на довгій фразі, яку легко запам'ятати. Замість повних слів використовуються лише перші літери з кожного слова. Для стійкості в пароль додаються цифри та знаки пунктуації. Нижче наведено приклад:

Крок 1. Вибір фрази

The Beatles – Let it be

Крок 2. Вибір перших літер в словах

TBLib

Крок 3. Додавання цифр та знаків пунктуації

Отриманий пароль: TBLib-1970

Інша популярна техніка створення стійких паролів, які можливо запам'ятати, полягає в тому, щоб об'єднати в паролі декілька логічно не пов'язаних слів, змінивши їх написання і додавши цифри та спеціалізовані символи. Нижче наведено приклад:

Крок 1. Вибір довільних слів

хмарно мрія

Крок 2. Зміна написання слів

кмарно лрія

Крок 3. Додавання цифр та використання великих літер

кмаРно7 лРія2

Крок 4. Заміна окремих літер на символи, які схожі візуально

км@Рно7 лР!я2

Крок 5. Об'єднання окремих частин паролю

Отриманий пароль: *км@Рно7-лР!я2*

6.2.3.3 Рекомендації по використанню паролів

При роботі з паролями категорично **не рекомендується**:

- повідомляти пароль іншим особам, в тому числі особам, які представляються ІТ-спеціалістами;
- передавати особистий пароль колегам на час своєї відсутності, відпустки або відрядження;
- використовувати однаковий пароль для роботи та особистих цілей (напр., соціальні мережі);
- використовувати пароль, що схожий на попередній (при його зміні);
- використовувати пароль, який було надано адміністраторами – для первинного доступу до програмного забезпечення, без його подальшої безвідкладної зміни.

Примітка: Змінюйте паролі регулярно – принаймні один раз на рік для паролей від важливих службових програм, якщо частіший період не рекомендовано керівництвом ЗОЗ.

6.2.3.4 Рекомендації по зберіганню паролів

Якщо Ви скористалися одним з вищенаведених методів по створенню пароля, який можливо запам’ятати, і у Вас є можливість відновити пароль через стандартний робочий процес – не записуйте пароль взагалі.

Якщо з певних причин пароль необхідно записати, **уникайте наступних сценаріїв**:

- ніколи не записуйте паролі на наліпках з подальшим розміщенням на моніторі або у блокноті, який зберігається прямо на робочому місці у відкритому доступі;
- в інших місцях, де з паролем можуть ознайомитися сторонні люди;
- в електронному вигляді у комп'ютері або смартфоні.

Примітка: Для зберігання паролів існує спеціалізоване програмне забезпечення, наприклад: KeePass _https://keepassxc.org/ або 1Password _https://1password.com/

Використання текстових редакторів та програм для нотаток загального призначення для зберігання паролів **категорично не рекомендується**.

6.2.4 Рекомендації по безпечній роботі в мережі Інтернет

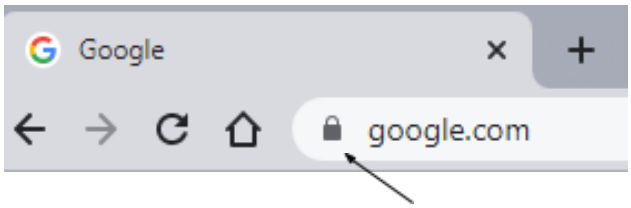
Мережа Інтернет надає безліч можливостей, але разом з тим, це є місцем, де користувач ризикує зіштовхнутися з безліччю кіберзагроз. Якщо бути уважним та дотримуватися кращих практик безпечної роботи, можливо захистити себе від злочинців.

6.2.4.1 Підроблені веб-сайти

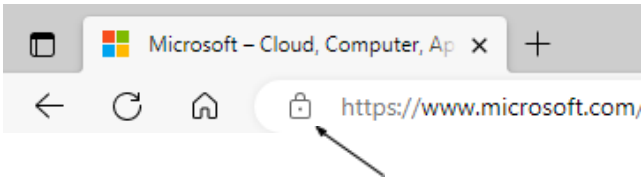
Зловмисники можуть різними способами заманити користувача на підроблений веб-сайт, який виглядатиме як точна копія оригіналу (копія порталу новин, соціальної мережі тощо). Головною відмінністю підробленого сайту буде його адреса. Але зловмисники намагатимуться зробити її дуже схожою на оригінал (наприклад, facelook.com, gooogle.com тощо).

6.2.4.2 Захищене підключення до веб-сайтів

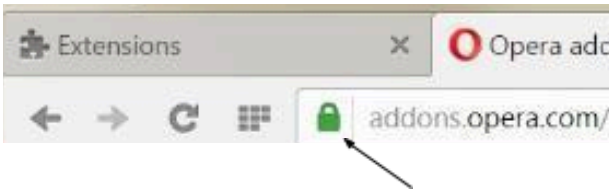
Переважна більшість комерційних і майже всі державні веб-сайти забезпечують технологію захищеного інтернет-підключення. Для того, щоб користувач міг впевнитися в цьому, розробники популярних програм для перегляду інтернет-сайтів (так звані, веб-браузери) виводять допоміжну інформацію поряд з адресою сайту, зазвичай у вигляді іконки замкненого замка (див. малюнки 5 – 7).



Малюнок 5. Іконка замкненого замка у веб-браузері Google Chrome



Малюнок 6. Іконка замкненого замка у веб-браузері Microsoft Edge



Малюнок 7. Іконка замкненого замка у веб-браузері Opera

Якщо немає впевненості, що сайт забезпечує технологію захищеного інтернет-підключення, будьте уважні і не вводьте жодні персональні, платіжні дані або пароль. Водночас захищене підключення ще не є гарантією того, що це не шахрайський сайт. Це значно ускладнює задачу створення шахрайського сайту, але не робить її неможливою.

6.2.4.3 Перевірка Інтернет-посилань

У разі сумнівів щодо надійності окремо взятого сайту можна скористатися безкоштовними Інтернет-сервісами для перевірки репутації того чи іншого веб-ресурсу. Розберемо цю задачу на прикладі сервісу Url Scan.

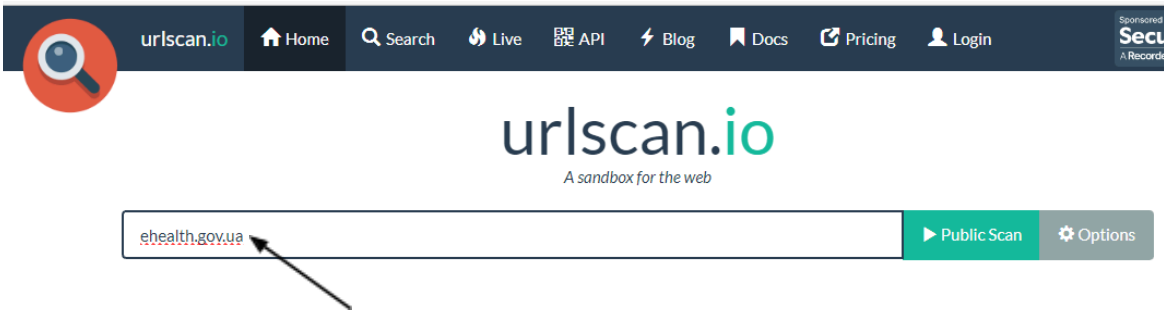
Крок 1. Скопіюйте адресу веб-сайту, репутацію якого треба перевірити, в «буфер обміну». Для цього виділіть текст адреси. Після чого, одночасно натисніть дві клавіши

на клавіатурі: «Ctrl» та «c».

Крок 2. Відкрийте веб-сервіс Url Scan за допомогою посилання https://urlscan.io/ (див. малюнок 8)

Малюнок 8. Фрагмент головної сторінки веб-сервісу Url Scan

Крок 3. Введіть адресу сайту у веб-сервіс Url Scan (див. малюнок 9)

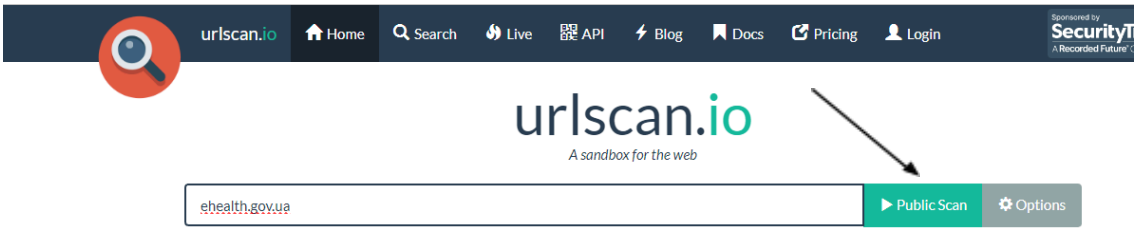


Малюнок 9. Перевірка адреси сайту у веб-сервісі Url Scan

Для цього, виконайте клік лівою клавішею мишки на полі для вводу адреси.

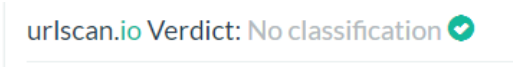
Після чого, одночасно натисніть дві клавіші на клавіатурі: «Ctrl» та «v».

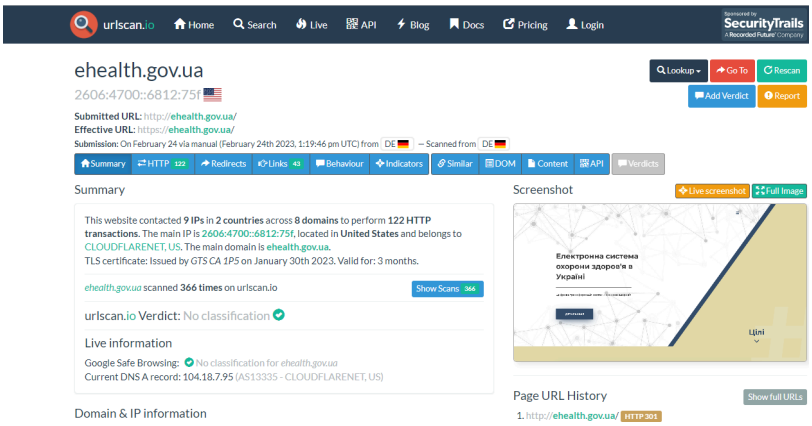
Крок 4. Натисніть зелену кнопку «Public Scan» (див. малюнок 10)



Малюнок 10. Перевірка адреси сайту у веб-сервісі Url Scan

Крок 5. Проаналізуйте аналіз сканування (див. малюнки 11-12)





Малюнки 11-12. Приклади результатів сканування

Ключовий рядок в результатах сканування – це «**urlscan.io Verdict**». У випадку, якщо на сторінці з результатами сканування у полі «urlscan.io Verdict» вказано значення **"malicious"** використання даного веб-сайту несе **ризики** для Вашої кібербезпеки!

6.2.4.4 Рекомендації при роботі з веб-браузером

Популярні програми для перегляду інтернет-сайтів (так звані, веб-браузери) самостійно оновлюють себе для підвищення захисту від вірусів, без участі користувача. Тому, використання популярних веб-браузерів дає користувачу додаткову перевагу.

Будьте обережні при встановленні додаткової функціональності в браузерах, так званих, add-on. Ці компоненти зазвичай є продуктами сторонніх розробників. В останніх можуть бути обмежені ресурси для підтримки їхньої безпеки та своєчасного випуску оновлень, порівняно з розробниками самих веб-браузерів. Вони можуть стати «слабким місцем» в безпеці роботи користувача в мережі Інтернет. Тому, не встановлюйте жодної додаткової функціональності в браузер, яка не потрібна для виконання робочих задач.

6.2.4.5 Рекомендації щодо використання проксі-ресурсів

Не рекомендується використання програмного забезпечення і веб-сайтів з метою приховування своєї діяльності в мережі Інтернет. До таких дій іноді звертаються працівники, які бажають використовувати службове Інтернет-з'єднання з робочого місця не за призначенням.

Визначення: ***Анонімайзер***
Веб-сайт, який допомагає користувачу опосередковано отримати доступ до інших інтернет-сайтів, приховуючи свою особистість.

Веб-сайти «анонімайзери» зазвичай створюються та підтримуються шахраями з метою крадіжки паролів, а також персональних даних і фінансової інформації користувача. Навіть при використанні таких «анонімайзерів» без введення особистих даних на сайті, виникає ризик для всієї інформації, що зберігається на робочому комп'ютері та в робочій комп'ютерній мережі.

6.2.4.6 Рекомендації при роботі з Wi-Fi мережею

У випадку необхідності використання робочих систем за межами приміщень установи може постати потреба у підключенні до мережі Інтернет.

Категорично не рекомендується підключатися до публічних безпровідних Wi-Fi мереж, маючи на комп'ютері або смартфоні службову інформацію.

Це є дуже небезпечним сценарієм, оскільки більшість таких мереж не гарантують захист від копіювання інформації або її викривлення. Окремим сценарієм є випадки, коли зловмисники створюють шахрайські публічні точки доступу до мережі Інтернет через Wi-Fi мережу з метою крадіжки паролів і цінних даних. Такі мережі можуть мати назву кафе та інших закладів поблизу, що вводить користувачів в оману.

Кіберзлочинці налагоджують фейкові безпровідні точки доступу, що дає їм можливість перехоплювати конфіденційну інформацію, наприклад, банківські реквізити, дані платіжних карток тощо.

Щоб вберегти себе від проникнення злочинців до персональних даних через публічну Wi-Fi мережу рекомендовано:

- вимкнути функцію автоматичного підключення до доступних безпровідних мереж;
- не виконувати робочі задачі та не вводити персональну чи платіжну інформацію при підключенні до мережі Інтернет через публічну Wi-Fi мережу.

6.2.4.7 Рекомендації по роботі з електронною поштою

Наступні рекомендації покликані зменшити ризик витоку конфіденційних даних через кіберзагрози, пов'язані з використанням робочої електронної пошти:

- не використовуйте корпоративну електронну пошту для відправки і отримання повідомлень, не пов’язаних із виконанням ваших посадових обов’язків. Також не використовуйте особисту пошту для робочого листування. Якщо не дотримуватися цього правила, Ви не можете бути впевнені, хто може мати доступ до ваших особистих і робочих даних. IT-відділ може бачити Вашу особисту переписку, а провайдери поштових сервісів — службову;
- бажано завести дві особисті поштові адреси для різних задач. Одну електронну пошту для підписок і реєстрацій в різних сервісах, іншу – для особистої переписки. Так адреса для особистої переписки не буде фігурувати в мережі Інтернет, а на Вашу особисту пошту буде приходити менше спаму;
- не зберігайте важливі документи в пошті довше необхідного часу – видаляйте їх після того, як потреба в них зникне;
- рекомендовано розглянути можливість використання програмного забезпечення для шифрування файлів перед відправкою електронною поштою за межі Вашої установи. Це застосовується для файлів з конфіденційною інформацією і в тих випадках, коли з отримувачем можна домовитися про такий порядок обміну файлами;
- остерігайтеся фішингових листів (див. розділ 6.2.5 Фішинг як одна з найпоширеніших загроз інформації);
- прикладом широко доступного програмного забезпечення з можливістю шифрування є архіватори з функцією захисту архіву паролем. Вміст архіву в такому випадку шифрується. Прикладом є популярний архіватор WinZip. Варто зауважити, що використання цього методу без попереднього погодження з отримувачем може мати негативні наслідки. Отримання архівів з паролем є підозрілим вмістом і буде розцінено відповідним чином;
- остерігайтеся листів, що можуть містити файли зі шкідливим програмним забезпеченням.

Примітка. Найбільш ризиковані типи файлів, на які треба звертати увагу при роботі з поштою:

- архіви файлів, особливо захищені паролем. Популярні розширення архівних файлів: .sfx, .zip, .7z, .rar;
- файли, які є програмним забезпеченням, наприклад, файли з розширенням .exe, .com, .cmd, .bat, .ps1, .swf, .jar, .js, .vbs;
- документи, що містять макроси, наприклад, файли з розширенням .docm, .xlsm, .pptm;
- файли векторної графіки з вбудованим кодом: .svg.

Перш ніж відкривати вкладений файл, перевірте файл на спеціалізованих публічних сервісах, наприклад: _https://virustotal.com/. Даний веб-сайт пропонує можливість завантажити файл для перевірки його безпечності. Веб-сайт має безкоштовну функціональність, яка доступна без реєстрації.

6.2.4.8 Правило порожнього робочого столу

Визначення: ***Правило порожнього робочого столу***
Під правилом порожнього робочого столу розуміють напрацювання звички не залишати жодні документи та цифрові носії інформації після завершення робочого дня або під час тривалої відсутності на безпосередньому робочому місці

Метою зазначеного правила є запобігання сценарію, коли з конфіденційним службовим документом ознайомиться особа, яка має фізичний доступ до Вашого робочого місця, але не має права доступу до документу, який лежить на столі. Прикладом такої особи може бути працівник, який прибирає приміщення або навіть сторонній відвідувач.

Похідним від правила порожнього робочого столу є правило порожнього екрану, яке передбачає закриття програм та електронних документів у Вашому робочому комп'ютері після завершення роботи з ними.

6.2.5 Фішинг як одна з найпоширеніших загроз інформації

6.2.5.1 Поняття фішингу

У кожному секторі економіки і в кожній країні працює правило: “користувач – це найбільш вразлива ланка ланцюга захисту інформації в організації.” Широке коло користувачів, професія яких не пов'язана безпосередньо з комп'ютерними технологіями, має обмежені знання про кіберзагрози інформації. Організована кримінальна спільнота, навпроти – має доступ до високо-технологічних інструментів і методик для скоєння комп'ютерних злочинів. В цих умовах постає гостра потреба в підвищені обізнаності медичних працівників з питань кібербезпеки.

Окрім технічних засобів, зловмисники активно використовують проти користувачів психологічні маніпуляції. Вони націлені на вразливість людини – довірливість, необачність, схильність до нелогічних дій у стані паніки або обурення. Цим психологічним прийомам сотні років, проте сьогодні з ними можна зіштовхнутися при роботі з комп'ютером, а не при живому спілкуванні. В таких умовах користувач вважає, що знаходиться в контрольованому та безпечному середовищі, і проявляє меншу обережність.

Серед вищезгаданих методів маніпуляції превалює «фішинг». Термін має англомовне походження – від англ. “рибалка”. Зазвичай жертва отримує “приманку” та “клюнувши на

неї" виконує дії, на які розраховує зловмисник. Результатом цих дій зазвичай стає отримання зловмисником конфіденційної інформації. Контакт з жертвою зазвичай встановлюється через електронну пошту, соціальні мережі або месенджери.

Визначення: ***Фішинг***
Техніка, яка направлена на отримання чутливої інформації, наприклад, деталі банківських рахунків, персональних даних тощо, шляхом шахрайських дій і введення користувача в оману, використовуючи при цьому комунікацію через електронну пошту або веб-сайти, видаючи особистість відправника за вартий довіри контакт з робочого оточення чи бізнес-середовища.

Як було зазначено, кінцева мета фішингу – це отримання конфіденційних даних. Нижче наводиться короткий огляд інформації, яка є пріоритетною для зловмисників.

6.2.5.2 Дані, за якими «полюють» зловмисники

У більшості випадків зловмисників найбільше цікавить наступна інформація ЗОЗ:

- списки імен, адреси електронної пошти, номери мобільних телефонів пацієнтів та адреси проживання;
- інформація про стан здоров'я та призначене лікування пацієнтів – особливо цінною є інформація, яка впливає на рішення суду (наприклад, психічний стан пацієнта) або факти, якими можна легко шантажувати пацієнта (наявність хвороби, яку негативно сприймає соціум – ВІЛ, наркоманія та інше);
- списки імен і посад співробітників, організаційна структура ЗОЗ, телефони співробітників (в тому числі, внутрішні телефонні номери);
- технічні засоби і програмно-апаратне забезпечення ЗОЗ;
- інформація про підрядників ЗОЗ;
- вся інформація, що Ви публікуєте особисто або Ваші друзі/колеги публікують про Вас у мережі Інтернет, може бути використано зловмисникам проти Вас. Чим більше інформації має злодій, тим вища ймовірність успіху в реалізації злочину.

6.2.5.3 Рекомендації по боротьбі з фішингом

Наступні рекомендації направлені на протидію фішингу через канал електронної пошти.

Необхідно відноситися з особливою обережністю та недовірою до електронних листів, які мають наступні ознаки:

- лист від невідомого відправника;
- лист від відомого відправника, але з поштової адреси, яка відрізняється від попереднього листування (зокрема частина адреси після символу @). Звертайте особливу увагу на листи від відправників, адреса яких не закінчується на .ua (реєстрація адреси в Україні);
- терміновість – фішингові повідомлення часто закликають до швидких дій, залишаючи менше часу на роздуми. Часто автор листа видає себе за керівний орган або підрозділ для підвищення відчуття терміновості;
- помилки в тексті або незвична побудова фраз – часто злочинці не говорять українською і використовують перекладачі;
- повідомлення, що написано іноземною мовою;
- пропозиція, від якої важко відмовитися – рекламні повідомлення дуже часто є фішинговими;

- лист з інтригуючою інформацією, який начебто помилково потрапив до Вас, наприклад, зарплатна відомість керівника, список працівників запропонованих до підвищення тощо;
- листи, в яких не згадується Ваше імя, які не адресовані особисто Вам, проте написані по шаблонній формі, наприклад, «Шановний клієнт» тощо;
- текст підпису з контактами відправника в кінці листа не відповідає фактичному відправнику листа або його поштовій адресі;
- запит на надання особистої інформації, в тому числі, шляхом запрошення до заповнення онлайн-форм через веб-посилання в листі;
- лист, який містить вкладені файли;
- лист, який пропонує перейти за посиланням або натиснути курсором “мишки” на зображення в електронному листі.

До підозрілих листів застосовуйте правило 30 секунд (див. розділ 6.2.5.4 Правило 30 секунд).

6.2.5.4 Правило 30 секунд

Якщо лист викликає підозри дайте собі 30 секунд на аналіз, не реагуйте на лист протягом цього часу. Від того, наскільки уважними Ви будете, залежить чи втратите Ви свою інформацію, чи ні.

Не поспішайте відкривати приєднані до електронного листа файли або переходити за посиланням в тексті листа.

У випадку сумнівів запитайте поради у керівника, чи IT спеціаліста Вашої установи.

Якщо лист надіслано від знайомого відправника, але має ознаки підозрілого – зв'яжіться з відправником альтернативним каналом зв'язку для підтвердження, що лист надіслав дійсно він.

6.2.5.5 Перевірка Інтернет-посилань

Перед відкриттям інтернет-посилання підведіть мишку до посилання не натискаючи курсором на нього. Ви побачите спливаючий рядок зі справжнім інтернет-посиланням, яке може відрізнятися від тексту посилання, яке Ви бачите спочатку в листі. Підведіть курсор та оцініть, чи не викликає адреса у Вас підозри.

Наприклад, посилання мало б перевести Вас на сайт української державної установи. При цьому справжня адреса посилання містить сайт, який завершується на “.ru”, отже велика ймовірність, що це фішинг.

Перш ніж переходити за посиланням, Ви також можете скористатися перевіркою репутації веб-сайту (сайт з безкоштовною функціональністю, доступний без реєстрації):

_https://urlscan.io/ — перевірка інтернет-посилання на шкідливий вміст

Детальніше питання розкрито в розділі 6.2.4.3 Перевірка Інтернет-посилань.

6.2.5.6 Протидія психологічній маніпуляції під час фішингу

Знання того, які сценарії шахрайства можливі, значно підвищує стійкість користувача до них. Нижче наведено важливі емоційні стани, які зловмисники намагаються викликати у користувача для власних цілей:

1. **Почуття відповідальності перед керівництвом**: співробітник більш охоче йде на співпрацю зі зловмисником, якщо той повідомляє про «термінове доручення від керівництва»;

2. **Страх:** страх провинитися перед керівництвом або страх перед комп'ютерними технологіями і небажання розбиратися в рекомендованих підходах до роботи з комп'ютером може підштовхнути користувача до необдуманого кроку;
3. **Сором: с**ором зізнатися в недостатності комп'ютерних знань і, як результат, несвоєчасне звернення за кваліфікованою допомогою;
4. **Доброта:** надмірна доброта і альтруїзм можуть спонукати людину надати допомогу, поступаючись звичайними правилами безпеки або втрачаючи пильність.
5. **Цікавість:** ще одне дуже вразливе місце, адже кому буде не цікаво подивитись на помилково відправлену вам зарплатну звітність або фотографії з корпоративної вечірки, на яку ви не змогли потрапити?

Для досягнення поставленого результату зловмисники можуть вдаватися до таких технік:

- представлятися іншою особою;
- відволікати увагу;
- нагнітати психологічну напругу.

У разі виявлення підозрілого листа одразу зверніться до Вашого керівника та/або до ІТ-фахівців, які обслуговують Вашу організацію.

6.2.5.7 Інші різновиди маніпуляцій

Окрім методу фішингу через канал електронної пошти, зловмисники застосовують інші канали та методи, що описані нижче.

Один з них «вішинг» — від англ. „voice“ та „fishing“.

Визначення: ***Вішинг***
Це різновид фішингу, але контакт з користувачем встановлюється за допомогою засобів голосового зв'язку (дзвінок по телефону або засобами Інтернет-телефонії). Зловмисник представляється колегою з іншого відділу/співробітником технічної служби/діловим партнером або клієнтом. Часто такий різновид фішингу застосовується в комплексі з попередніми видами атак.

Іншою технікою, яка вимагає доступу зловмисника до фізичного місця роботи користувача є «підкидання» флеш-накопичувача зі шкідливим вмістом.

Зазвичай, це робиться на вході до будівлі організації. Зловмисники хочуть створити видимість, що флеш-накопичувач загубив хтось із персоналу організації. Іншими популярними місцями є парковки, столові, вбиральні та робочі місця співробітників. На жаль, працівники ЗОЗ не завжди можуть бути впевнені в тому, що пацієнт, який зайшов до їх кабінету не є зловмисником.

Коли співробітники організації знаходять подібний флеш-накопичувач, вони або бажають його присвоїти, або знайти володаря. В обох сценаріях співробітник забажає перевірити вміст флеш-накопичувача, для чого під’єднає його до комп'ютера. Саме цієї поведінки очікує зловмисник. Флеш-накопичувач містить шкідливе програмне забезпечення. В найгіршому випадку це програмне забезпечення зможе приховано контролювати комп'ютер або знищити всю інформацію на ньому.

Для того, щоб співробітник не став чекати повернення додому, а застосував флеш-накопичувач саме в робочий комп'ютер, зловмисники вдаються до додаткових хитрощів. Наприклад, наносять на флеш-накопичувач напис “Бухгалтерія” або “Зарплатна відомість”.

Тема 6.3 Автоматизоване робоче місце працівника сфери охорони здоров‘я

6.3.1 Вступ

Багато з перерахованих в даній темі завдань покладаються на працівників, яких в ЗОЗ призначено відповідальними за підтримку ІТ-технологій. Тому роль користувачів автоматизованих робочих місць ЗОЗ зводиться до розуміння базових понять з метою того, щоб своєчасно та коректно повідомити про можливі проблеми відповідальну особу за підтримку ІТ-технологій ЗОЗ.

6.3.2 Рекомендації щодо антивірусного захисту

Наявність засобів антивірусного захисту є обґрунтованою та нагальною потребою для будь-якої комп'ютерної станції, яка використовується для службових потреб. За виключенням випадків, коли комп'ютер повністю ізольовано від зовнішніх мереж та зовнішніх носіїв інформацій. Нижче наведено базові рекомендації з антивірусного захисту.

6.3.2.1 Поняття шкідливого програмного забезпечення

Організовані кримінальні групи певною мірою використовують спеціальне програмне забезпечення для скоєння комп’ютерних злочинів. Це програмне забезпечення може бути створене індивідуально однією кримінальною групою або складатися з компонентів, які продаються і купуються на «чорному» ринку. Таке програмне забезпечення прийнято називати зловмисним, або шкідливим програмним забезпеченням (далі — ПЗ).

Враховуючи мету кінцевого результату, виділяють такі поширені категорії комп’ютерних вірусів:

- **ПЗ-вимагачі** – віруси, які вимагають викуп у атакованої організації, наприклад, шляхом спотворення робочої інформації з подальшим шантажем організації щодо її відновлення; та/або крадіжки робочої інформації і шантажу атакованої організації наміром опублікувати вкрадену інформацію у загальному доступі або продажі інформації на «чорному» ринку.
- **ПЗ-вейпери** – віруси, які націлені на знищення або спотворення інформації.
- **ПЗ-майнери** – віруси, які використовують комп'ютерні ресурси жертви для отримання криптовалюти (вид цифрової валюти, емісія та облік якої виконується децентралізованою платіжною системою повністю в автоматичному режимі, без можливості внутрішнього або зовнішнього адміністрування).
- **ПЗ-шпигуни** – віруси, які крадуть інформацію та приховано управляють комп'ютером.
- **Рекламне ПЗ** – віруси, які направлені на несанкціонований показ реклами користувачам та перенаправлення користувачів на рекламовані веб-сайти.

Для того, щоб добитися завантаження та запуску шкідливого програмного забезпечення на комп'ютерних системах атакованих організацій зловмисники використовують різні тактики. Нижче описано найбільш поширені з них.

6.3.2.2 Поняття комп'ютерного вірусу

За аналогією з живою природою, характерною рисою комп’ютерного вірусу є здатність «інфікувати» нові комп'ютерні системи при контакті з ними.

Визначення: ***Комп’ютерний вірус***
Вид шкідливого програмного забезпечення, яке здатне автоматично поширювати власні копії від одного комп'ютера до інших, з якими перший комп'ютер взаємодіє.

За технологією зараження комп’ютерні віруси поділяють на такі категорії:

- **Файлові** — інфікують файли з розширеннями «.exe» або «.com».
- **Макровіруси**, що вбудовуються в програми для роботи з текстами або електронними таблицями. Прикладом є Microsoft Word (.doc) та Microsoft Excel (.xls).
- **Скриптові** — підвид файлових вірусів, які написані на мовах скриптів (vbs, JavaScript, bat, php тощо). Цей тип здатний інфікувати інші формати файлів, наприклад, HTML.
- **Завантажувальні** — атакують завантажувальні сектори змінних носіїв (диски, дискети та флеш-накопичувачі) та заражають комп'ютер під час підключення пристрою до нього.

6.3.2.3 Троянські програми як різновид шкідливого програмного забезпечення

Визначення: ***Троянський кінь***
Вид шкідливого програмного забезпечення, яке для потрапляння на цільову комп'ютерну систему потребує активних дій користувача. Для спонукання користувача до цих дій використовується тактика «троянський кінь» по аналогії зі стародавньою легендою про військову атаку на місто Троя та підступним подарунком у вигляді статуї коня.

Як зазначено вище, шкідливе програмне забезпечення, яке діє по принципу «троянський кінь» часто використовується як неформальний термін «троян» та передбачає, що користувач здійснить очікувані зловмисником дії в комп'ютерній системі (завантажить файл, відкриває інтернет-посилання тощо). Одним з поширених методів розповсюдження даного типу шкідливого програмного забезпечення є «фішинг». Детальніше питання розкрито в розділі 6.2.5 Фішинг як одна з найпоширеніших загроз інформації

6.3.2.4 Засоби антивірусного захисту

Для боротьби зі шкідливим програмним забезпеченням існує широкий асортимент засобів антивірусного захисту, орієнтований на різний спектр організацій, як за розміром, так і за сектором економіки.

Наприклад, компонент антивірусного захисту Windows Security входить у пакет популярної комерційної операційної системи Microsoft Windows (для версій операційної системи Windows 10 і 11). Даний компонент забезпечує базовий рівень захисту. Багато організацій витрачають додатковий бюджет на придбання систем антивірусного захисту операційних систем Microsoft Windows від інших виробників.

Категорично не рекомендується використання неліцензійних копій систем антивірусного захисту.

Такі системи самі представляють джерело загрози для комп'ютерної системи і є шкідливим програмним забезпеченням на глибокому рівні.

Поява нових видів шкідливого ПЗ та нових модифікацій існуючого шкідливого ПЗ відбувається щодня. В зв'язку з цим, **рекомендується** забезпечити налаштування періодичного оновлення систем антивірусного захисту в частині бази даних відомих зразків шкідливого ПЗ. Таким чином, система антивірусного захисту буде підготовлена до боротьби зі шкідливим ПЗ, яке отримало розповсюдження останнім часом.

6.3.3 Рекомендації з оновлення програмного забезпечення

Кожна людина помиляється і це частина нашої природи, але саме цими помилками користуються злочинці. Варто зауважити, що чим складніше продукт людської праці, тим вище ризик помилки. Це повною мірою стосується програмного забезпечення. Не дивлячись на велику кількість етапів контролю якості під час розробки програмного забезпечення, жодна компанія-розробник не здатна випустити програмне забезпечення (ПЗ), в якому повністю відсутні помилки.

Деякі помилки в роботі ПЗ виявляються лише під час неочікуваної поведінки користувача. Наприклад, користувач вводить в поле для прізвища послідовність з 1000 літер. Якщо в ПЗ не передбачена така поведінка, то може виникнути помилка, яка своєю чергою порушить роботу інших елементів ПЗ, в тому числі, блоку, що контролює правильність паролю або інші механізми безпеки.

Для кращого розуміння важливості та масштабів проблеми приведемо приклад. Microsoft, виробник найпопулярнішої у світі операційної системи Windows, публікує інформацію про помилки у своєму ПЗ, що впливають на безпеку, щотижня. Велика частка організацій застосовує ці оновлення із запізненням, чим наражає свої комп'ютерні системи на значні ризики.

Варто зазначити, що виробники ПЗ ранжують свої оновлення безпеки за важливістю.

Також рекомендуємо увімкнути автооновлення (Auto-Update) в операційній системі Windows Вашого особистого комп’ютера. На службовому комп’ютері таку процедуру для Вас повинен зробити відповідальний IT спеціаліст.

Отже, ПЗ та додатки періодично оновлюються не тільки для покращення їх роботи, але й для «закриття» вразливостей і підвищення надійності систем безпеки, що допомагає захиститися від кіберзлочинців.

Щоб оновлення програмного забезпечення та додатків не заважало роботі, можливо обирати в якості часу встановлення оновлень години поза графіком робочого дня, за умови, що пристрій підключено до електромережі та мережі Інтернет.

Рекомендується використовувати лише ліцензійне програмне забезпечення. Оскільки неліцензійні копії ПЗ дуже часто містять в собі приховане шкідливе програмне забезпечення.

На жаль, в Україні має місце поширене використання так званих “піратських” або неліцензійних версій програмного забезпечення.

Якщо Ви використовуєте смартфон для доступу до робочої інформації, наприклад, до електронної пошти, важливо дотримуватися режиму частого періодичного оновлення ПЗ на цьому мобільному пристрої в тому числі.

Коли на екрані Вашого гаджета з'являється смс-повідомлення про те, що треба оновити ту чи іншу програму, не ігноруйте такі повідомлення. Витрачаючи декілька хвилин на оновлення, Ви «оздоровлюєте» Ваш пристрій і гарантовано зменшуєте ризики виникнення неприємних ситуацій в майбутньому.

6.3.4 Безпечна роботи з кваліфікованим електронним підписом

Сьогодні порядок і організація електронного документообігу, а також правовий статус та використання електронного підпису визначаються Законом України «Про електронні довірчі послуги» (далі — Закон), який набрав чинності 7 листопада 2018 року.

Одним із важливих нововведень Закону є те, що він запроваджує поняття «кваліфікований електронний підпис», яке замінило термін «електронного цифрового підпису».

Визначення: ***Кваліфікований електронний підпис (КЕП)***
Удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа. КЕП гарантує захист інформації від її випадкової чи умисної модифікації (зміни, спотворення) або знищення під час обробки та обміну в електронній системі.

Процедура формування КЕП передбачає генерацію двох ключів, необхідних для подальшої роботи в електронній системі охорони здоров'я – відкритого та закритого. Відкритий ключ потрібен для подальшої валідації автентичності КЕП особи, а закритий – є файлом, захищеним особистим паролем, який буде використовуватися тільки при накладанні підпису. Відкритий ключ згодом розміщується на офіційних ресурсах і є доступним для перевірки статусу.

Таким чином, підписати електронний документ можна виключно за допомогою закритого ключа, а перевірити накладений КЕП – за відкритим ключем, який відповідає закритому і згенерований парою разом з ним.

Згідно з Законом КЕП має таку ж юридичну силу, як і власноручний підпис. Відповідно, і електронний документ, який підписаний за допомогою КЕП, матиме таку ж юридичну силу, як паперовий документ, підписаний від руки. Різниця між КЕП та власноручним підписом залишається лише у формі. Як наслідок, берегти свій КЕП треба так, ніби ти бережеш свій власноручний підпис.

КЕП можна зберігати на наступних захищених носіях:

- токен;
- депозитарій (захищене хмарне сховище).

Визначення: ***Токен***
USB-пристрій, який зовні схожий на флеш-носій, з унікальним інвентарним номером, що затверджений Державною службою спеціального зв'язку та захисту інформації України.

На токені зберігається ключова інформація щодо власника електронного підпису та ключів. Головна відмінність від збереження ключа на звичайному флеш-носії в тому, що при ідентифікації зчитується не лише сам файл, а й параметри носія, на якому він зберігається. Такий ключ неможливо скопіювати на інший пристрій. Секретний ключ ніколи не залишає

носій, так ключ існує в єдиному екземплярі. Токен захищений паролем доступу, з обмеженою кількістю спроб підбору пароля (7 можливих спроб підбору паролю після чого він блокується). Отже, це вже не файл з ключем, який можна скопіювати та переслати, а надійний пристрій.

Також КЕП може зберігатись в захищеному хмарному сховищі.

Визначення: ***Хмарне сховище КЕП***
Програмно-апаратний комплекс, який дозволяє зберігати особисті ключі електронного підпису чи печатки у спеціальному захищеному сховищі (депозитарії), яке побудовано з дотриманням норм чинного законодавства у сфері захисту інформації та електронних довірчих послуг.

Сервіс дає можливість користувачам електронних довірчих послуг зберігати ключі електронного підпису чи печатки в захищеному сховищі і самостійно керувати доступом до особистого ключа, та статусами кваліфікаційних сертифікатів без відвідування віддалених пунктів реєстрації, представництв, офісів кваліфікованих надавачів електронних довірчих послуг. До хмарного сховища користувач має цілодобовий віддалений доступ.

Тема 6.4. Принципи побудови стійкої системи кіберзахисту. Вимоги законодавства щодо захисту інформації в медичних закладах та основи захисту інформації в закладі охорони здоров'я

6.4.1 Вступ

Інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді (стаття 1 Закону України «Про інформацію»).

Інформація є нематеріальним благом, яке не зводиться до матеріальних об'єктів, де вона закріплена (записи на папері, відео-, аудіоплівки), тому, інформація характеризується майже безкінечною можливістю її тиражування та розповсюдження.

Інформацію, в свою чергу, за порядком доступу можна поділити на такі категорії:

- відкрита інформація;
- інформація з обмеженим доступом: конфіденційна, таємна (персональні дані, лікарська таємниця) та службова.

Законодавство розмежовує інформацію наступним чином: будь-яка інформація є відкритою, крім тієї, що віднесена законодавством до інформації з обмеженим доступом (ст. 20 Закону України "Про інформацію").

Відкрита інформація не потребує захисту, бо часто є відомою та загальнодоступною всім (наприклад, адреса медичного закладу або послуги, які надаються).

Інша ситуація з інформацією з обмеженим доступ. До її захисту встановлюються особливі вимоги, однак ці вимоги залежать від того про яку саме інформацію з обмеженим доступом

йде мова. Нижче наведено огляд видів інформації з обмеженим доступом, що найчастіше зустрічається у ЗОЗ.

Конфіденційна інформація

Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку, або ж в інших конкретних випадках, визначених законом. Тобто, інформація про фізичну особу належить саме до конфіденційної інформації. Власне, в розумінні законодавства, інформація про фізичну особу і є персональними даними.

Визначення: ***Конфіденційна інформація***

Інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень (ст. 21 Закону України "Про інформацію"). Наприклад, інформація про технологію виробництва певного препарату у фармацевтичній компанії.

Законодавство не дає вичерпного переліку персональних даних (далі – ПД), а лише встановлює, що персональними даними є будь-яка інформація, яка прямо ідентифікує або дозволяє ідентифікувати людину. Іншими словами, це та інформація, яка дозволяє визначити, відрізнити з-поміж усіх людей конкретну особу.

Визначення: ***Персональні дані***

Це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована (ст. 2 Закону України "Про захист персональних даних"). Наприклад, номер телефону пацієнта, його електронна пошта, адреса тощо.

ПД можуть бути виражені у формі: літер (ім'я); чисел (ідентифікаційний код особи); зображення (підпис, фото), звуку (запис телефонної розмови зі страховою компанією), відео (запис з камер відеоспостереження) тощо. На практиці персональними даними може бути наступна інформація: ПІБ, паспортні дані, реєстраційний номер облікової картки платника податків, адреса реєстрації або місце перебування особи, національність, сімейний стан, релігійні переконання, стан здоров'я, матеріальне становище, дата і місце народження, адреса електронної пошти тощо.

Дані можуть вважатись персональними незалежно від форми, в якій вони зберігаються (наприклад, електронна медична картка чи паперова) та сфери життя особи, якої стосуються дані (наприклад, особисте, сімейне, професійне життя тощо).

В свою чергу, ПД включають в себе дані, обробка яких становить особливий ризик для прав і свобод суб'єктів ПД (чутливі дані, *sensitive data*). Таким ПД законодавство надає особливий статус та встановлює вимоги до їх обробки. Це пов'язано із тим, що обробка чутливих даних може призвести до значних ризиків для фундаментальних прав і свобод людини.

До особливих категорій ПД (чутливих даних) відноситься в тому числі інформація про: расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в

політичних партіях та професійних спілках, притягнення до кримінальної відповідальності, дані, що стосуються здоров'я, статевого життя, біометричні або генетичні дані.

Медичні дані – усі особисті дані про стан здоров'я фізичної особи, а також дані, які чітко та тісно пов'язані з даними про стан здоров'я і генетичними даними.

Отже, оскільки вичерпного переліку ПД немає, потрібно щоразу аналізувати будь-яку інформацію на предмет того, чи дозволяє ця інформація встановити особу, якій вона належить, і чи несе підвищений ризик обробка такої інформації для суб'єкта ПД.

Немає також єдиної формули, яка дозволяє визначити чи мова йде про персональні дані чи про знеособлену інформацію. У кожному окремому випадку необхідно аналізувати чи є можливість ідентифікувати конкретну особу**.**

Лікарська таємниця

Лікарська таємниця є найпоширенішим видом інформації з обмеженим доступом, що зустрічається у закладах охорони здоров'я. Регулювання лікарської таємниці встановлюється ст. 39-1, 40 Закону України «Основи законодавства України про охорону здоров'я».

Визначення: ***Лікарська таємниця***
Лікарська таємниця включає в себе відомості про: хворобу, результати медичного обстеження, оглядів та їхні результати, інтимну і сімейну сторони життя громадянина (ст. 39-1 Закону України "Основи законодавства України про охорону здоров'я"), які стали відомі медичним працівникам у зв'язку з виконанням професійних або службових обов'язків, та які медичні працівники не мають право розголошувати, крім випадків прямо передбачених законодавчими актами.

Таку інформацію забороняється вимагати та подавати за місцем роботи або навчання (ст. 286 Цивільного Кодексу України).

Умови та випадки за яких дозволяється розкриття лікарської таємниці, передбачені у різних актах. Наприклад, відповідно до ст. 30 Сімейного кодексу України, результати медичного обстеження є таємницею і повідомляються лише нареченим. Іншим прикладом, може бути надання доступу до лікарської таємниці на підставі суду, слідчого-судді про надання тимчасового доступу до речей і документів, які містять охоронювану законом таємницю відповідно до Кримінального процесуального кодексу України.

Малюнки 13 – 14 демонструють співвідношення та взаємозв'язок різних видів інформації.

Малюнок 13. Співвідношення різних видів інформації

Малюнок 14. Співвідношення лікарської таємниці з персональними і чутливими даними

Для того, щоб у ЗОЗ забезпечити відповідність роботи з персональними даними вимогам законодавства, а також підтримувати цю відповідність протягом тривалого часу на належному рівні, розглянемо наступні рекомендації, що наведені у вигляді практичних кроків:

1. Розробка та затвердження положення (порядку) про захист персональних даних, інших внутрішніх документів (наприклад, облік працівників, що мають доступ до персональних даних пацієнтів, план дій на випадок несанкціонованого доступу до

персональних даних, пошкодження технічного обладнання та виникнення надзвичайних ситуацій). Такі документи дозволять створити систему обробки персональних даних та забезпечити їхній захист.

- Основним документом ЗОЗ, що регулює обробку персональних даних, повинен бути порядок обробки персональних даних. Типовий порядок обробки персональних даних в Україні розроблено на законодавчому рівні, тому ЗОЗ може скористатися ним під час оформлення відповідного внутрішнього документу.
- Типовий порядок містить норми, що використовуються, як для обробки персональних даних із застосуванням автоматизованих засобів, так і без них. Такий документ приймається у порядку передбаченому для прийняття локальних правових актів у ЗОЗ. Внутрішній документ зазвичай затверджується керівником ЗОЗ, шляхом видання відповідного наказу. Порядок обробки персональних даних має бути доступним для кожного працівника ЗОЗ. Зміни, які вносяться до Порядку обробки персональних даних мають своєчасно доводитися до відома всіх працівників.

2. Визначення відповідального працівника за забезпечення захисту персональних даних. Такий працівник має консультувати персонал з приводу питань дотримання законодавства про захист персональних даних.

   У ЗОЗ, які здійснюють обробку персональних даних, потрібно створювати (визначати) структурний підрозділ або відповідальну особу, що буде організовувати роботу, пов’язану із захистом персональних даних при їх обробці. Оскільки інформація про стан здоров’я входить до персональних даних, що становить особливий ризик для прав і свобод суб’єктів, тому у ЗОЗ має бути визначено такий структурний підрозділ або відповідальна особа.

   Законодавство не передбачає обов’язкової наявності підрозділу або працівника, що відповідає лише за питання обробки персональних даних. На практиці такі обов’язки часто покладаються на підрозділи або осіб, що паралельно виконують інші функції, наприклад, юридичний відділ або юриста, канцелярію, відділ кадрів тощо.

3. Підписання зобов'язання про нерозголошення персональних даних тими працівниками, які мають доступ до персональних даних у зв'язку з виконанням їхніх професійних обов'язків.

   Кожен працівник, який має доступ до персональних даних, має надати своєму роботодавцю письмове зобов’язання про нерозголошення тих персональних даних, які їм було довірено або які стали їм відомі у зв’язку з виконанням професійних обов’язків.

   При позбавленні медичного працівника доступу до персональних даних вживаються заходи, що унеможливлюють доступ такої особи до персональних даних. Документи та інші носії, що містять персональні дані суб’єктів, передаються іншому працівнику.

Таке зобов'язання має містити реквізити працівника, його посаду, рівень його доступу до персональних даних, обмеження доступу (у разі наявності). Також працівник повинен прийняти на себе зобов'язання не розголошувати у будь-який спосіб персональних даних інших осіб, що стали відомі у зв'язку з виконанням посадових обов'язків або повноважень.

4. Проведення регулярних навчань персоналу, що має доступ до персональних даних пацієнтів щодо правил поводження з персональними даними. Такий крок не є обов'язковою вимогою законодавства, проте повинен сприяти розвитку культури роботи з персональними даними.

Отже, до інформації з обмеженим доступом, яка обробляється ЗОЗ, застосовуються додаткові вимоги щодо її захисту. Основи захисту такої інформації встановлені у наступних законодавчих документах:

- Закон України «Про інформацію»
- Закон України «Про захист персональних даних»
- Закон України «Основи законодавства України про охорону здоров'я»
- Типовий порядок обробки персональних даних у базах персональних даних

В сучасному світі захист інформації став надзвичайно важливим аспектом управління діяльності організацій, і водночас найбільш цінним активом. Одним з надійних і комплексних засобів захисту інформації в організації є запровадження системи управління інформаційною безпекою на основі міжнародних стандартів серії ISO/IEC 27000. Ключовим стандартом серії є стандарт ISO 27001 «Системи управління інформаційною безпекою». Цей стандарт описує як саме має бути запроваджена система управління інформаційною безпекою (СУІБ) в організації.

6.4.2 Принципи побудови стійкої системи кіберзахисту

Визначення: ***Кіберстійкість***
Можливість системи або організації функціонувати на належному рівні та досягати поставлених цілей, не дивлячись на спроби кібератак, які на неї можуть здійснюватися.

Отже, систему кіберзахисту вважають стійкою, якщо вона успішно захищає організацію від суттєвих наслідків при втручанні в роботу її інформаційних систем з боку кіберзлочинців.

Для систематизованого підходу до оцінки кіберстійкості використовують наступні методи та підходи:

- Моделювання загроз
- Аналіз впливу
- Оцінка вірогідності

Під моделюванням загроз розуміють експертну оцінку того, які саме види та варіації кібератак є можливими та релевантними. Формулюється перелік або, так званий, каталог загроз зі стандартизованою класифікацією по типам.

Наступним етапом є прогнозування наслідків для організації від реалізації кібератак. Цей вид аналізу називається аналіз впливу. Необхідно зрозуміти, наскільки сильно постраждає конфіденційність, цілісність та доступність інформації від окремо взятої потенціальної атаки.

Завершальним кроком є оцінка вірогідності успішного виконання кібератаки. До уваги треба брати як наявність механізмів кіберзахисту, так і технічну складність реалізації кібератаки злочинцями. Також на вірогідність спроб атаки впливає співвідношення ресурсів, які необхідно витратити на атаку і цінності інформації та інформаційної системи, яку атакують.

Можна виділити наступні принципи побудови стійкої системи кіберзахисту:

- Принцип процесного підходу
- Принцип ешелонованого захисту

Розглянемо їх детальніше детальніше у 6.4.2.1 Принцип процесного підходу до кіберзахисту і 6.4.2.2 Принцип ешелонованого захисту

6.4.2.1 Принцип процесного підходу до кіберзахисту

Хорошою практикою вважається побудова системи кіберзахисту як сукупності взаємопов'язаних процесів. Популярною моделлю для цього є СУІБ – система управління інформаційною безпекою, побудованою на основі ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT). В СУІБ прийнято включати наступний перелік процесів:

- Управління ресурсами
- Безпека людських ресурсів
- Фізична безпека та безпека інфраструктури
- Управління комунікаціями та функціонуванням
- Контроль доступу
- Придбання, розроблення та підтримка інформаційних систем
- Управління інцидентом інформаційної безпеки
- Управління інцидентами інформаційної безпеки та вдосконаленням
- Управління безперервністю бізнесу

6.4.2.2 Принцип ешелонованого захисту

Окремий принцип побудови стійкої системи кіберзахисту – впровадження декількох заходів захисту від однієї потенційного кіберзагрози. Це обумовлено тим, що будь-яка технологія може давати збій. Якщо заходи захисту передбачають залучення людини, то варто згадати вислів «помилятися – це частина людської природи». Таким чином, недосконалість або відмову в спрацюванні одного рівня захисту необхідно компенсувати побудовою додаткового механізму кібербезпеки. Прикладом з повсякденного життя є установка двох типів замків для дверей в офісне приміщення – механічного та електронного. В сфері кібербезпеки, прикладом є навчання користувачів навичкам кібергігієни з одного боку, та

розгортання системи автоматичного маркування підозрілих електронних листів з другого. Також, на рівні IT-спеціалістів під ешелонованим захистом часто розуміють встановлення підсистеми захисту для кожного типу IT-систем – окремо для телекомунікаційного обладнання, окремо для програмного забезпечення та окремо для бази даних.

Тема 6.5 Удосконалення системи кібербезпеки

6.5.1 Вступ

Розбудова системи кібербезпеки – це поетапний процес. Після впровадження базових заходів організації слід переходити до планування побудови посилених механізмів кібербезпеки.

Оскільки впровадження і розвиток системи кібербезпеки потребує певних фінансових та часових інвестицій, важливо при плануванні цільового стану кібербезпеки керуватися принципом Кірхгофа.

Визначення: ***Принцип Кірхгофа***

У спрощеній формі принцип Кірхгофа можна пояснити наступним чином: вартість системи захисту інформації не повинна бути дорожчою за цінність інформацію, яку вона захищає.

6.5.2 Моделі зрілості системи кібербезпеки

Для того, щоб організації мали спільний орієнтир при розвитку системи кібербезпеки, хорошою практикою вважається застосування моделей зрілості системи кібербезпеки.

Визначення: ***Модель зрілості системи кібербезпеки***

Формалізована модель для виміру рівнів вдосконалення системи кібербезпеки організації. Зазвичай моделі зрілості кібербезпеки фокусуються на процесному підході до побудови кібербезпеки та розраховані на вище керівництво організації в якості цільової аудиторії.

Модель зрілості системи кібербезпеки допомагає вирішити ряд наступних задач:

- об'єктивна самооцінка поточного стану кібербезпеки;
- порівняння власного стану кібербезпеки з середнім рівнем по галузі;
- формування стратегії розвитку кібербезпеки;
- пошук «спільної мови» між технічними спеціалістами та керівництвом організації.

Популярними стандартизованими моделями зрілості системи кібербезпеки є наступні:

- Cybersecurity Capability Maturity Model – C2M2 (розроблено для Департаменту енергетики США)
- NIST Cybersecurity Framework (розроблено Національним інститутом стандартів США)
- Cybersecurity Maturity Model Certification (розроблено для Департаменту оборони США)

Таблиця 1. Порівняльна характеристика моделей зрілості системи кібербезпеки

Коротка назва моделі	C2M2	NIST CSF	Cybersecurity Maturity Model Certification
Кількість рівнів зрілості	3	4	5
Кількість категорій заходів (доменів) кібербезпеки	10	21	17
Тип оцінки	Самооцінка	Самооцінка	Зовнішня оцінка/ сертифікація
Рік публікації	2012	2013	2020

6.5.3 Модель зрілості системи кібербезпеки NIST CSF

Пропонуємо розглянути модель зрілості системи кібербезпеки NIST CSF більш детально, оскільки методологію NIST CSF було адаптовано в українському законодавчому полі, а саме, як підхід до організації кібербезпеки об'єктів критичної інформаційної інфраструктури.

Таблиця 2. Чотири рівні зрілості Моделі NIST CSF

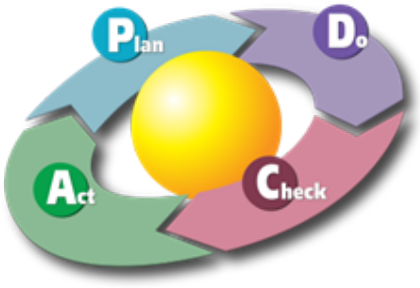
Рівень зрілості NIST CSF	**Коротка назва**	**Опис**

1	Частковий	Заходи кібербезпеки не формалізовано. Обмежена поінформованість персоналу про ризики кібербезпеки.
2	Поінформований	Поінформованість про ризики кібербезпеки присутня. Заходи з кібербезпеки офіційно затверджено керівництвом, але відсутній систематичний та всеохоплюючий підхід керівництва до кібербезпеки.
3	Повторюваний	Заходи кібербезпеки запроваджено на рівні формальних політик організації. Запроваджено системний підхід до управління ризиками в сфері кібербезпеки.
4	Адаптивний	Організація аналізує попередній досвід та поточну ситуацію для постійної адаптації системи кібербезпеки до поточних ризиків.

Передбачається, що організація виконує самооцінку для визначення поточного стану процесів системи кібербезпеки. Після чого керівництво має обрати бажаний рівень зрілості на досягнення якого направити ресурси та час. Необов'язково, щоб кожна організація ставила собі за мету досягнення максимального рівня зрілості в короткий час (рівень Адаптивний). Розвиток системи кібербезпеки відбувається поступово і з огляду на присутні на поточний момент загрози кібербезпеці організації.

6.5.4 Принцип Демінга-Шухарта

В менеджменті популярною методологією безперервного вдосконалення процесів є Принцип Демінга-Шухарта, також відомий як принцип або цикл PDCA: Plan-Do-Check-Act – Плануй-Роби-Перевіряй-Дій (див. малюнок 15).



Малюнок 15. Принцип Демінга-Шухарта або цикл PDCA

Принцип Демінга-Шухарта – це алгоритм дій по управлінню процесом з метою його вдосконалення:

- Планування: постановка цілей, планування їх досягнення, а також розподіл ресурсів;
- Виконання: реалізація запланованих робіт;
- Перевірка: збір інформації про результати роботи згідно процесу, зокрема вимір ключових індикаторів виконання (key performance indicators); у випадку відхилень — пошук причини проблеми;
- Коригування: застосування заходів для уникнення відхилень від плану в подальшому, внесення змін в розподіл ресурсів та майбутнє планування.

Принцип Демінга-Шухарта є дуже популярним методом підвищення зрілості системи кібербезпеки в організації.

Тема 6.6 Захист персональних даних пацієнта при роботі з інформаційно-комунікаційними системами електронної охорони здоров'я

6.6.1 Вступ

Із впровадженням Електронної системи охорони здоров'я (далі — ЕСОЗ), питання захисту персональних даних (далі – ПД) пацієнтів стало надзвичайно актуальним. Адже з перенесенням медичних даних в електронний вигляд та недостатнім розумінням щодо поводження з ПД, ризики розголошення конфіденційної інформації суттєво зростають. Витік масиву інформації про пацієнтів, стан їхнього здоров'я і деталей лікування може призвести до негативних наслідків для пацієнта, працівника ЗОЗ, що спричинив такий витік, а також ЗОЗ в цілому. Саме тому забезпечення належного рівня захисту ПД пацієнтів є важливим аспектом при роботі з ЕСОЗ.

Ключова термінологія по даній темі визначена у попередніх розділах, а саме: інформація (див. розділ 6.1.1 Вступ), конфіденційна інформація, персональні дані, лікарська таємниця (див. розділ 6.4.1 Вступ).

6.6.2 Учасники відносин, пов'язаних з персональними даними

Важливо розуміти ключові терміни, що визначають ролі учасників відносин, пов'язаних з обробкою і захистом ПД, а саме:

Визначення: ***Суб'єкт ПД***
Фізична особа, персональні дані якої обробляються (ст. 2 Закон України "Про захист персональних даних").

Кожна особа є суб'єктом персональних даних, наприклад, ім'я, дата народження, номер телефону тощо. В контексті теми даного документу, найчастіше суб'єктом ПД виступає саме пацієнт.

Визначення: ***Володілець ПД (далі - Володілець)***
Фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом (ст. 2 Закон України "Про захист персональних даних").

Наприклад, лікувальний заклад отримавши ПД пацієнта, починає здійснювати їхню обробку та стає володільцем персональних даних пацієнта.

Визначення: ***Розпорядник ПД (далі - Розпорядник)***
Фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця (ст. 2 Закон України "Про захист персональних даних").

Володілець може доручити обробку ПД розпоряднику відповідно до договору, укладеного в письмовій формі. Розпорядник може обробляти ПД лише з метою і в обсязі, визначених у договорі.

Розглянемо приклад ситуації, щоб коректно визначити розпорядника і володільця.

ЗОЗ співпрацює з лабораторією і передає їй матеріали для досліджень разом з контактними даними пацієнта, а далі, лабораторія самостійно надсилає результати таких досліджень пацієнту. В даній ситуації суб’єкт ПД (пацієнт) надав свої дані володільцю (ЗОЗ), в свою чергу останній передав ці дані на підставі договору розпоряднику (лабораторії).

Визначення: ***Третя особа***
Будь-яка особа, за винятком суб’єкта ПД, володільця чи розпорядника ПД та Уповноваженого Верховної Ради України з прав людини, якій володільцем чи розпорядником персональних даних здійснюється передача ПД (ст. 2 Закон України "Про захист персональних даних").

Визначення: ***Одержувач***
Фізична чи юридична особа, якій надаються ПД, у тому числі третя особа (ст. 2 Закон України "Про захист персональних даних").

6.6.3 Ключові вимоги при обробці персональних даних

Основною вимогою до всіх осіб, які здійснюють обробку ПД є забезпечення належного захисту ПД для того, щоб треті особи не отримали доступу до ПД з метою їхнього знищення або втрати. Тобто, мова йде про вимоги до всіх володільців та розпорядників.

Для того, щоб створити та забезпечити механізм захисту ПД, діюче законодавство України ставить ряд вимог до володільців та розпорядників, зокрема:

- використання ПД володільцем має здійснюватися лише тоді, коли володілець створив умови для захисту цих даних;
- використання ПД працівниками володільця, має здійснюватися лише відповідно до їхніх професійних/службових/трудових обов'язків. Ці працівники зобов'язані не допускати розголошення у будь-який спосіб ПД, які

їм було довірено або які стали відомі у зв'язку з виконанням професійних/службових/трудових обов'язків, крім випадків, передбачених законом. Таке зобов'язання чинне також і після припинення ними діяльності, пов'язаної з ПД;
- ПД можуть оброблятися у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, у строк не більше, ніж це необхідно відповідно до мети їхньої обробки. В будь-якому разі вони обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються в не довше, ніж це передбачено законодавством у сфері архівної справи та діловодства.

Окрему увагу варто акцентувати на строках обробки ПД. Закон України "Про захист персональних даних" передбачає те, що обробка ПД допускається у термін, що не є довшим ніж для цього є обґрунтована мета та належна підстава. Важливо зазначити, що документи, які містять ПД мають певні законодавчо встановлені терміни зберігання. Наприклад, історії хвороби стаціонарних хворих мають зберігатися не менше 25 років, а амбулаторних – не менше 5 років після вибуття. Тобто, при визначенні термінів обробки ПД пацієнтів можна також опиратися і на ці строки, а також встановлені строки для зберігання інших документів.

6.6.4 Права і обов'язки суб'єкта персональних даних

Чітке розуміння правового статусу пацієнта, як суб'єкта персональних даних, допоможе правильно побудувати свою роботу з персональними даними пацієнта, а також допоможе у спілкуванні з пацієнтами та/або при вирішенні нестандартних ситуацій.

Пацієнт, будучи суб'єктом персональних даних – тобто особою, дані якої обробляються, має певні права та обов'язки, які слідують з цього статусу. Як було зазначено раніше, медичні дані (чутливі дані) є частиною та входять до складу персональних даних.

Права пацієнтів, як суб'єктів персональних даних, встановлюються Законом України «Про захист персональних даних». Такі права пацієнтів умовно можна об'єднати у три групи:

- права, що пов'язані з доступом до даних;
- права, що пов'язані з розпорядженням даними;
- права, що пов'язані з захистом ПД.

Права пацієнтів, що пов'язані з доступом до ПД

Ця група прав пов'язана з обізнаністю пацієнта, як суб'єкта ПД, щодо інформації про те, хто та в якому обсязі матиме доступ до його ПД:

1. Пацієнт має право знати про місцезнаходження своїх ПД, мету їх обробки, місцезнаходження володільця чи розпорядника ПД

   Наприклад, пацієнт повідомляється про мету обробки ПД під час підписання Декларації про вибір лікаря, який надає первинну медичну допомогу, затверджену Наказом Міністерства охорони здоров'я України № 503 від 19.03.2018.

2. У разі передачі ПД третім особам, пацієнт має право отримувати інформацію про таку передачу, зокрема осіб, яким передаються його ПД.

3. Пацієнт має право на доступ до своїх ПД.

Законодавство передбачає право пацієнта, як користувача ЕСОЗ, вносити та переглядати інформацію про себе в системі. Хоча наразі технічна можливість реалізувати це право відсутня, однак активно триває розробка модулю “Кабінет пацієнта”, де пацієнт зможе ознайомлюватись та редагувати інформацію про себе в ЕСОЗ. Зазвичай пацієнт реалізує це право шляхом звернення із запитом до медичного закладу з проханням ознайомитися з історією хвороби або іншою медичною інформацією. Медичний працівник зобов’язаний надати доступ до такої інформації. Запит повинен містити інформацію про ПІБ пацієнта, місце його проживання, документ, що посвідчує особу.

4. Пацієнт має право отримувати інформацію щодо того чи обробляються його ПД.

   Реалізація цього права здійснюється шляхом направлення відповідного запиту. Запит повинен направлятись у письмовій формі в порядку та у спосіб, що передбачені Законом України “Про звернення громадян”. Відповідь на запит повинна бути надана протягом місяця. Якщо в результаті розгляду звернення питання не було вирішено, суб'єкт ПД може звернутися за захистом/поновленням своїх прав до Уповноваженого Верховної Ради України з прав людини.

Права пацієнтів, що пов’язані з розпорядженням своїми ПД

В цю категорію входять права пацієнта, як суб’єкта ПД, пов’язані з можливістю вчиняти певні дії щодо своїх ПД, зокрема:

1. Пацієнт має право вимагати зміни своїх недостовірних ПД володільцем та розпорядником шляхом пред’явлення вмотивованої письмової вимоги (з поясненнями в чому саме недостовірність або невідповідність). Після отримання такої вимоги володілець або розпорядник зобов’язаний внести зміни до недостовірних ПД пацієнта.

2. Пацієнт має право вимагати знищення своїх ПД будь-яким володільцем та розпорядником, якщо ці дані обробляються незаконно (наприклад, якщо ПД обробляються без належної правової підстави або якщо обробляються дані обробка яких заборонена законом). Таке право реалізується шляхом направлення письмової вимоги з обґрунтуванням причин необхідності видалення ПД, зокрема незаконності їхньої обробки.

3. Право вносити застереження стосовно обмеження (встановлювати певні обмеження) права на обробку своїх ПД під час надання згоди (застосовується, коли згода є підставою для обробки ПД). Такі обмеження можуть стосуватись мети обробки ПД, передачі ПД третім особам тощо. Володільці та розпорядники зобов’язані враховувати застереження при обробці ПД.

4. Пацієнт має право відкликати згоду на обробку ПД.

В контексті ЕСОЗ, Постанова КМУ № 411 від 25.04.2018 року «Деякі питання електронної системи охорони здоров’я» дублює це право пацієнта, говорячи про можливість направляти заяву про відкликання заяви про надання згоди на обробку ПД. Відкликання згоди є

можливим, якщо ПД обробляються на підставі згоди та має відбуватися у такій самій формі, у якій така згода надавалась.

Права пацієнтів, що пов’язані з захистом своїх ПД

Ця група об’єднує права пацієнта, як суб’єкта ПД, які спрямовані на реалізацію базового фундаментального принципу в сфері ПД – їхнього захисту:

1. Пацієнт має право на захист своїх ПД від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням. У випадку порушення цього права, пацієнт має право захищати свої права шляхом звернення до Уповноваженого Верховної Ради України з прав людини, судових органів.

2. Пацієнт має право звертатися зі скаргами на обробку своїх ПД до Уповноваженого Верховної Ради України з прав людини або до суду, застосовувати інші можливі засоби правового захисту. Пацієнт також може звертатися з претензією до самого володільця або розпорядника.

3. Пацієнт має право на захист від автоматизованого рішення, яке має для нього правові наслідки та знати механізм автоматичної обробки ПД.

   Наприклад, в медичній сфері це може бути певна програма, яка за наявними ПД визначає чи має право особа брати участь у реабілітаційних програмах, програмах лікування тощо. Тому в разі наявності такого алгоритму і використання ПД пацієнта в ньому, пацієнт повинен бути попереджений/повідомлений про такий механізм автоматизованої обробки і мати можливість заперечити проти застосування його результатів.

Отже, пацієнти, як суб’єкти ПД мають значно більше прав ніж обов’язків. Це обумовлено тим, що суб’єкт ПД передає свій важливий ресурс, тобто персональні дані.

6.6.5 Доступ третіх осіб до персональних даних

Як зазначалось у попередніх розділах, унеможливлення доступу третіх осіб до ПД є однією з ключових вимог при роботі з ПД. Однак, в деяких випадках, такий доступ може чи повинен надаватись з урахуванням правового статусу особи, що запитує інформацію та конкретних обставин.

Нижче наводимо інформацію щодо найбільш поширених випадків можливого правомірного розкриття ПД пацієнта третіми особами:

Члени сім’ї пацієнта

Часто на практиці виникають ситуації, коли родичі пацієнта просять надати їм інформацію про стан здоров'я пацієнта. В таких ситуаціях потрібно розуміти чи мають члени сім’ї право на доступ до інформації про пацієнтів, і якщо так, то хто саме, та в якому обсязі.

Ст. 285 Цивільного Кодексу України та ст. 39 Закону України «Основи законодавства України про охорону здоров'я» передбачають, що батьки (усиновлювачі), опікун, піклувальник мають право на доступ до інформацію про стан здоров'я дитини або підопічного.

Однак, медичні працівники мають право **дати неповну інформацію** про стан здоров'я фізичної особи, обмежити можливість їхнього ознайомлення з окремими медичними документами, якщо інформація про хворобу фізичної особи може: погіршити стан її здоров'я, погіршити стан здоров'я батьків (усиновлювачів), опікуна або піклувальника, зашкодити процесу лікування.

Працівники медичних закладів

Використання ПД працівниками суб'єктів відносин, пов'язаних з ПД (наприклад, ЗОЗ), повинно здійснюватися лише відповідно до їхніх професійних, службових або трудових обов'язків.

В той же час, такому використанню кореспондує обов'язок працівників не допускати розголошення у будь-який спосіб ПД, які їм було довірено або які стали відомі у зв'язку з виконанням професійних, службових або трудових обов'язків. Крім того, такий обов'язок зберігається після припинення ними діяльності, пов'язаної з ПД.

Обсяг доступу до даних пацієнта є обмеженим. Він обмежується з метою доступу чи використання персональних даних – виконанням професійних, трудових або службових обов'язків. Тобто, працівники ЗОЗ повинні користуватися доступом лише до тих ПД пацієнтів (їхніх частин), які необхідні їм у зв'язку з виконанням їх професійних, службових або трудових обов'язків.

Тобто, лікар може працювати виключно з ПД пацієнтів, яким надається медична допомога таким лікарем, або з даними, які необхідні йому для надання медичної допомоги.

Роботодавці та навчальні заклади

Ст. 39^1 Закону України «Основи законодавства України про охорону здоров'я» прямо забороняє надавати інформацію про діагноз і методи лікування пацієнта за місцем роботи або навчання. Тобто, якщо до ЗОЗ або безпосередньо до медичного працівника надходить запит від роботодавця чи навчального закладу (вищі навчальні заклади, школи, дитячі садочки тощо) щодо стану здоров'я працівника або особи, що навчається, медичний працівник не має права надавати роботодавцю чи навчальному закладу відомості про пацієнта, що становлять лікарську таємницю.

Винятками є випадки інформування підприємства, де працює особа, що постраждала внаслідок нещасного випадку на виробництві. ЗОЗ зобов'язаний невідкладно передати екстрене повідомлення про звернення потерпілого з посиланням на нещасний випадок на виробництві (у разі можливості, з висновком про ступінь тяжкості травм) підприємству де працює потерпілий або на якому він виконував роботу. У контексті інфекційних захворювань, лише головні державні санітарні лікарі (їхні заступники) можуть вносити власникам підприємств та установ подання про відсторонення від роботи або іншої діяльності (навчання) осіб, які, наприклад, є носіями збудників інфекційних захворювань, були в контакті з такими хворими тощо.

Інші особи

Окрім самого пацієнта, його родичів, медичного персоналу, доступ до персональних даних пацієнта можуть також отримати треті особи – особи, які не мають родинних зв'язків з пацієнтом та не приймають участь у процесі надання медичної допомоги. На практиці, це може бути широке коло осіб, як: адвокати, правоохоронні органи (органи поліції, органи

прокуратури, Служба Безпеки України, Пенітенціарна служба України), суди, громадські організації, банки, страхові організації та інші фінансові установи, журналісти тощо.

За загальним правилом, поширювати персональні дані про особу можна лише за згодою такої особи. Однак, відповідно до Закону України «Про захист персональних даних», дані пацієнтів можуть надаватись третім особам без згоди суб'єкта за умови:

1. Третя особа бере на себе зобов'язання щодо забезпечення виконання вимог Закону України «Про захист персональних даних» (наприклад, не допускати будь-якого розголошення даних, не допускати несанкціонований доступ третіх осіб та інші вимоги). Якщо третя особа не здатна забезпечити виконання вимог цього закону або не бере на себе таке зобов'язання, то ПД передаватись не можуть.

2. Третя особа подала запит, який містить всю необхідну інформацію, передбачену ч. 4 ст. 16 Закону України «Про захист персональних даних», а саме:

   - відомості про особу заявника: прізвище, ім'я та по батькові (далі – ПІБ), місце проживання, реквізити паспорту для фізичної особи; найменування, місцезнаходження юридичної особи, яка подає запит, посада, ПІБ, яка засвідчує запит; підтвердження того, що зміст запиту відповідає повноваженням юридичної особи (наприклад, запит державного органу має містити інформацію, яка підтверджує, що зміст запиту відповідає повноваженням певного державного органу);
   - ПІБ, а також інші відомості, що дають змогу ідентифікувати фізичну особу, стосовно якої робиться запит;
   - відомості про базу ПД, стосовно якої подається запит або відомості про володільця чи розпорядника;
   - перелік ПД, що потрібні третій особі згідно з запитом;
   - мета та/або правові підстави для запиту.

Відповідь на запит повинна бути надана у певних часових рамках:

- 10 робочих днів (з дня надходження запиту) надається для вивчення запиту на предмет можливості його задоволення. Тобто, в межах цього строку необхідно довести до відома особи, яка подала запит, що запит буде задоволено або відповідні ПД не підлягають наданню із зазначенням правової підстави;
- 30 календарних днів (з дня надходження запиту) надання запитуваних даних у разі задоволення запиту.

Таким чином, кожна ситуація розкриття ПД потребує індивідуального підходу. Саме тому, з урахуванням викладеної інформації, пропонуємо приблизний алгоритм аналізу обґрунтованості запитів та оцінки прав третіх осіб на доступ до даних пацієнта:

1. визначення відомостей щодо яких надійшов запит;
2. встановлення особи, яка запитує відомості, її повноважень та підстав для отримання відомостей про пацієнта;
3. перевірка порядку надання відомостей (наприклад, чи має запит на отримання персональних даних усі реквізити, чи відповідає Ухвала про

надання тимчасового доступу до речей та документів вимогам законодавства, чи підтверджує адвокатський чи інший запит наявність згоди пацієнта на розкриття ПД або лікарської таємниці);

4. прийняття рішення про надання або ненадання запитуваних відомостей.

У разі порушення правил поширення даних та лікарської таємниці та отримання третіми особами неправомірного доступу, медичні працівники можуть нести відповідальність (див. 6.6.7 Права та відповідальність медичних працівників

6.6.6 Особливості захисту персональних даних при роботі з ЕСОЗ

Визначення: ***Електронна система охорони здоров'я (ЕСОЗ)***
Інформаційно-телекомунікаційна система, що забезпечує автоматизацію ведення обліку медичних послуг та управління медичною інформацією шляхом створення, розміщення, оприлюднення та обміну інформацією, даними і документами в електронному вигляді, до складу якої входять центральна база даних та електронні медичні інформаційні системи, між якими забезпечено автоматичний обмін інформацією, даними та документами через відкритий програмний інтерфейс (Закон України «Основи законодавства України про охорону здоров'я»).

Отже, з вищенаведеного можна підкреслити наступні ознаки ЕСОЗ:

- інформаційно-телекомунікаційна система, тобто сукупність систем, які у процесі обробки інформації діють як одне ціле;
- персональні дані у ЕСОЗ зберігаються і обробляються в електронному вигляді;
- до складу ЕСОЗ входять дві основні складові: центральна база даних (далі – ЦБД) і електронні медичні інформаційні системи.

Ключовим документом, який регулює основні правила роботи ЕСОЗ, порядок внесення та обміну інформації в ЕСОЗ, реєстрацію користувачів є Постанова КМУ № 411 від 25.04.2018 року «Деякі питання електронної системи охорони здоров'я».

Обробка ПД в ЕСОЗ здійснюється з дотриманням вимог Закону України «Про захист персональних даних». Це означає, що правила, підстави обробки даних в ЕСОЗ, права та обов'язки ключових учасників базуються та повинні відповідати саме принципам, закладеним у Законі України «Про захист персональних даних». З іншої сторони, враховуючи специфіку ЕСОЗ, при обробці ПД можуть виникати і деякі особливості.

До роботи ЕСОЗ, як до багатофункціональної системи, залучається багато різних сторін. Тому, ключовими зацікавленими сторонами виступає широке коло суб'єктів, до яких можемо віднести:

- держава, в особі державних установ та органів, зокрема: Національної служби здоров'я України та Державного підприємства «Електронне здоров'я». Національна служба здоров'я України є розпорядником реєстрів і володільцем їх відомостей та іншої інформації у центральній базі даних. ДП «Електронне здоров'я» – адміністратором ЦБД.
- медичні інформаційні системи (далі – МІС). Саме за допомогою програмного забезпечення МІС лікарі у ЗОЗ або лікарі, які займаються

приватною практикою, мають можливість доступу до даних у ЦБД і, відповідно, до персональних даних та даних про здоров'я пацієнтів. Таким чином, МІС допомагають автоматизувати роботу медзакладів з ЦБД та є своєрідним «мостами» між ЦБД та користувачами.

- ЗОЗ, їх керівники та працівники, приватна медична практика.

З'ясувавши основні права пацієнтів щодо своїх ПД, більше детальніше розглянемо права пацієнтів як користувачів ЕСОЗ, оскільки обробка даних пацієнта в ЕСОЗ та права доступу пацієнта до цієї системи обумовлюють виникнення деяких додаткових прав.

Зокрема, Постанова КМУ № 411 від 25.04.2018 року «Деякі питання електронної системи охорони здоров'я» також передбачає:

1. Право подавати заяви про внесення змін та доповнень до відповідних відомостей, у тому числі ПД, у Реєстрі пацієнтів.
2. Зміни та доповнення до інформації, що міститься в Реєстрі пацієнтів здійснюються НСЗУ за заявою пацієнта (його законного представника).
3. Право вносити та переглядати інформацію про себе (законний представник має таке право по відношенню до пацієнта, якого він представляє). Реалізувати таке право пацієнт зможе через модуль "Електронного кабінету" після його запуску.
4. Право подавати заяву про відкликання заяви про надання згоди на обробку ПД, що міститься у центральній базі даних. Заява пацієнта (його законного представника) про відкликання заяви про надання згоди на обробку ПД, повинна бути опрацьована протягом трьох робочих днів.
5. Право надавати доступ медичним працівникам та іншим користувачам до інформації про себе (інформації про пацієнта, законним представником якого є така особа), що міститься у центральній базі даних ЕСОЗ. Доступ до даних про себе, що містяться в центральній базі даних ЕСОЗ надається на основі згоди у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди.
6. Можливість надання пацієнтами (їх законними представниками) доступу до даних про себе (про пацієнта для законних представників), що міститься в ЕСОЗ, лікарям, третім особам.
7. Право отримувати витяг з Реєстру медичних записів, записів про направлення та рецептів в ЕСОЗ (фактично отримувати інформацію про свої ПД). Витяг містить наявні відомості про пацієнта з системи відповідно до заданих критеріїв.
8. Для отримання витягу, пацієнт або його законний представник повинні звернутись з проханням (законодавство чітко не встановлює форму такого такого прохання – письмова чи усна) до медичного працівника з правом доступу до відповідних даних в системі. Медичний працівник повинен надати запитуваний витяг з Реєстру з дотриманням вимог Закону України «Про захист персональних даних».

Наведені вище права належать як пацієнтам, що отримують первинну медичну допомогу, так і пацієнтам, що отримують вторинну медичну допомогу, наприклад, проходячи реабілітацію тощо.

Відповідно до Постанови КМУ № 411 від 25.04.2018 року «Деякі питання електронної системи охорони здоров'я» пацієнт, як суб'єкт персональних даних, має наступні обов'язки:

- надання відповідному надавачу медичних послуг достовірної інформації та документів, необхідних для отримання медичних послуг та лікарських засобів. Законодавством України не передбачено адміністративної чи кримінальної відповідальності для пацієнтів за надання недостовірної інформації. Варто зауважити, що підписуючи Декларацію про вибір лікаря, пацієнт підтверджує достовірність наданих даних;
- внесення актуальних даних про себе до ЦБД ЕСОЗ.

6.6.7 Права та відповідальність медичних працівників

Окрім прав та обов'язків медичні працівники при обробці персональних даних мають ще й відповідальність.

Визначення: ***Відповідальність***
Передбачені законами негативні наслідки особистого, майнового чи організаційного характеру, яких зазнає особа за вчинення певного порушення.

Відповідальність за порушення законодавства України в сфері персональних даних включає:

1. **Дисциплінарна відповідальність.** Особа, яка допустила порушення прав пацієнта на захист ПД, може бути притягнута до дисциплінарної відповідальності відповідно до ст. 147 – 152 Кодексу законів про працю України. Наприклад, до медичного працівника може бути застосовано догану чи звільнення. Варто звернути увагу, що законодавством, статутами і положеннями про дисципліну можуть бути передбачені й інші дисциплінарні стягнення.
2. **Цивільно-правова відповідальність** передбачена ст. 1166 – 1167, ст. 1172 Цивільного кодексу України. Потерпіла особа, тобто особа, чиї права на захист ПД були порушені, може звернутися з вимогою (в т.ч. з позовом до суду) про відшкодування їй майнової та/або моральної шкоди, завданої порушенням. В такому випадку, шкода завдана медичним працівником, відшкодовується медичним закладом. В свою чергу, медичний заклад, має право зворотної вимоги до медичного працівника щодо компенсації виплаченого відшкодування.
3. **Адміністративна відповідальність** встановлена у ст. 188-39 Кодексу України про адміністративні правопорушення. Якщо недотримання законодавчих вимог щодо захисту ПД призвело до незаконного доступу до таких даних або порушення прав особи, на винних осіб (наприклад, медичного працівника) може бути накладено штраф у розмірі від 1 700 до 8 500 гривень, а у разі повторного вчинення такого порушення – штраф у розмірі від 17 000 до 34 000 гривень. Якщо порушення вчинено посадовою особою (наприклад, керівником медичного закладу), розмір такого штрафу складатиме від 5 100 до 17 000 гривень, а у разі повторного вчинення такого порушення – штраф у розмірі від 8 500 до 34 000 гривень.

4. **Кримінальна відповідальність** закріплена у ст. 145, 182 Кримінального кодексу України. Особливістю кримінальної відповідальності є те, що вона може настати лише у разі умисних неправомірних дій щодо ПД або даних про здоров'я. В якості приклада, розглянемо покарання за умисні неправомірні дії:
    - Умисні неправомірні дії щодо конфіденційної інформації (ст. 182 Кримінального кодексу України). За такі дії може наступати відповідальність у формі штрафу від 8 500 грн до 17 000 грн, або виправних робіт на строк до 2 років, або арешту на строк до 6 місяців, або обмеження волі на строк до 3 років (в окремих випадках арешт на строк від 3 до 6 місяців), або в окремих випадках, обмеженням або позбавлення волі від 3 до 5 років. Відповідальними за умисні неправомірні дії щодо конфіденційної інформації (ст. 182 ККУ) можуть бути будь-які працівники медичного закладу, які вчинили такі дії.
    - Умисні неправомірні дії щодо інформації, що становить лікарську таємницю, якщо це спричинило тяжкі наслідки (ст. 145 Кримінального кодексу України). Такі дії можуть проявлятися у розголошенні лікарської таємниці або порушенні обов'язку щодо захисту персональних даних (наприклад, незаконне збирання, зберігання, використання, знищення, розкриття персональних даних третім особам). Тяжкими наслідками може вважатися звільнення з роботи, самокалічення або погіршення здоров'я особи, інформація щодо якої розголошена. Питання про визнання наслідків тяжкими повинне вирішуватись індивідуально у кожній справі з урахуванням усіх обставин. Відповідальність за такі дії може бути у вигляді штрафу від 17 000 грн до 68 000 грн, або громадських робіт на строк до 240 годин, або позбавлення права обіймати певні посади чи займатися певною діяльністю на строк до 3 років, або виправні роботи на строк до двох років.

Важливо наголосити, що кримінальна відповідальність та адміністративна не можуть застосовуватись одночасно за одне й те саме діяння.

Наприклад, медичний працівник допустив розголошення персональних даних, що становлять лікарську таємницю, чим порушив законодавство про захист персональних даних. Як наслідок, до нього може бути застосовано адміністративне або кримінальне покарання разом з майновою та дисциплінарною відповідальністю. При цьому, конкретний вид відповідальності за порушення законодавства в сфері ПД залежатиме від характеру вчиненого діяння, ступеня вини порушника, інших обставин та повинен бути проаналізований індивідуально в кожному випадку.

Варто зазначити не лише про відповідальність, але й про право медичних працівників на судовий захист. У разі порушення пацієнтами прав медичних працівників, медичні працівники мають право на судовий захист професійної честі та гідності (ст. 77 Закону України "Основи законодавства про охорону здоров'я"). Крім того, лікар має право відмовитись від подальшого ведення пацієнта, якщо останній не виконує медичних приписів або правил внутрішнього трудового розпорядку ЗОЗ, однак за умови, що це не загрожуватиме життю хворого і здоров'ю населення (ч. 4 ст. 34 Закону України "Основи законодавства про охорону здоров'я").

Кращі практики та рекомендацій

На практиці можуть траплятись нестандартні ситуації, які з недостатньою чіткістю врегульовані законодавством, або ситуації, коли медичний працівник сумнівається, як правильно працювати з ПД. У таких випадках, необхідно звертатися за кваліфікованою порадою до юристів, відповідального за обробку ПД у закладі (якщо він призначений), керівника ЗОЗ. Також, корисним може бути пошук роз'яснень в Уповноваженого ВРУ з прав людини.

6.6.8 Висновки

Законодавство не містить вичерпного переліку поняття ПД. Термін «персональні дані» охоплює всю інформацію, що дозволяє ідентифікувати конкретну особу.

Медичні дані, та лікарська таємниця становлять особливі категорії ПД конфіденційність яких повинна особливо оберігатись.

Працівники медичних закладів та інші особи, що отримують доступ до ПД пацієнтів, повинні дотримуватись конфіденційності ПД, не допускати їхнього розголошення та надавати доступ до ПД пацієнтів третім особам лише у випадках, що передбачені законодавством.

Базовим документом, який встановлює правове регулювання персональних даних є Закон України «Про захист персональних даних». При цьому, зважаючи на особливості функціонування ЕСОЗ, деякі особливості обробки ПД, прав пацієнтів наявні зазначені в Постанові КМУ № 411 від 25.04.2018 року «Деякі питання електронної системи охорони здоров'я».

За порушення правил обробки та захисту ПД (залежно від порушення та його наслідків) може наступати адміністративна; кримінальна; дисциплінарна та майнова відповідальність

Корисні посилання

- Закон України «Про інформацію»
- Закон України «Про захист персональних даних»
- Закон України «Основи законодавства України про охорону здоров'я»
- Закон України «Про державні фінансові гарантії медичного обслуговування населення»
- Типовий порядок обробки персональних даних у базах персональних даних
- Постанова КМУ № 411 від 25.04.2018 року «Деякі питання електронної системи охорони здоров'я»
- «Роз'яснення основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних»
- Бем М., Городиський І. Захист персональних даних: правове регулювання та практичні аспекти: науково-практичний посібник