НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВОДНОГО ГОСПОДАРСТВА ТА ПРИРОДОКОРИСТУВАННЯ
Навчально-науковий економіки та менеджменту
Кафедра менеджменту та публічного врядування

Пояснювальна записка
до кваліфікаційної магістерської роботи

на тему «Особливості реалізації безпекових стандартів в закладах охорони здоров'я (на прикладі Комунального підприємства «Рівненська обласна клінічна лікарня імені Юрія Семенюка" Рівненської обласної ради)»

Виконав:студент 2 курсу,
групи ПУА-61м
спеціальності 281 «Публічне управління та адміністрування»
Бабич Сергій Васильович
Керівник: к.і.н., доцент
Цецик Я. П.
Рецензент: Доцент, К.ДЕРЖ.УПР
Вівсяник О. М.

Рівне – 2024

Звіт подібності

метадані

Заголовок
проект-магістерська бабич с..docx

Автор
Бабич Сергій Васильович

Науковий керівник / Експерт
Бабич Сергій Васильович

підрозділ
National University of Water and Environmental Engineering

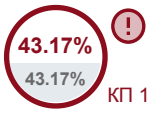
Тривога

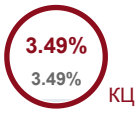
У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв	ß	19
Інтервали	A⟶	4
Мікропробіли	·	176
Білі знаки	ß	0
Парафрази (SmartMarks)	a	314

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.





25
Довжина фрази для коефіцієнта подібності 2

25766
Кількість слів

197090
Кількість символів

Подібності за списком джерел

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз — Колір тексту

ПОРЯДКОВИЙ НОМЕР	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)	
1	https://zakononline.com.ua/documents/show/500068___767586	340	1.32 %
2	https://krs.chmnu.edu.ua/jspui/bitstream/123456789/3131/1/%D0%9A%D0%92%D0%90%D0%9B%D0%86%D0%A4%D0%86%D0%9A%D0%90%D0%A6%D0%86%D0%99%D0%9D%D0%90%20%D0%A0%D0%9E%D0%91%D0%9E%D0%A2%D0%90%20%D0%92%D0%B0%D1%81%D0%B8%D0%BB%D0%B5%D0%BD%D0%BA%D0%BE.pdf	334	1.30 %
3	https://krs.chmnu.edu.ua/jspui/bitstream/123456789/3131/1/%D0%9A%D0%92%D0%90%D0%9B%D0%86%D0%A4%D0%86%D0%9A%D0%90%D0%A6%D0%86%D0%99%D0%9D%D0%90%20%D0%A0%D0%9E%D0%91%D0%9E%D0%A2%D0%90%20%D0%92%D0%B0%D1%81%D0%B8%D0%BB%D0%B5%D0%BD%D0%BA%D0%BE.pdf	268	1.04 %

ЗМІСТ

ГЛОСАРІЙ ТА УМОВНІ СКОРОЧЕННЯ

Анонімайзер – веб-сайт, який допомагає користувачу опосередковано отримати доступ до інших інтернет-сайтів, приховуючи свою особистість.

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.

Відповідальність – передбачені законами негативні наслідки особистого, майнового чи організаційного характеру, яких зазнає особа за вчинення певного порушення.

Вішинг – це різновид фішингу, але контакт з користувачем встановлюється за допомогою засобів голосового зв'язку (дзвінок по телефону або засобами Інтернет-телефонії).

Володілець персональних даних – фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом.

Доступність інформації – властивість, яка гарантує те, що забезпечується своєчасний доступ авторизованих осіб і/або процесів до інформації, а також відсутні затримки в процесі її обробки.

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.

Е-здоров’я, або eHealth – сфера електронної охорони здоров’я.

Захист інформації – сукупність правових, адміністративних, організаційних, технічних й інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

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.

Кібератака – навмисне втручання в роботу комп'ютерних систем, мереж або отримання несанкціонованого доступу до систем та даних.

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.

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

Кіберстійкість – можливість системи або організації функціонувати на належному рівні та досягати поставлених цілей, не дивлячись на спроби кібератак, які на неї можуть здійснюватися.

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.

Конфіденційна інформація – інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень.

Конфіденційність інформації – властивість, яка гарантує те, що доступ до інформації можуть одержати тільки авторизовані особи або процеси.

Культура кібербезпеки – це набір припущень, уявлень, ставлення до предметної області, моделей поведінки та робочих звичок, які підсилюють кібербезпеку організації.

Лікарська таємниця – включає в себе відомості про: хворобу, результати медичного обстеження, оглядів та їхні результати, інтимну і сімейну сторони

життя громадянина, 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.

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.

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.

Одержувач – фізична чи юридична особа, якій надаються персональні дані, у тому числі третя особа.

Персональні дані (ПД) – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

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.

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.

Принцип Демінга-Шухарта (цикл PDCA) – алгоритм дій по управлінню процесом з метою його вдосконалення, що включає етапи: Планування, Виконання, Перевірка, Коригування.

Принцип Керкгоффза – у спрощеній формі принцип можна пояснити наступним чином: вартість системи захисту інформації не повинна бути дорожчою за цінність інформації, яку вона захищає.

Розпорядник персональних даних – фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця.

Суб'єкт персональних даних – фізична особа, персональні дані якої обробляються.

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

Третя особа – будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника персональних даних та Уповноваженого Верховної Ради України з прав людини, якій володільцем чи розпорядником персональних даних здійснюється передача персональних даних.

Троянський кінь – вид шкідливого програмного забезпечення, яке для потрапляння на цільову комп'ютерну систему потребує активних дій користувача.

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.

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.

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

ВСТУП

Актуальність теми. Відомо, що безпека інформації, особливо персональних даних, важлива для кожного окремо та для всіх людей, корпорацій, установ та організацій, у секторі охорони здоров'я існують спеціальні вимоги, які повинні бути виконані для забезпечення конфіденційності, цілісності, доступності та звітність про особисте здоров'я або конкретну інформацію або категорії персональних даних. Цей тип інформації вважається одним із найбільш конфіденційних з усіх видів особистої інформації. Захист конфіденційності важливий для збереження конфіденційності компонентів догляду. Цілісність медичної інформації має бути захищена для забезпечення безпеки пацієнтів, і одним із важливих компонентів забезпечення безпеки цієї інформації є забезпечення ретельного аудиту всього життєвого циклу інформації. Доступність медичної інформації також має вирішальне значення для ефективної медичної допомоги. IT-системи повинні відповідати особливим вимогам, щоб мати можливість забезпечити безперервність роботи в разі збоїв, кризових ситуацій, стихійних лих і різного роду атак. Таким чином, захист конфіденційності, цілісності та доступності медичної інформації вимагає спеціальних знань у галузі охорони здоров'я.

В роботі оглянуто питання кібербезпеки в сфері електронної охорони здоров'я, що є екосистемою інформаційних відносин учасників медичного середовища держави, які базуються на економічно ефективному та безпечному використанні інформаційно-комунікаційних технологій, спрямованих на підтримку системи охорони здоров'я, включаючи медичні послуги, профілактичний нагляд за здоров'ям, медичну літературу та медичну освіту, знання та дослідження.

Досліджуються питання реалізації безпекових стандартів в межах сфери електронної охорони здоров'я (далі – Е-здоров'я, або eHealth). Ціллю даної реалізації є підвищення рівня кібербезпеки в закладах охорони здоров'я (далі – ЗОЗ) відповідно регламентуючої документації щодо цього питання та Плану заходів щодо реалізації Концепції розвитку охорони здоров'я, затвердженого розпорядженням Кабінету Міністрів України від 29.09.2021 року № 1175-р, зокрема.

Дослідження, в межах виконання магістерської роботи, були на підставі отриманих знань під час проходження навчання на магістратурі в складі групи ПУА61м. В роботі, також, використовуються дослідження зі статей, що були підготовлені протягом навчального процесу.

Метою роботи є дослідження підвищення рівня кібербезпеки в закладах охорони здоров'я шляхом впровадження ризик-орієнтованого підходу управління інформаційною безпекою стандарту ISO 27001 з використанням спеціального стандарту ISO 27799 та порівнянням його з уніфікованою версією ISO 27002.

Завдання дослідження, що були поставлені в цілях досягнення мети роботи:

– провести аналіз сфери питання кібербезпеки в сфері охорони здоров'я;

– визначити сутність захисту інформації та роботи з персональними даними у закладі охорони здоров'я;

– дослідити організаційно-правове забезпечення сфери захисту інформації та роботи з персональними даними в закладах охорони здоров'я;

– проаналізувати іноземний досвід питань кібербезпеки в закладах охорони здоров'я;

– з'ясувати зміни в сфері стандартів кібербезпеки, що можуть бути застосовані в закладах охорони здоров'я, зокрема – огляд стандарту ISO 27799 як розвиток ISO 27002 для закладів охорони здоров'я;

– провести аналіз ефективності імплементації безпекового стандарту ISO 27001 в закладах охорони здоров'я, а саме – версії ISO 27799 для закладів охорони здоров'я ;

– охарактеризувати особливості імплементації стандарту ISO 27799 в закладі охорони здоров'я;

– провести аналіз переваг та перспектив імплементації стандарту ISO 27799 в закладі охорони здоров'я.

Об'єкт дослідження – процес реалізації захисту інформації та роботи з персональними даними у закладі охорони здоров'я з використанням безпекового стандарту ISO 27799.

Предмет дослідження – загальна сукупність теоретичних та практичних інструментів регулювання кібербезпеки в закладах охорони здоров'я та супровідних стандартів щодо реалізації даного питання.

Теоретична основа і ступіть висвітлення проблеми дослідження у науковій літературі. Над теоретико-методологічною складовою формування та цифрового впровадження в медицині працює ряд дослідників, науковців та докторів як закордонних, так і українських, а саме: В. Бадянов – експерт з Е-здоров'я в Україні, О. Голубовська – вчена у сфері медичної інформатики та біомедичної статистики, О. Трофименко, І. Волинець, А. Стрєлкіна, Б. Коваль та інші – досліджують безпекові питання в сфері медичних систем та охорони здоров'я. Інші дослідження оглянуті в пункті 1.2.2..

Практичне значення результатів дослідження зосереджене у практичних рекомендаціях щодо імплементації стандартів ISO 27001 та ISO 27799 в цілях підвищення рівня кібербезпеки закладу охорони здоров'я. Як результат даних практичних рекомендацій – сформовані типові політики безпеки, у відповідності до стандарту.

Структура роботи. Робота складається із вступу, трьох розділів та висновків до них, загального висновку та списку використаної в роботі літератури, а також додатків з рекомендованими типовими політиками безпеки.

Методологічна основа дослідження: у процесі написання роботи використано сукупність загальнонаукових і спеціальних методів: за допомогою діалектичного методу наукового пізнання проаналізовано поняття та сутність об'єкту дослідження, структурно-функціональний метод застосовувався під час дослідження його складових, абстрактно-логічний, для визначення сутності кібербезпеки в даній сфері, статистичний метод був використаний для аналізу статистичних даних з питань кіберзахисту в закладах охорони здоров'я, статистико-математичний для оцінки сучасного стану та стратегій імплементації безпекових стандартів, як об'єкту дослідження.

Інформаційна база дослідження: нормативно-правові акти центральних органів влади, що безпосередньо регулюють питання кібербезпеки в сфері Е-здоров'я. Особливої уваги надано документальній базі на сайті Міністерства охорони здоров'я України та Постановам Кабінету Міністрів України, що регулюють сферу оглянутих в роботі питань. Важливу роль займають аналітичні огляди стандартів ISO 27001, ISO 27002, ISO 27799 та екосистему нормативно-правової документації як запити та рекомендації щодо їх імплементації. Аналіз вищесказаного створив умови щодо цілісного дослідження питання імплементації безпекових стандартів кібербезпеки в закладах охорони здоров'я.

РОЗДІЛ 1
ТЕОРЕТИЧНЕ ПІДГРУНТЯ РЕАЛІЗАЦІЇ БЕЗПЕКОВИХ СТАНДАРТІВ В ЗАКЛАДАХ ОХОРОНИ ЗДОРОВ'Я

Кібербезпека – це не продукт.

Кібербезпека – це процес.

Кібербезпека у сфері охорони здоров'я стає одним із ключових питань для медичних закладів та держави. Розвиток електронної охорони здоров'я та активна цифровізація процесів вимагають від медичної спільноти не лише цифрових знань і навичок, а й знань щодо основ кібербезпеки і навичок захисту власних даних і даних пацієнта у цифровому просторі [1].

Кіберзахист – це захист цифрової інформації, що передбачає такі заходи, як захист від вірусів, хакерських атак, запобігання підробці даних та іншим діям, наслідками яких можуть бути не тільки видалення або викрадення даних, а й потенційно шкідливий вплив на роботу і продуктивність співробітників закладу охорони здоров'я, використання незаконно отриманої інформації проти фізичної чи юридичної особи, зупинка процесу надання медичної допомоги та пов'язаних послуг, тощо [1-4].

Кібербезпека - це захищеність комп'ютерних інформаційних пристроїв та систем від несанкціонованого доступу, що забезпечує конфіденційність, цілісність та доступність інформації як основ кіберзахисту [1 - 4].

Сфера охорони здоров'я - одна із лідерів у світі за зростанням кількості кібератак. У 2022р. на тиждень відбувалось 1463 кібератаки, що на 74% більше, ніж у 2021р. [1]. Витоки даних у медичній сфері найдорожчі - у середньому вони обходились медичним закладам західних країн у $10 млн [5].

Як показують порушення, про які повідомляють ЗМІ, вразливості кібербезпеки використовуються. Охорона здоров'я наразі є однією з найбільш цільових галузей.

Звіти підкреслюють зростання кількості нападів і зростання кількості крадіжок медичних даних – мільйони медичних записів були викрадені по всьому світу [6-10].

Електронна система охорони здоров'я зберігає та обробляє медичні дані мільйонів українських пацієнтів. Вона надійно захищена. Персональні та медичні дані українців зберігаються в реєстрах у центральній базі даних, для них створено систему захисту інформації. Відповідальність за захист окремих медичних інформаційних систем несуть їхні розробники. Однак і медичні заклади відповідають за виконання передбачених угодою із МІС вимог щодо безпечної експлуатації цих систем. Але завжди слабкою ланкою будь-якої системи є людина. 61% кібератак у медичній сфері відбувається через недотримання правил кібербезпеки користувачами [1].

В даній роботі оглянуто кібербезпеку як загрозу для критичної інфраструктури країни, в котрій триває війна. Підвищення якостей кібербезпеки, на даний час, не носить точно виокремлений та єдино-систематизований характер, хоча, в більшості випадків, буде йти мова про стандарт ISO 27001 [2; 10], як сертифікаційну основу та стандарт ISO 27002 [3; 11] як методики її імплементації. В даній роботі оглянуто рекомендаційні конфігурації від Міністерства Охорони Здоров'я України та стандарт ISO 27799 зокрема [4], що надає вказівки для медичних організацій та інших організацій, які обробляють особисті дані, пов'язані зі здоров'ям, щодо того, як найкраще захистити конфіденційність, цілісність і доступність такої інформації. Стандарт ISO 27799 ґрунтується [4] на загальних рекомендаціях, що містяться в ISO 27002: 2016 [3; 4], і розширює їх, враховуючи особливі потреби управління інформаційною безпекою в секторі охорони здоров'я та його унікальних робочих середовищах. В свою чергу ISO 27001 [2; 10] береться в редакції ISO 27001:2022 [2; 10; 11], як найбільш новітню версію імплементації в Україні відповідно до ДСТУ ISO 27002:2023 [11; 12].

Кроки для впровадження ISO 27799 є типовими для усього сімейства ISO 27000 (а тому, більшість процедур та політик будуть типовими з точки зору уніфікованого характеру документів):

Крок 1 : Попередній аудит і оцінка впровадження ISO 27799;

Крок 2 : Розробка та впровадження документації системи управління інформаційною безпекою

Крок 3: Розробка та впровадження схеми управління інцидентами та нагляду

Крок 4: Навчання внутрішніх аудиторів, керівництва та персоналу

Крок 5: Інформація про аудит системи менеджменту безпеки

Крок 6: Коригувальні дії

1.1. Теоретично-нормативне обґрунтування питання кібербезпеки в закладах охорони здоров’я та сфері електронної охорони здоров’я

Перш за все, варто окреслити межі кібербезпеки в сфері eHealth, так як це достатньо екзотичне місце застосування безпекових стандартів в Україні (як за регламентуванням зі сторони нормативно-правової бази так й за успішним й централізованим досвідом імплементації ефективних рішень). Побудова системи кібербезпеки в ЗОЗ передбачає ряд організаційних та технічних заходів, включно навчання і підвищення обізнаності серед широкого кола працівників організації. Саме недостатня обізнаність працівників і низький рівень загальної цифрової грамотності стає «слабким місцем». З іншого боку проінформований персонал створює перший ешелон захисту за допомогою дотримання простих повсякденних правил поведінки з інформацією в цифровому вигляді. Наявність розуміння потреби в захисті інформації та знання простих правил для його підтримки – ключові складові культури кібербезпеки в ЗОЗ [1].

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 необхідно за стислий термін пройти ті ж етапи еволюції в області безпеки інформації, що відбувалися у фінансовому секторі та державних установах впродовж останніх п'ятдесяти років.

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».

1.1.1. Вступ до кібербезпеки в сфері Е-здоров’я.

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

З огляду на це заклади і установи повинні впроваджувати політики та правила кібербезпеки, що допоможе знизити до мінімуму результати кібератак. Заклади повинні дотримуватись нормативно-правових вимог для захисту конфіденційних даних пацієнтів, а також відповідати певним міжнародним вимогам, таким як Загальний регламент захисту даних (GDPR). Цей регламент вимагає від організацій, які володіють, обробляють та зберігають персональні дані громадян держав-учасниць ЄС, вжити ряд заходів з кібербезпеки [13].

У питаннях кібербезпеки фундаментальним завданням є розуміння яка саме інформація обробляється і зберігається в інституції, та від яких негативних факторів її необхідно захищати. Визначення цих критеріїв називається моделюванням загроз [14; 15].

Типові загрози безпеці інформації – це загрози викрадення, пошкодження, змінення або знищення інформації. Крім того, цифрові пристрої можуть бути зламані і це може завдати прямої шкоди пацієнтам [14].

Стан захищеності інформації визначають через наступні параметри – **конфіденційність**, **цілісність** та **доступність** інформації, а отже, до складових кібербезпеки входить гарантування відповідних якостей цифрових активів [1].

1.1.2. Параметри захищеності інформації в сфері Е-здоров'я.

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 [16].

Працівники закладів повинні знати про чутливий характер медичних і персональних даних, що отримує заклад 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.

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 [16].

На практиці це означає, що лікар повинен мати можливість отримати доступ до електронної 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 хосту тощо).

Для можливості відновлення даних пацієнтів, що зберігаються у закладах, 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 [16].

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 [17]. 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.

Окремо варто уваги і хакерська атака з боку країни-агресора проти України в 2017 році [18] з використанням вірусу Petya, XData та інших. Масштабна деструктивна атака завдала шкоди близько 10% персональним комп’ютерам в країні і вразила ті сфери та галузі, що найменш були захищені безпековими протоколами та процедурами, в тому числі і галузь охорони здоров’я [18].

Відповідно до нормативно-правових вимог керівництво ЗОЗ несе повну відповідальність за підтримання належного рівня інформаційної безпеки закладів [14; 15].

1.1.3. Захист інформації при роботи з даними в сфері Е-здоров'я.

Виходячи з визначення належного рівня інформаційної безпеки, а саме такого стану, що 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 збереженні, а також при передачі чи обробці (див. рис. 1.1).

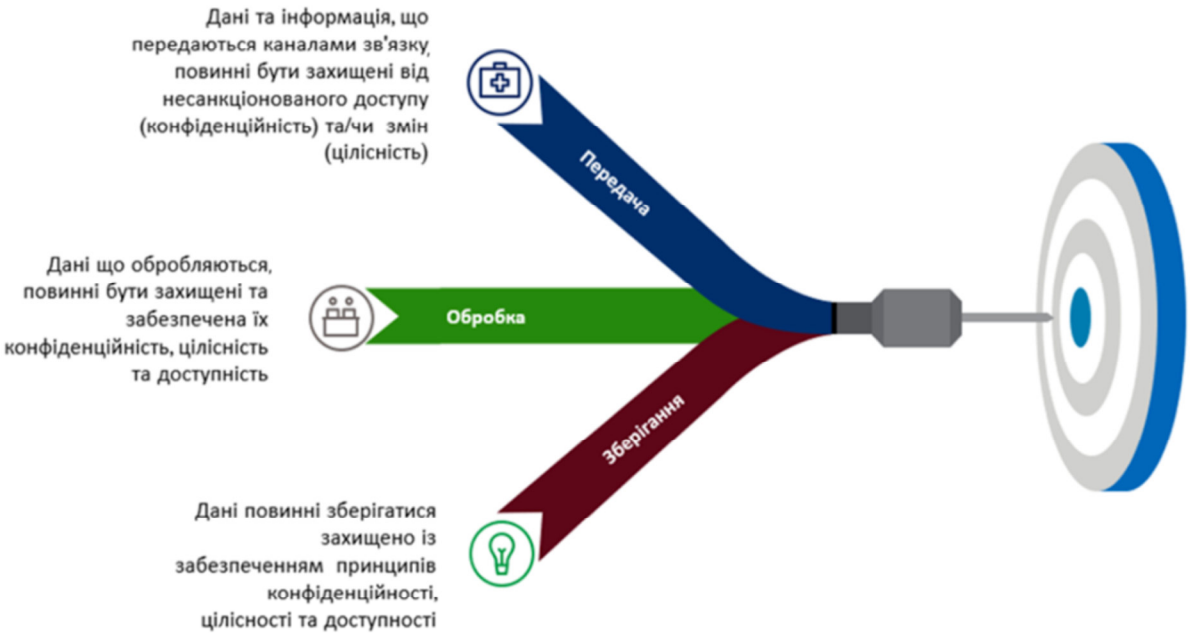


Рис. 1.1 Спостережність та контрольованість інформаційних систем (джерело: офіційний сайт МОЗ України)

Дані й інформація, що передаються каналами зв'язку, повинні бути захищені від несанкціонованого доступу (забезпечена конфіденційність) та/чи змін (цілісність). 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 в такий

спосіб, щоб було забезпечено виконання принципів інформаційної безпеки із забезпечення конфіденційності, цілісності та доступності [14; 15].

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 зберігання.

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 [19]. 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 [20].

Куб МакКамбера — це спосіб оцінки системи безпеки з огляду на всі її аспекти [21]. 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 зберіганні. Третя видима поверхня цього кубу відноситься до складових, пов’язаних із управлінням людьми, процесами і технологіями (див. рис. 1.2).

Рис. 1.2 Куб кібербезпеки або куб МакКамбера

Окремо варто зупинитись на зазначеній посадовій особі, що контролює всю поточну діяльність, пов'язану з розробкою, впровадженням та підтримкою політики інформаційної безпеки ЗОЗ, так як дана особа ще й забезпечує

дотримання належного рівня кіберзахисту, оптимізує методи цифрового захисту та ефективно використовує наявні ресурси.

1.1.4. Відповідальність в сфері кіберзахисту Е-здоров’я.

Рекомендується, щоб відповідальним за інформаційну безпеку (ВІБ) був заступник керівника ЗОЗ [1 – 4]. 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. рис. 1.3). 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 – Service-Level-□greement (SL□) [1; 10; 14; 22].

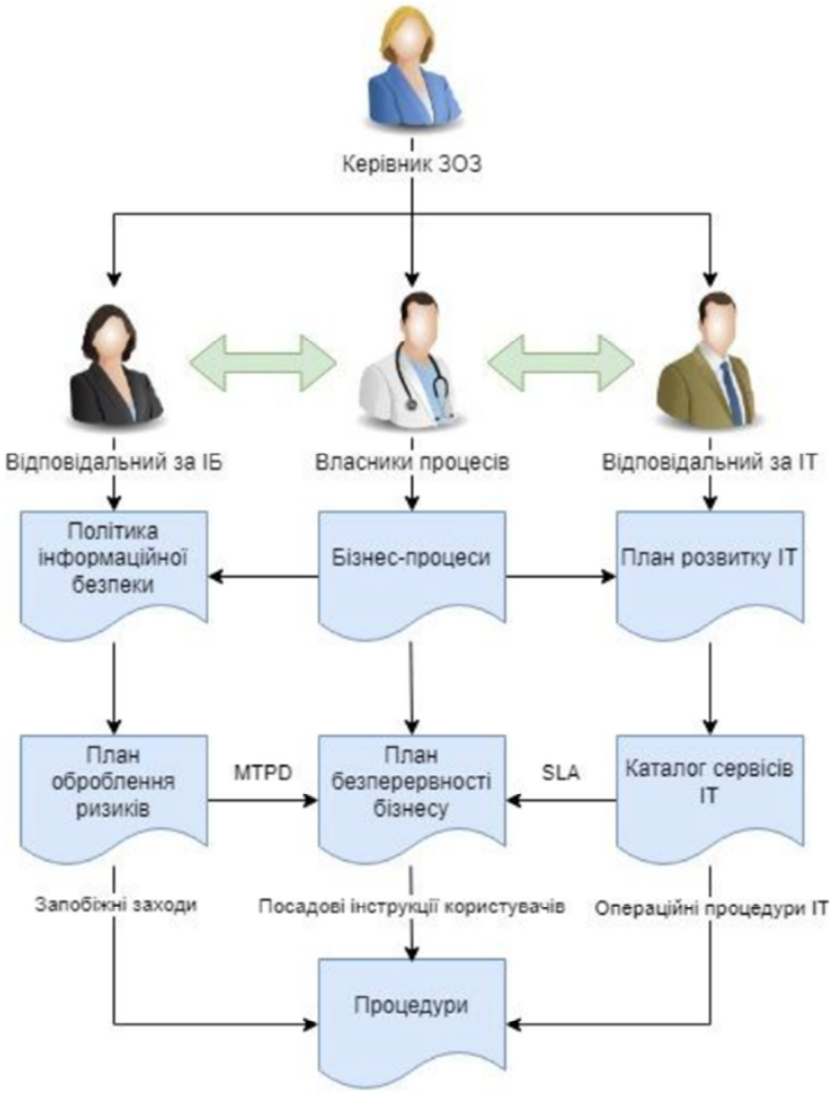


Рис. 1.3 Можливий розподіл відповідальності та повноважень щодо інформаційної безпеки між посадовими особами закладу

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 буде необхідно припинити надавати окремі ІТ-сервіси, щоб запобігти ризикам інформаційної безпеки. Саме таке протиріччя краще всього вирішується розподіленням повноважень та ескалацією ухвалення 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 [1; 6; 14; 15].

1.1.5. Процеси кібербезпеки в сфері Е-здоров’я.

Підвищення обізнаності і навчання працівників принципам кібербезпеки – один з багатьох напрямів роботи ВІБ. Проте головним завданням ВІБ є побудова ефективної системи кіберзахисту. Для практичної реалізації зазначеного завдання існують стандарти з кібербезпеки: одним з них є NIST Cybersecurity Framework («Рамкова модель кібербезпеки NIST») [24]. Відповідно до стандарту кібербезпеку організації потрібно забезпечувати циклічно, виконуючи певні процеси (див. рис. 1.4):

Рис. 1.4 Забезпечення кібербезпеки відповідно до NIST

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 [25].

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 [25].

Виявлення. Відноситься до подій інформаційної безпеки та ідентифікації 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 [25].

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 [25].

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 [25].

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.

Головний процес забезпечення інформаційної безпеки організації складається із організації трьох рівнів захисту: фізичного (передбачає різні фізичні елементи, які запобігають вторгненню, — це охоронці, камери відеоспостереження, замкнені двері, системи біометричної перевірки тощо), адміністративного (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) та технологічного.

1.1.6. Технології кіберзахисту в сфері електронного здоров’я.

Технологічна складова кіберзахисту включає всі комп‘ютерні і програмні ресурси, які використовуються для забезпечення спостережності інформаційних систем та зменшення ризиків інформаційної безпеки [14; 15].

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 та 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 пристрої 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 [26]. 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 [14; 15].

1.1.7. Захист персональних даних в сфері електронного здоров’я.

Із впровадженням електронної системи охорони здоров’я питання захисту персональних даних 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 інформації про пацієнтів, стан їхнього здоров’я і деталей лікування може призвести до негативних наслідків для пацієнта, працівника закладу, з вини якого стався такий витік, а також закладу охорони здоров'я в цілому. Саме тому забезпечення належного рівня захисту ПД пацієнтів є важливим аспектом при роботі з ЕСОЗ.

Кожна особа є суб’єктом персональних даних, таких як ім’я, дата народження, номер телефону тощо. У контексті теми цього документа найчастіше суб’єктом ПД виступає саме пацієнт.

Основною вимогою до всіх осіб, які здійснюють обробку ПД, є забезпечення належного захисту ПД для того, щоб треті особи не отримали доступу до ПД. Для того, щоб створити та забезпечити механізм захисту ПД, діюче законодавство України ставить низку вимог до володільців та розпорядників, зокрема [14; 15; 27]:

– 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, 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, 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 потрібно також враховувати ці строки, а також встановлені строки для зберігання інших документів.

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 [27; 28]:

– права, що пов’язані з доступом до даних;

– права, що пов’язані з розпорядженням даними;

– права, що пов’язані з захистом ПД.

1.1.8. Особливості захисту персональних даних при роботі з електронною системою охорони здоров’я.

З вищенаведеного можна підкреслити такі ознаки ЕСОЗ:

– інформаційно-комунікаційна 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 – є постанова [29].

Обробка ПД в ЕСОЗ здійснюється з дотриманням вимог [27].

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 органів

– Медичні інформаційні системи (далі – МІС). Саме за допомогою програмного забезпечення МІС лікарі мають можливість доступу до даних у ЦБД і, відповідно, до персональних даних та даних про здоров’я пацієнтів.

Таким чином, МІС допомагають автоматизувати роботу медичних закладів та є своєрідними «мостами» між ЦБД та користувачами.

– Заклади охорони здоров'я, їх керівники та працівники.
– Пацієнт.

1.1.9. Огляд безпекових стандартів ISO 27001, ISO 27002, ISO 27779.

Щоб належним чином та ефективно захистити інформацію, слід дотримуватися належної практики управління інформаційною безпекою: з цією метою Міжнародна організація стандартизації (ISO) опублікувала кодекс практики управління інформаційною безпекою, а саме ISO 27002 [3]. Цей стандарт широко використовується в промисловості, але є загальним стандартом, призначеним для всіх галузей. Тому він не враховує унікальні потреби безпеки певного середовища [30; 31]. Варто зауважити, що сертифікація як така – відбувається саме на підставі сертифікату ISO 27001, але саме версія ISO 27002 слугує, в більшій мірі, методичним керівництвом щодо імплементації та подальшої сертифікації [2 - 3].

Через унікальну природу особистої медичної інформації та вимог до її безпеки та конфіденційності було визначено потребу запровадити спеціальний стандарт охорони здоров’я для управління інформаційною безпекою. Таким чином, стандарт ISO 27799 опублікований як галузевий варіант стандарту ISO 27002, що спрямований на вирішення вимог безпеки з медичними даними [4]. Він слугує посібником щодо впровадження ISO 27002 у сфері Е-здоров’я.

Відповідно до даних досліджень, можна стверджувати, аби відповідати вимогам законодавства та продемонструвати, що до захисту даних ЗОЗ було належну обережність можна застосувати шляхом впровадження певної форми передового досвіду захисту критично важливих інформаційних активів компанії. Цього можна досягти за допомогою стандартів або інструкцій з управління інформаційною безпекою (ISM). Широко відомі приклади стандартів ISM включають:

ISO 27002: Кодекс практики управління інформаційною безпекою, який встановлює керівництво та загальні принципи для ініціювання, впровадження, підтримки та вдосконалення управління інформаційною безпекою в організації.

ISO 27001: Вимоги до систем управління інформаційною безпекою, який визначає вимоги до створення, впровадження, експлуатації, моніторингу, перегляду, підтримки та вдосконалення задокументованої системи управління інформаційною безпекою в контексті загальних бізнес-ризиків організації.

Хоча назва ISO 27799 відноситься лише до ISO 27002, у стандарті зазначено, що: «ISO 27799 не призначений для заміни ISO 27002 або ISO 27001. Скоріше він є доповненням до цих більш загальних стандартів» [4].

Таким чином, стандарт також намагається розглянути впровадження системи управління інформаційною безпекою (СУІБ), а не розглядати СУІБ в окремому стандарті, як це було зроблено в ISO 27001.

1.2. Принципи імплементації системи кіберзахисту з використанням безпекових стандартів в закладах охорони здоров'я

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 [11; 14 -16]. 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 [32]. 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 доступом. 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 зустрічаються у закладах (див. рис. 1.5, 1.6). 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 [14; 15].

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 [27]. 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. Таку інформацію забороняється вимагати та подавати за місцем роботи або навчання [33].

Рис. 1.5 Співвідношення різних видів інформації
(джерело: офіційний сайт МОЗ України)

Рис. 1.6 Співвідношення лікарської таємниці з персональними і чутливими даними
(джерело: офіційний сайт МОЗ України)

Умови та випадки, за яких дозволяється розкриття лікарської таємниці, передбачені у різних актах.

А ось результати медичного обстеження є таємницею і повідомляються лише нареченим [34]. 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. Отже, до інформації з обмеженим доступом, яка обробляється закладами, застосовуються додаткові вимоги щодо її захисту.

Основи захисту такої інформації встановлені у наступних законодавчих документах:

– Закон України «Про інформацію» [32];

– Закон України «Про захист персональних даних» [27];

– Закон України «Основи законодавства України про охорону здоров'я» [35];

– Типовий порядок обробки персональних даних у базах персональних даних [36].

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 [10]:

– Моделювання загроз;

– Аналіз впливу;

– Оцінка вірогідності.

Під моделюванням загроз розуміють експертну оцінку того, які саме види та варіації кібератак є можливими та релевантними. Формується 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 [37]:

– Принцип процесного підходу
– Принцип ешелонованого захисту

Процесний підхід. Хорошою практикою вважається побудова системи кіберзахисту як сукупності взаємопов'язаних процесів. Популярною моделлю для цього є СУІБ – система управління інформаційною безпекою, побудованою на основі [10]. Відповідно до даного стандарту ISO, у 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.

Ешелонований підхід. 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, недосконаліть

або відмову в спрацюванні одного рівня захисту необхідно компенсувати побудовою додаткового механізму кібербезпеки.

В сфері кібербезпеки, прикладом є навчання користувачів навичкам кібергігієни з одного боку, та розгортання системи автоматичного маркування підозрілих електронних листів з другого [14; 15; 37].

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.

1.2.1. Подальший розвиток системи кібербезпеки в ЗОЗ.

Розбудова системи кібербезпеки – це поетапний процес. Після впровадження базових заходів організації слід переходити до планування побудови посилених механізмів кібербезпеки [1; 37].

Оскільки впровадження і розвиток системи кібербезпеки потребує певних фінансових та часових інвестицій, важливо при плануванні цільового стану кібербезпеки керуватися принципом Керкгоффза. Для того, щоб організації мали спільний орієнтир при розвитку системи кібербезпеки, хорошою практикою вважається застосування моделей зрілості системи кібербезпеки.

Моделі зрілості мають характер набору характеристик, практик та процесів у стилі «Повзи/Йди/Біжи» та слугують інструментом для порівняння поточних можливостей і визначення цілей та пріоритетів для вдосконалення (див. рис. 1.7).

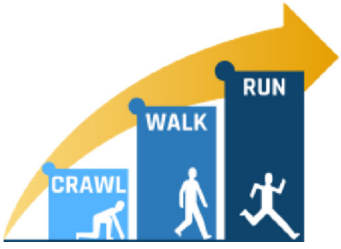


Рис. 1.7 Бачення практик та процесів у стилі «Повзи/Йди/Біжи» для моделі зрілості систем кібербезпеки
(джерело: офіційний сайт МОЗ України)

Модель зрілості системи кібербезпеки допомагає вирішити низку таких завдань: 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 (див. таблиця 1.1):

– Cybersecurity Capability Maturity Model – C2M2 [38];
– NIST Cybersecurity Framework [24; 25];
– Cybersecurity Maturity Model Certification [39].

Таблиця 1.1

Порівняльна характеристика моделей зрілості системи кібербезпеки

Назва моделі	**Cybersecurity Capability Maturity Model**	**NIST Cybersecurity Framework**	**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

Джерело: складено на основі [24; 25; 38; 39]

Розглянемо 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 (див таблиця 1.2).

Таблиця 1.2

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 [24; 25; 38; 39].

У менеджменті популярною методологією безперервного вдосконалення процесів є Принцип Демінга-Шухарта, також відомий як принцип або цикл PDC□: Plan-Do-Check-□ct – Плануй-Роби-Перевіряй-Дій.

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 (див. рис.1.8) [40].

Рисунок 1.8 Принцип Демінга-Шухарта або цикл Plan-Do-Check-□ct (PDC□)

1.2.2. Дослідження проблематики діджиталізації та принципів імплементації кіберзахисту з використанням безпекових стандартів в ЗОЗ.

Дослідженню проблематики діджиталізації у сфері охорони здоров'я присвячено чимало наукових праць таких авторів та дослідників: О. Глазачов, О. Лікарев, О. Шадрін – висвітлювали нагальність розвитку та впровадження електронних сервісів у медичній сфері; Д. Блум, Е. Гордон, К. Келлер, К. Сонг, М. Фрайдберг – окреслювали проблеми стандартизації та інтеграції, безпеки та кіберзпеки, ефективності та практичності медичних інформаційних систем.

Варто зауважити, що тема кібербезпеки в сфері ЗОЗ за межі проблематики діджиталізації розглядається значно рідше. Це важлива закономірність, яка буде розглянута в наступних розділах. Разом з тим, після повномасштабного вторгнення в Україну в 2022 році – дана тематика отримала «нове дихання» в причинах збільшення актуальності через постійні кібернетичні атаки на критичну інфраструктуру, ЗОЗ до якої відноситься [41; 42]. Окремо досліджували і питання забезпечення інформаційної безпеки в медичних освітніх закладах [43]. А також погляд на безпеку ЗОЗ в контексті забезпечення національної безпеки в Україні [44]. Також було досліджено питання забезпечення трудових прав, в тому числі для працівників ЗОЗ, в умовах воєнного стану [45]. Розглядалось питання інформаційної безпеки ЗОЗ і через узагальнюючу призму мережевих інформаційних ресурсів екосистеми eHealth [46 – 48].

Дослідження викликів діджиталізації в Україні [81], діджиталізації глобального характеру [82], діджиталізації медичних послуг [83] та проблеми кібербезпеки в сфері охорони здоров'я [84] було проведено протягом навчання.

Дослідження систем кібербезпеки активного характеру, на підставі яких проводяться аудити з кіберзахисту та подальшу імплементацію безпекових стандартів – досліджено в магістерській роботі «Технології та алгоритми обману для боротьби з кібератаками» спеціальності 125 – Кібербезпека [85].

1.3. Нормативно-правове забезпечення кібербезпеки в закладах охорони здоров’я та сфері електронної охорони здоров’я: міжнародний та національний стан

Щодо законодавчого регулювання, то воно грає важливу роль у впровадженні діджиталізації системи охорони здоров'я. Воно встановлює норми та правила, що регулюють збір, обробку та збереження медичної інформації, а також забезпечують права та обов'язки медичних закладів та пацієнтів у цифровому середовищі. Ось деякі ключові міжнародні закони, стандарти та організації [49]:

1) Закон Про права пацієнтів та електронні медичні записи (HITECH ct) – прийнятий у Сполучених Штатах 17 лютого 2009 року, цей закон встановлює стандарти електронних медичних записів та захисту конфіденційної інформації пацієнтів.

2) Міжнародні стандарти HL7 та FHIR: HL7 – це міжнародний стандарт для обміну медичною інформацією між системами охорони здоров'я. FHIR (Fast Healthcare Interoperability Resources) – це новий стандарт, розроблений HL7, призначений для полегшення обміну даними між різними системами електронної медичної документації.

3) Європейський загальний регламент про захист персональних даних (GDPR) – цей регуляторний акт встановлює стандарти для обробки та захисту персональних даних, включаючи медичну інформацію.

4) Директива про права пацієнтів Європейського Союзу – ця директива, яка прийнята у 2011 році, встановлює права пацієнтів на доступ до своїх медичних записів та вимагає встановлення електронних систем для обміну медичною інформацією між країнами ЄС.

5) Стандарти IHE (Integrating the Healthcare Enterprise) – ця організація розробляє стандарти та профілі для полегшення інтеграції медичних інформаційних систем.

6) Стандарти ISO та NSI – міжнародна організація стандартизації (ISO) та Американський національний інститут стандартів (NSI) також визначають норми та стандарти, які можуть бути застосовані у цифровій медичній сфері [попереднє]. У 2005 році була прийнята перша резолюція ВООЗ з впровадження електронної системи у охорону здоров'я, що започаткувало розробку та впровадження Глобальної стратегії. З того часу в рамках цієї ініціативи успішно проводять національну політику в галузі цифровізації охорони здоров'я та розвивають внутрішні стратегії понад 120 країн [50].

Кіберзахист - це відповідь на активну діджиталізацію сфери охорони здоров'я. Аби оцінити дану тенденцію варто переглянути нормативно-правові рухи в цьому напряму (див. таблиця 1.3).

Таблиця 1.3

Нормативно-правове регулювання діджиталізації в ЗОЗ України

Закони України	«Про інформацію» від 2 жовтня 1992 р. «Основи законодавства України про охорону здоров'я» від 19.11.1992 р. «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 р. «Про Національну програму інформатизації» від 04.02.1998 р. (із змінами) «Про телекомунікації» від 18.11.2003 р. «Про електронні документи та електронний документообіг» від 22.05.2003 р. «Про електронний цифровий підпис» від 22.05.2003 р. «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 рр.» від 09.01.2007р. «Про захист персональних даних» від 01.06.2010 р. Модельний закон «Про телемедицинські послуги» від 28.10. 2010 р. «Про підвищення доступності та якості медичного обслуговування у сільській місцевості» від 14 листопада

	2017р.

Продовження табл. 1.3

Постанови Кабінету Міністрів України	«Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах» №1772 від 16 листопада 2002 р. «Про заходи щодо створення електронної інформаційної системи «Електронний Уряд»» №208 від 24 лютого 2003 р. «Про затвердження Порядку використання комп'ютерних програм в органах виконавчої влади» №1433 від 10.09.2003 р. «Про затвердження Положення про Національний реєстр електронних інформаційних ресурсів» №326 від 17 березня 2004 р. «Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності» №1452 від 28 жовтня 2004 р. «Деякі питання електронної системи охорони здоров'я» №411 від 25 квітня 2018 р. − «Про внесення зміни до пункту 8 Порядку функціонування електронної системи охорони здоров'я» №526 від 19 червня 2019 р. «Про особливості ведення Електронного реєстру листків непрацездатності до забезпечення інформаційної взаємодії електронної системи охорони здоров'я з Електронним реєстром листків непрацездатності» №159 від 3 березня 2020 р. «Про внесення змін до деяких постанов Кабінету Міністрів України щодо питань електронної системи охорони здоров'я» №348 від 15 квітня 2020 р.; − «Про затвердження Державної стратегії регіонального розвитку на 2021-2027рр.» №695 від 5

	серпня 2020р. «Про утворення Міжгалузевої ради з питань цифрового розвитку, цифрових − трансформацій і цифровізації» №595 від 8 липня 2020 р.

Закінчення табл. 1.3

Накази МОЗ України	«Про створення Єдиного інформаційного поля системи охорони здоров'я України» №127 від 21 травня 1998 р. «Про упорядкування статистичної звітності в закладах та установах системи МОЗ України» №180 від 30 червня 1998 р. «Про перехід органів і закладів охорони здоров'я України на Міжнародну статистичну класифікацію хвороб і споріднених проблем охорони здоров'я Десятого перегляду» №297 від 8 жовтня 1998 р. «Про затвердження Переліку конфіденційної інформації, що є власністю держави, у системі МОЗ України» №143 від 9 червня 1999 р. 19 «Про затвердження Концепції галузевої програми «Електронна система реєстрації та обміну медичною інформацією між закладами, установами і організаціями охорони здоров'я»» №409 від 25 липня 2008 р. «Про затвердження галузевої програми «Електронна система реєстрації та обміну медичною інформацією між закладами, установами і організаціями системи охорони здоров'я»» №675 від 25 листопада 2008 р. «Про впровадження телемедицини в закладах охорони здоров'я» №261 від 26 березня 2010 р. «Про затвердження нормативних документів щодо застосування телемедицини у сфері охорони здоров'я» №681 від 19 жовтня 2015 р. «Деякі питання ведення Реєстру медичних записів, записів про направлення та рецептів в електронній системі охорони здоров'я» №587 від 28 лютого 2020 р.
Додатково	Наказ Міністерства цифрової трансформації України «Про затвердження Порядку обробки та захисту персональних даних,

	власником яких є Міністерство цифрової трансформації України» №72 від 20 травня 2020 р.

Розпорядження Кабінету Міністрів України від 10 липня 2019 року № 526-р «Про схвалення Стратегії розвитку сфери інноваційної діяльності на період до 2030 року», на сьогоднішній день також сприяє та формує основні цілі процесу впровадження діджиталізації [51].

Головними джерелами регулювання доступу до інформації в медичних закладах, в Україні, здійснюється завдяки Законам України:

1. «Про інформацію» [32];
2. « Про захист персональних даних» [27];
3. «Основи законодавства України про охорону здоров'я» [35];

4. Цивільному кодексу України [33] та ряду інших спеціальних нормативних актів, що регулюють питання доступу до інформації фізичних осіб, організацій, органів та служб [14 - 16; 28; 33; 34].

Закон України «Про інформацію» ст. 1, 11 [32] регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації. Інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Відповідно до ст. 11 даного закону:

1. Інформація про фізичну особу (персональні дані) - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

2. Не допускається збирання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом.

До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження. Кожному забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законом

Закон України «Про захист персональних даних» ст. 2 [27] поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці. Відповідно до ст. 2 закону «Про захист персональних даних»:

Персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована;

Знеособлення персональних даних - вилучення відомостей, які дають змогу прямо чи опосередковано ідентифікувати особу;

Відповідно до ст. 7 Закону «Особливі вимоги до обробки персональних даних» [52]:

1. Забороняється обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров’я, статевого життя, біометричних або генетичних даних.

2. Положення ч. 1 цієї статті не застосовується, якщо обробка здійснюється за умови:

2.1. надання суб'єктом персональних даних однозначної згоди на обробку таких даних;

2.2. необхідна для здійснення прав та виконання обов'язків володільця у сфері трудових правовідносин відповідно до закону із забезпеченням відповідного захисту;

2.3. необхідна для захисту життєво-важливих інтересів суб'єкта персональних даних або іншої особи у разі недієздатності або обмеження цивільної дієздатності суб'єкта персональних даних;

3. необхідна для обґрунтування, задоволення або захисту правової вимоги;

4. необхідна в цілях охорони здоров’я, встановлення медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг за

умови, що такі дані обробляються медичним працівником або іншою особою закладу охорони здоров’я, на якого покладено обов’язки щодо забезпечення захисту персональних даних та на якого поширюється законодавство про лікарську таємницю;

5. стосується вироків суду, виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом та здійснюється державним органом в межах його повноважень, визначених законом;

6. стосується даних, які були явно оприлюднені суб'єктом персональних даних.

Поняття лікарської таємниці - найважливіше поняття медичної етики. Лікарська таємниця юридично охороняється, а її розголошення тягне за собою юридичну відповідальність (цивільно-правову, дисциплінарну або кримінальну).

Лікарська таємниця визнана на законодавчому рівні поряд із адвокатською та нотаріальною.

В основному спеціальному законі - законі України «Основи законодавства України про охорону здоров'я» в межах ст. 40 зазначено: медичні працівники та інші особи, яким у зв'язку з виконанням професійних або службових обов'язків стало відомо про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторони життя громадянина, не мають права розголошувати ці відомості, крім передбачених законодавчими актами випадків [35].

Поняття лікарської таємниці в цивільному законодавстві: щодо «Права на таємницю про стан здоров'я» говориться ст. 286:

1. Фізична особа має право на таємницю про стан свого здоров'я, факт звернення за медичною допомогою, діагноз, а також про відомості, одержані при її медичному обстеженні.

2. Забороняється вимагати та подавати за місцем роботи або навчання інформацію про діагноз та методи лікування фізичної особи.

3. Фізична особа зобов'язана утримуватися від поширення інформації, зазначеної у ч. 1 цієї статті, яка стала їй відома у зв'язку з виконанням службових обов'язків або з інших джерел [33].

Право на інформацію в цивільному законодавстві. «Право на інформацію про стан свого здоров'я» ст. 285 зазначається:

1. Повнолітня фізична особа має право на достовірну і повну інформацію про стан свого здоров'я, у тому числі на ознайомлення з відповідними медичними документами, що стосуються її здоров'я.

2. Батьки (усиновлювачі), опікун, піклувальник мають право на інформацію про стан здоров'я дитини або підопічного.

3. Якщо інформація про хворобу фізичної особи може погіршити стан її здоров'я або погіршити стан здоров'я фізичних осіб, визначених ч. 2 цієї статті, зашкодити процесові лікування, медичні працівники мають право дати неповну інформацію про стан здоров'я фізичної особи, обмежити можливість їх ознайомлення з окремими медичними документами.

4. У разі смерті фізичної особи члени її сім'ї або інші фізичні особи, уповноважені ними, мають право бути присутніми при дослідженні причин її смерті та ознайомитись із висновками щодо причин смерті, а також право на оскарження цих висновків до суду [33].

Поняття лікарської таємниці в кримінальному законодавстві. В ст. 145 Кримінального кодексу України «Незаконне розголошення лікарської таємниці» визначено, що:

- умисне розголошення лікарської таємниці особою, якій вона стала відома у зв'язку з виконанням професійних чи службових обов'язків, якщо таке діяння спричинило тяжкі наслідки,

- карається штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або громадськими роботами на строк до двохсот сорока годин, або позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років, або виправними роботами на строк до двох років [54].

Тяжкими наслідками розголошення вказаних відомостей можуть бути визнані самогубство чи самокалічення потерпілого, серйозне загострення його хвороби внаслідок переживань тощо [53]. Настання таких наслідків розголошення лікарської таємниці, як самогубство потерпілого, заподіяння йому тяжких чи середньої тяжкості тілесних ушкоджень не охоплюється ст. 145 [54] і за наявності підстав потребує додаткової кваліфікації ст. 120, 128 [54].

Суб'єктом злочину при цьому є медичні працівники та інші особи, у т. ч. і службові, яким відповідна інформація стала відома у зв'язку з виконанням професійних чи службових обов'язків. Для кваліфікації злочину не має значення, була така інформація довірена особі (надана за обліковим документом) чи стала відома за інших обставин (навіть і випадково, але у зв'язку з виконанням професійних чи службових обов'язків - обов'язків лікаря, адвоката, нотаріуса, вихователя, спеціаліста-психолога тощо).

В Законі України «Основи законодавства України про охорону здоров’я», Цивільному кодексі України, як і в Кримінальному кодексі України, не визначено, що інформація повинна бути задокументованою. Тобто будь-яка інформація (письмова чи усна), що стосується факту звернення за медичною допомогою, медичного огляду чи його результатів, інтимного чи сімейного життя пацієнта, становить лікарську таємницю.

Категорії інформації, які складають лікарську таємницю: відповідно до Цивільного кодексу України ст. 285, 286 [33] та Закону України «Основи законодавства України про охорону здоров’я» ст. 39, 40 у медичних закладах можна виділити наступні категорії інформації, що мають статус інформації з обмеженим доступом (конфіденційної):

1. факт та привід звернення за медичною допомогою;
2. стан здоров'я та захворювання пацієнта;
3. факт медичного огляду та його результати;
4. інтимне та сімейне життя пацієнта;
5. інші відомості, які отримані під час обстеження та лікування [35].

У ст. 65 Кримінального процесуального кодексу України зазначено, що не можуть бути допитані як свідки медичні працівники з приводу того, що їм довірено або стало відомо при здійсненні професійної діяльності, якщо вони не звільнені від обов'язку зберігати професійну таємницю особою, що довірила їм ці відомості. Звільнення здійснюється:

1. У письмовій формі;

2. У визначеному обсязі;

3. За підписом особи, що довірила зазначені відомості.

У ст. 51 Цивільного процесуального кодексу України також зазначено: не підлягають допиту як свідки особи, які за законом зобов'язані зберігати в таємниці відомості, що були довірені їм у зв'язку з їхнім службовим чи професійним становищем.

Далі розглянемо спеціальні закони, що регулюють діяльність фізичних та юридичних осіб, органів та служб щодо правомірності надання їм інформації з обмеженим доступом (конфіденційної). В Законі України «Про оперативно-розшукову діяльність» ст. 5 визначено, що оперативно-розшукова діяльність здійснюється оперативними підрозділами:

1. МВС України - кримінальною, транспортною, спеціальною та судовою міліцією;

2. Служби безпеки України - спеціальними підрозділами по боротьбі з корупцією, оперативно-технічними тощо;

3. Податкової міліції;

4. Органів і установ виконання покарань Державної пенітенціарної служби України тощо [55].

Відповідно до ст. 11 підприємства, установи, організації незалежно від форми власності зобов'язані сприяти оперативним підрозділам у вирішенні завдань оперативно-розшукової діяльності. Забороняється залучати до виконання таких завдань осіб, професійна діяльність яких пов'язана зі збереженням професійної таємниці, а саме: адвокатів, нотаріусів, медичних

працівників тощо, якщо таке співробітництво буде пов’язано з розкриттям інформації професійного характеру [55].

Чинний Закон України «Про прокуратуру» [56], доповнений Законом України «Про прокуратуру» [57] визначає особливості доступу до інформації працівників прокуратури. Відповідно до ст. 20 прокурор має право:

- мати доступ до документів і матеріалів, необхідних для проведення перевірки, у т. ч. за письмовою вимогою, і таких, що містять інформацію з обмеженим доступом;

- письмово вимагати подання в прокуратуру у визначений ним розумний строк зазначених документів та матеріалів, видачі необхідних довідок.

- отримувати від посадових та службових осіб і громадян усні або письмові пояснення, в тому числі шляхом виклику відповідної особи до органу прокуратури [57].

Зазначені дії можуть бути вчинені виключно під час проведення перевірки в порядку, передбаченому ст. 21 [57]. Відповідно до ст. 21 [56] «Перевірки та порядок їх проведення»: Для здійснення перевірки прокурор приймає постанову, в якій зазначає підстави, що свідчать про можливі порушення законності, та обґрунтовує необхідність вчинення дій, передбачених ст. 20 даного Закону. Не допускається проведення перевірки без надання копії зазначеної постанови представнику організації незалежно від форми власності, підпорядкованості чи приналежності, фізичній особі – підприємцю. Оригінали витребуваних прокурором документів мають бути повернуті відповідним особам після закінчення перевірки, крім випадків долучення їх до матеріалів кримінального провадження в порядку, передбаченому процесуальним законодавством. У разі необхідності до закінчення перевірки можуть бути повернуті копії зазначених документів.

Закон України «Про адвокатуру та адвокатську діяльність» [58] говорить, що адвокат має право:

1. Звертатися з адвокатськими запитами, у т. ч. щодо отримання копій документів, до підприємств, установ, організацій, тощо (ст. 20 п. 2);

2. Ознайомлюватися на підприємствах, в установах і організаціях з необхідними для адвокатської діяльності документами та матеріалами, крім тих, що містять інформацію з обмеженим доступом (ст. 20 п. 4);

3. Керівники підприємств, установ, організацій, яким направлено адвокатський запит, зобов’язані не пізніше 5 робочих днів з дня отримання запиту надати адвокату відповідну інформацію, копії документів, крім інформації з обмеженим доступом (ст. 24 п. 2.).

В Законі України «Про страхування» [59] говориться, що у разі необхідності страховик може робити запити про відомості, пов'язані із страховим випадком, до правоохоронних органів, банків, медичних закладів та інших організацій, що володіють інформацією про обставини страхового випадку, а також можуть самостійно з'ясовувати причини та обставини страхового випадку. Підприємства, установи та організації зобов'язані надсилати відповіді страховикам на запити про відомості, пов'язані із страховим випадком, у т. ч. й дані, що є комерційною таємницею. При цьому страховик несе відповідальність за їх розголошення в будь-якій формі, за винятком випадків, передбачених законодавством України [59].

Відповідно до ст. 40 інформація щодо фізичних осіб надається у таких випадках:

1. На письмовий запит та з письмового дозволу власника такої інформації;

2. На письмові вимоги суду або за рішенням суду;

3. Органам прокуратури України, Служби безпеки України, МВС України на їх письмову вимогу у разі повідомлення про підозру у вчиненні кримінального правопорушення даній особі [59].

Закон України «Основи законодавства про охорону здоров’я» не містять переліку випадків, коли і кому надається інформація щодо фізичних осіб, як це визначено ст. 40. За принципом аналогії закону, можемо зробити припущення, що в аналогічних випадках інформація з обмеженим доступом (конфіденційна

інформація; інформація, що становить лікарську таємницю) може надаватися і медичними закладами [59].

На підставі вищерозглянутих нормативних актів можемо зробити наступні узагальнення:

1. Медичні працівники та інші особи, яким у зв'язку з виконанням професійних або службових обов'язків стало відомо про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторони життя громадянина, не мають права розголошувати ці відомості, крім передбачених законодавчими актами випадків.

2. Не лише задокументована інформація, але й усна становить лікарську таємницю.

3. Поняття лікарської таємниці стосується не лише лікарів і не лише медичного персоналу, а й адміністративного, технічного персоналу та решти осіб, які у зв'язку з виконанням професійних або службових обов'язків мають доступ до зазначених відомостей.

4. До категорій інформації, які складають лікарську таємницю відносяться:

А) факт та привід звернення за медичною допомогою;

Б) стан здоров'я та захворювання пацієнта;

В) факт медичного огляду та його результати;

Г) інтимне та сімейне життя пацієнта;

Д) інші відомості, які отримані під час обстеження та лікування.

5. Надання інформації про пацієнта регулюються як загальними так і спеціальними законами, зокрема законом України «Основи законодавства про охорону здоров'я», Цивільним кодексом України, Кримінальним кодексом України, Законами України: «Про оперативно-розшукову діяльність», «Про прокуратуру», «Про адвокатуру та адвокатську діяльність», «Про страхування» тощо.

6. За принципом аналогії закону інформація про фізичну особу може бути надана у випадках:

1) на письмовий запит та з письмового дозволу власника такої інформації;

2) на письмові вимоги суду або за рішенням суду;

3) органам прокуратури України, Служби безпеки України, МВС України на їх письмову вимогу у разі повідомлення про підозру у вчиненні кримінального правопорушення даній особі та в інших передбачених законодавством випадках

Окремо варто зауважити, що 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 та прав пацієнтів зазначені в постанові [60] «Деякі питання електронної системи охорони здоров'я» та нормативно-правові акти, якими регулюється порядок ведення окремих реєстрів.

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

Висновки до розділу 1

Проаналізувавши праці науковців та узагальнивши теоретичні засади стосовно «діджиталізації» та «кібербезпеки» в охороні здоров'я можна зробити висновок, що на перший погляд взаємопов'язані процеси відображають дещо різні аспекти. Спільним цих двох ключових понять є їх мета – покращення форм надання медичної допомоги населенню. Визначено, що на сьогодні діджиталізація є одним з найважливіших завдань державної політики в системі охорони здоров'я багатьох країн, включаючи Україну. Фундамент для її ефективної реалізації вбачають в інформаційній та технологічній основі, складовими яких є розвиток: електронних медичних записів; телемедицини; мобільних додатків для моніторингу стану здоров'я; аналітичних систем для прийняття рішень тощо.

Визначивши основні методологічні принципи дослідження, а саме інтероперабельність, конфіденційність та безпека даних, залучення і навчання актуальним методикам кібербезпеки для медичних працівників та пацієнтів, можна побачити основні стратегії у використанні сучасних технологій в медичній сфері. Забезпечити їх доцільність допоможе законодавче та нормативно-правове підґрунтя, серед яких виділяють міжнародні закони, акти, стандарти та директиви. Одними з основних документів, якими регламентується державна політика в охороні здоров'я України з приводу діджиталізації є розпорядження Кабінету Міністрів Україні [61] «Про схвалення Стратегії розвитку інноваційної діяльності на період до 2030 року» та «Концепцією розвитку електронної охорони здоров'я» [62], які розглядають електронну охорону здоров'я, як систему гармонійних та взаємоприйнятних інформаційних відносин між всіма учасниками медичного середовища країни. Окрім того, законодавство не містить вичерпного переліку 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 їх розголошення та надавати доступ до ПД пацієнтів третім особам лише у випадках, що передбачені законодавством.

Складність та комплексність даної проблемної сфери, з тезисів, що згадані вище – очолює перелік причин щодо актуальності імплементації версії ISO 27799, що має орієнтацію саме на ЗОЗ. В наступному розділі буде проведено більш глибокий аналіз імплементації безпекових стандартів сімейства ISO 2700x, зокрема версії ISO 27799 з аргументацією обраного варіанту та супровідних процедур процесу «Кібербезпека».

РОЗДІЛ 2
АНАЛІЗ ОСОБЛИВОСТЕЙ РЕАЛІЗАЦІЇ БЕЗПЕКОВИХ СТАНДАРТІВ В ЗАКЛАДАХ ОХОРОНИ ЗДОРОВ'Я

2.1. Публічне адміністрування в сфері охорони здоров'я

В цілях актуалізації аналізу стану кібербезпеки, приймаючи до уваги тезис з попереднього розділу, що «кібербезпека в ЗОЗ оцінюється саме в межах діджиталізації, в своїй сутності» варто звернути увагу на діджиталізацію ЗОЗ через призму публічного адміністрування в сфері охорони здоров'я.

Отже, у різних країнах світу вже давно йде процес цифрової трансформації систем охорони здоров'я, які працюють за різними моделями: це можуть бути централізовані, тобто коли влада та прийняття рішень зосереджені в центральному органі чи центральному керівництві, децентралізовані – влада та відповідальність розподілені між різними рівнями або локальними підрозділами. Кожна з них має свої плюси і мінуси, які виявляються та виправляються в процесі експлуатації, з урахуванням особливостей фінансування і технічних можливостей. Україна обрала дворівневу модель електронної системи охорони здоров'я, що передбачає центральний (державний) та периферійний (регіональний) рівні (див. таблиця 2.1) [63, с. 167-168].

Центральний рівень включає центральну базу даних, а периферійний – медичні інформаційні системи. В свою чергу, центральна база даних – збирає і зберігає дані, які надходять до загального центрального сховища та є доступними для Міністерства охорони здоров'я, Національної служби здоров'я та інших медичних постачальників, що зареєстровані в електронній системі охорони здоров'я. Медична інформаційна система – це периферійна частина електронної системи охорони здоров'я, яка забезпечує зберігання та обробку даних в медичних установах. Вона є інструментом для вирішення локальних

завдань для пацієнтів, керівників та медичних працівників в установах охорони здоров'я. Наразі Україна знаходиться в процесі розбудовування електронного здоров'я, маючи на меті збалансований і синхронний розвиток цих двох рівнів (див. рис. 2.1) [64, с. 43].

Таблиця 2.1

Суб'єкти дворівневої моделі електронної системи охорони здоров'я України

Центральний рівень (державний)	**Периферійний рівень (регіональний)**
Міністерство охорони здоров'я України (МОЗ) – центральний орган виконавчої влади, відповідальний за формування та реалізацію державної політики у сфері охорони здоров'я	Обласні державні адміністрації та їх структури – відповідають за організацію та координацію медичної допомоги на регіональному рівні
Державна служба України з лікарських засобів та контролю за наркотиками (Держлікслужба) – орган, відповідальний за регулювання та контроль якості і безпеки лікарських засобів	Обласні управління охорони здоров'я – органи, які допомагають обласним адміністраціям у плануванні і виконанні програм у галузі охорони здоров'я
Державний центр забезпечення електронних публічних послуг (ДЦЗЕП) – орган, що відповідає за розвиток та управління електронною системою охорони здоров'я на державному рівні	Лікарні, клініки та інші медичні установи – на регіональному рівні надається медична допомога населенню
Інші органи і служби, пов'язані з охороною здоров'я: державні медичні та наукові установи	

На центральному (державному) рівні, який представляє собою державний компонент, відбувається накопичення та зберігання медичної інформації у центральній базі даних. Ця інформація необхідна для ефективного управління системою охорони здоров'я в цілому: моніторинг і аналіз ключових показників роботи галузі та якості надання медичної допомоги, контролю за розподілом і використанням бюджетних коштів, що призначені для утримання медичних та інших галузевих установ [65, с. 20].

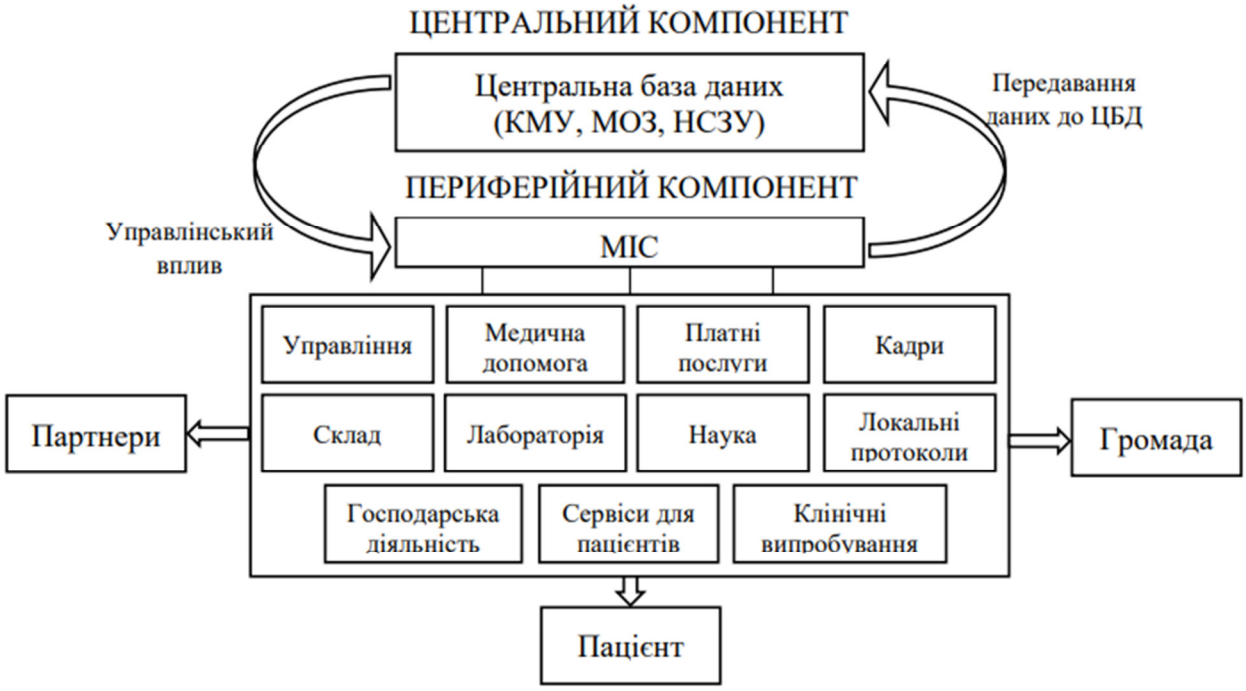


Рис. 2.1. Дворівнева модель електронної системи охорони здоров'я

Зазвичай, інформація потрапляє до центрального компонента безпосередньо з медичних установ через медичні інформаційні системи. Слід наголосити, що державний рівень, який фінансує Національна служба здоров'я України та керує галуззю Міністерство охорони здоров'я України, має право контролювати цільове і раціональне використання ресурсів та показників системи. Нажаль у сучасних умовах усі системи охорони здоров'я стикаються з обмеженими фінансовими та матеріальними ресурсами, тому і немає якогось сталого ідеалу. Так, ключовим завданням центрального (державного) рівня є максимально ефективне використання дефіцитних ресурсів у галузі.

Електронна система охорони здоров’я на цьому рівні є невід’ємним інструментом, який дозволяє керувати ресурсами на рівні системи та отримувати необхідні цільові показники здоров’я населення за виділеним бюджетом [64, с. 45]. Периферійний (регіональний) компонент електронного здоров’я діє на місцевому рівні та забезпечується медичними інформаційними системами. Головні завдання яких полягають у передачі даних до центральної бази, а також накопичення та обробки інформації для потреб місцевого рівня. На даний момент медичні установи майже повністю зосереджені на зборі та передачі у центральну базу даних електронної охорони здоров’я інформації, запитаної державою, оскільки це безпосередньо впливає на їх фінансування.

Однак дані, які необхідні медичним установам для ефективного управління своєю діяльністю, часто залишаються без належної уваги [64, с. 47].

Місцевий рівень включає в себе безліч процесів, які повинні бути автоматизовані, і різноманітні дані, які потрібно обробляти. Це стосується роботи лабораторій, наукових відділень, послуг для пацієнтів, а також адміністративних процесів – управління персоналом, ліжкофондом, складом, документообігом тощо.

Дана інформація дуже важлива не лише для керівників, які вже зацікавлені у покращені ефективності своїх медичних установ, а й для місцевих органів самоврядування, через які громадськість контролює діяльність цих установ. Однією з головних складнощів є те, що для ефективного використання фінансових ресурсів, які надходять з державного бюджету, необхідна всеосяжна інформатизація місцевого рівня, переважно на основі медичних інформаційних систем, але не тільки [64, с. 48].

Нажаль цифрова трансформація регіонального рівня обмежена майже тільки збором інформації для задоволення потреб центрального рівня. Тому, формально модель системи охорони здоров’я України ієрархічно є дворівневою, але з точки зору принципу управління та залежності одне від одного, можна стверджувати, що вона «асиметрично дворівнева», або навіть «центроцентрична».

2.2. Особливості безпекового стандарту ISO 27799 та його відмінності від ISO 27002

Отримавши вичерпні відомості щодо теоретичного підґрунтя кібербезпеки в ЗОЗ, варто провести глибший аналіз в постановці проблеми: забезпечення безпеки в інформаційному просторі закладів охорони здоров’я в умовах відсутності централізованих регламентуючих документів із чіткою структурою та послідовністю дій щодо імплементаційних заходів. Чому ж фокус уваги саме на стандарті ISO 27799 та чи відповідає від потребам галузі?

Це досягається шляхом вирішення наступного списку другорядних цілей, які підтримують основну мету:

– Дослідження сектору охорони здоров'я та даних сектору

– Вивчення практики управління інформаційною безпекою в цілому, а також у сфері охорони здоров'я.

– Аналітичне порівняння стандартів ISO 27002 та ISO 27799.

– Структуризація результатів порівняльного аналізу статей про контроль безпеки в обох стандартах.

– Визначення підходу ISO 27799 щодо створення СУІБ.

– На основі вищезазначених дій – дано оцінку використання ISO 27799 в сфері охорони здоров’я, а саме – імплементація в закладах охорони здоров’я.

2.2.1. Огляд передумов імплементації ISO 27799: теоретичні відомості.

Міжнародні стандарти системи управління являють модель для налагодження та функціонування системи управління. Ця модель включає в себе функції, за якими експерти досягли згоди на підставі міжнародного досвіду, накопиченого в цій області. При використанні сімейства стандартів систем управління інформаційною безпекою (СУІБ), організації можуть реалізовувати, вдосконалювати, і підготувати СУІБ до незалежної оцінки, що

застосовується для захисту інформації, такої як фінансова інформація, інтелектуальна власність, інформація про персонал, а також інформація, довірена клієнтами або третьою стороною (загальний погляд).

Сімейство стандартів СУІБ призначене для допомоги організаціям будь-якого типу і величини в реалізації та функціонуванні СУІБ. Сімейство стандартів СУІБ складається з наступних міжнародних стандартів під загальною назвою «Information technology - Security techniques» - IT - Методи і засоби забезпечення безпеки [2 - 4; 10] (див. таблиця 3.2):

Таблиця 3.2

Сімейство стандартів «Information technology - Security techniques»

Шифр стандарту	**Опис стандарту**
ISO / IEC 27000	СУІБ. Загальний огляд і термінологія
ISO / IEC 27001	СУІБ. Вимоги
ISO / IEC 27002	Звід правил з управління ІБ
ISO / IEC 27003	Керівництво по реалізації СУІБ
ISO / IEC 27004	УІБ. Вимірювання
ISO / IEC 27005	Управління ризиками ІБ
ISO / IEC 27006	Вимоги для органів, що забезпечують аудит і сертифікацію СУІБ
ISO / IE 27007	Керівництво для проведення аудиту СУІБ
ISO / IE TR 27008	Керівництво для аудиту механізмів контролю ІБ
ISO / IE 27010	УІБ для міжсекторальних і міжорганізаційних комунікацій
ISO / IEC 27011	Керівництво по УІБ організацій, що пропонують телекомунікаційні послуги, на основі ISO / IEC 27002

Продовження табл. 3.2

ISO / IE 27013	Керівництво з інтегрованої реалізації стандартів ISO / IEC 27001 та ISO / IEC 20000-1
ISO / IE 27014	Управління ІБ вищим керівництвом
ISO / IE TR 27015	Керівництво з УІБ для фінансових сервісів
ISO / IE TR 27016	УІБ. Організаційна економіка
ISO / IE 27035	Управління інцидентами ІБ
ISO 27799	Інформатика в охороні здоров'я. УІБ за стандартом ISO / IEC 27002 (Міжнародний стандарт, що не має загальної назви)

Актуальним нині є ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT), відповідно [10].

Одним з ключових факторів успішності системи управління інформаційною безпекою підприємства – це побудова її на базі міжнародних стандартів ISO/IEC27001. Стандарт ISO/IEC 27001 дає інструмент для розробки, впровадження, супроводу, моніторингу, підтримки та вдосконалення добре документованої СУІБ в контексті розгляду бізнес ризиків. СУІБ забезпечує вибір пропорційних та адекватних засобів і методів контролю та захисту інформації, і тим самим, довіру зацікавлених сторін.

Побудова системи управління інформаційною безпекою — це комплексний процес, направлений на мінімізацію зовнішніх і внутрішніх загроз із врахуванням обмежень на ресурси і час. Для побудови ефективної системи інформаційної безпеки необхідно спочатку описати процеси діяльності, потім визначити поріг ризику, тобто рівень загрози, при якому вона потрапляє в процес управління ризиками. Отже, потрібно побудувати таку систему інформаційної безпеки, яка забезпечить досягнення заданого рівня ризику.

Зважаючи на сукупність бізнес-процесів, специфіку інформаційного продукту, переважно мультимедійного видання, з методологічного погляду, створення СУІБ може бути реалізовано в такі шість етапів (див. рис. 2.1).

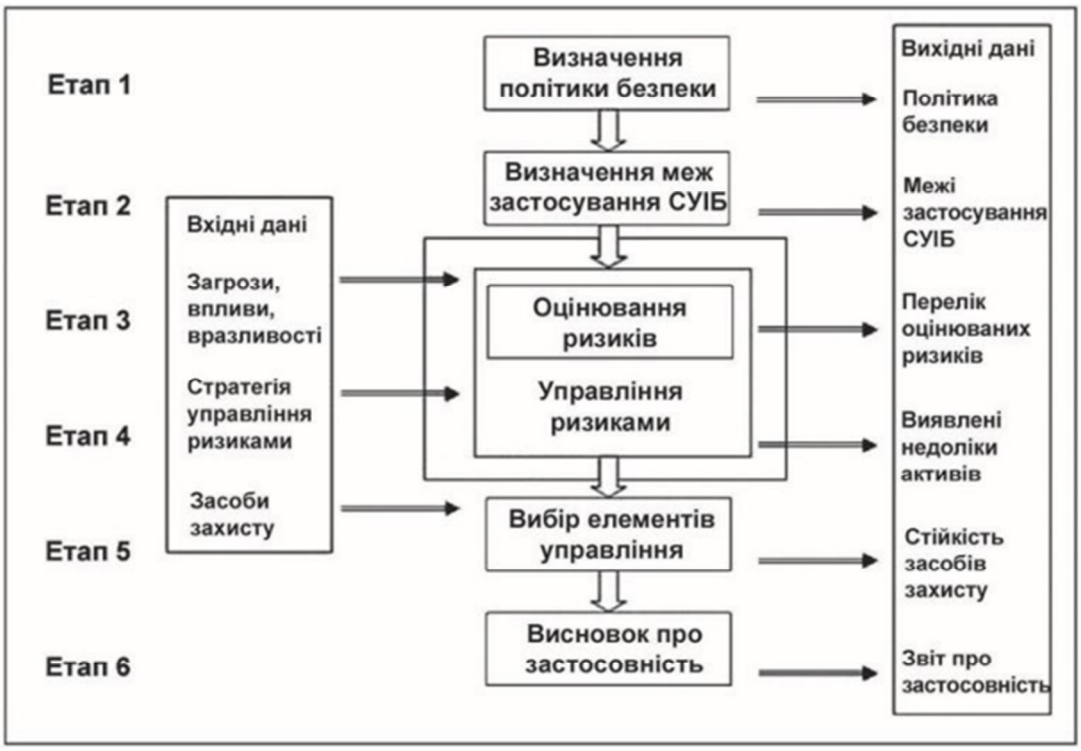


Рис. 2.1 Етапи процесу створення СУІБ

Аналіз моделі управління ризиками потребує розгляду в рамках узагальненої моделі системи інформаційної безпеки, із розкриттям таких понять як об’єкт захисту, види і модель загроз, модель порушника і т.д.

Ось тут і відображаються головні переваги ISO 27799 – в практичній орієнтації на ЗОЗ. Адже навіть при використанні ISO 27799, організації можуть реалізовувати і поліпшувати СУІБ та підготуватися до незалежної оцінки їх СУІБ в органах оцінки відповідності, які є акредитованими та визнаними в міжнародній системі акредитації International □ccreditation Forum (I□F). Далі під СУІБ будемо розуміти саме таку систему, що створена у відповідності до вимог стандартів серії ISO 27000.

2.2.2. Огляд передумов імплементації ISO 27799: аналіз досліджень.

Інформаційні системи в секторі охорони здоров'я, спочатку були створені для використання на вторинному рівні для адміністративних та організаційних процесів. Вони не були створені для використання на первинному рівні – для підвищення ефективності догляду за пацієнтами [66]. Автор [67] зазначає, що технологію слід розглядати комплексно, в цілях підвищення якості і ефективності медичних послуг, а також, що важливо, замінити всі життєздатні та повторювані процеси менш дорогою або економічно-ефективною технологією автоматизації: багато адміністративних і медичних обов'язків у сфері охорони здоров'я повторюються, і їх можна покращити за допомогою відповідної автоматизованої технології для покращення якості та надання послуг. Діджиталізація охорони здоров'я допомагає лікарям у прийнятті рішень і діях, а також покращує результати лікування пацієнтів шляхом кращого використання інформації та підвищення ефективності способу збору, обробки, передачі та застосування даних пацієнтів і медичних знань [67].

Різні автори погоджуються, що існує потреба в технологічному прогресі в секторі охорони здоров'я, але виникає питання, як цей технологічний прогрес покращить якість обслуговування в різних підрозділах сектору охорони здоров'я? Інші дослідження стверджують [68], що технологічні досягнення будуть реалізовані за допомогою інструментів інформаційних технологій, які мають відношення до сектору охорони здоров'я – формування складних ERP – подібних інформаційних систем. Важливість EPR підкреслюється тим фактом, що все більше країн встановлюють національні плани – формування цілісних та комплексних EPR, щоб сприяти раціоналізації потоку інформації, що підтримує повний процес надання медичної допомоги в організації охорони здоров'я, і сприяти спільному догляду за межами кордонів галузевого та національного характеру. Подібне, комплексне рішення і є спільною ознакою щодо потреби застосування безпекового стандарту сімейства ISO 27000, але лишилось визначити чи саме версія ISO 27799 буде найбільш раціональною.

Варто оцінити процес імплементації безпекового стандарту і з точки зору «більш практичної» реалізації, а саме: поведінкові сценарії переходу на електронну документацію (знову ж таки, нерозривність із діджиталізацією).

Дані, що зберігалися в паперових сховищах, були фрагментованими, неструктурованими, серйозно схильні до несумісної термінології та семантики загалом. Ці умови – розділяли клінічні та адміністративні дані, чим спричиняли розрив даних пацієнтів у часі та просторі [69]. Розташування цих архаїчних нині сховищ перешкоджало оптимальному використанню величезної кількості даних, які вони містили. Технологічний прогрес покращив структуру зберігання записів пацієнтів шляхом збору автоматизованих даних пацієнтів, які є більш точними, вичерпними, стандартизованими, своєчасними та доступними [70]. Згідно з Австралійською мережею лікарів загальної практики, дані повинні мати такі характеристики, щоб бути корисними [71]:

Точність (дійсність та надійність, як риси інформації з точки зору кіберзахисту) – підтвердження від пацієнта та медичного працівника;

Вичерпність (повнота та достовірність);

Стандартизованість (типізація та уніфікація), що дає змогу працювати з даними в режимі реального часу;

Своєчасність (актуальність та неспростовність) – доступність у потрібний час і готовий до використання, доступність незалежно від власності та з належним урахуванням конфіденційності пацієнта.

Характер середовища ЗОЗ – є одним із компонентів, котрий впливає на унікальні потреби безпеки та конфіденційності в секторі охорони здоров’я: згідно з [72], існує дві цілі щодо інформаційної безпеки в охороні здоров’я, а саме:

- Високий рівень безпеки: можливість пацієнтам отримати найкращу якість медичних послуг за допомогою актуальної та доступної інформації;

- Високий рівень конфіденційності пацієнта: захистити пацієнтів від розповсюдження конфіденційної інформації (ПД) неавторизованим особам.

Окремі дослідження [73] аргументували, що сектор охорони здоров’я має деякі унікальні характеристики з точки зору інформаційної безпеки (перешкоди до імплементації), які включають:

- Чутливість електронних медичних записів;
- Велику кількість малих організацій та сегментованих процесів;
- Стан законодавства про конфіденційність медичних даних;

Окремим компонентом, який впливає на унікальні потреби в безпеці та конфіденційності в секторі охорони здоров’я, є постійно змінювані вимоги дотримання законодавства, встановлені законами та рекомендаціями. На міжнародному рівні законодавці визнали проблеми щодо захисту даних і передачі даних про здоров’я та вжили заходів, видавши різні акти про захист даних, наприклад, Американський закон про перенесення та підзвітність медичного страхування (HIP□□), який часто хочуть застосувати і в Україні [74].

Повернемось до призначення ISO 27799. У відповідності до [4]:

ISO 27799:2016 містить керівні принципи для стандартів організаційної інформаційної безпеки та практик управління інформаційною безпекою, включаючи вибір, впровадження та управління засобами контролю з урахуванням середовища (середовищ) ризиків інформаційної безпеки організації. Стандарт визначає керівні принципи для підтримки тлумачення та впровадження в медичну інформатику ISO/IEC 27002 і є доповненням до цього Міжнародного стандарту.

ISO 27799:2016 містить вказівки щодо впровадження засобів контролю, описаних у ISO/IEC 27002, і доповнює їх за необхідності, щоб їх можна було ефективно використовувати для керування інформаційною безпекою охорони здоров'я. Впроваджуючи ISO 27799:2016, організації охорони здоров'я та інші зберігачі медичної інформації зможуть забезпечити мінімальний необхідний рівень безпеки, який відповідає обставинам їхньої організації, і який зберігатиме конфіденційність, цілісність і доступність особистої медичної інформації, яка перебуває під їхнім наглядом.

Вона застосовується до інформації про здоров'я в усіх її аспектах, незалежно від того, яку форму має інформація (слова та цифри, звукозаписи, малюнки, відео та медичні зображення), які б засоби не використовувалися для її зберігання (друк або запис на папері чи зберігання в електронному вигляді), а також будь-які засоби використовуються для її передачі (вручну, факсом, через комп'ютерні мережі або поштою), Оскільки інформація завжди повинна бути належним чином захищена.

ISO 27799:2016 та ISO/IEC 27002 разом визначають, що потрібно з точки зору інформаційної безпеки в охороні здоров'я, але вони не визначають, як ці вимоги мають бути виконані. Іншими словами, наскільки це можливо, ISO 27799:2016 є технологічно нейтральним [75; 76]. Важливою рисою є нейтралітет щодо впровадження технологій. Технології безпеки все ще перебувають на стадії швидкого розвитку, і темпи цих змін тепер вимірюються місяцями, а не роками. На противагу цьому, хоча міжнародні стандарти підлягають періодичному перегляду, очікується, що вони в цілому залишатимуться чинними протягом багатьох років. Не менш важливим є те, що технологічна нейтральність дозволяє постачальникам медичних послуг вільно пропонувати нові, розробляючи технології, що відповідають необхідним вимогам, описаним ISO 27799:2016 [75; 76].

Як зазначалося у вступі, знайомство з ISO/IEC 27002 є необхідним для розуміння ISO 27799:2016, так як є його підґрунтям.

Поза сферою дії ISO 27799:2016 знаходяться такі напрямки інформаційної безпеки:

а) методології та статистичні тести для ефективного знеособлення особистої інформації про здоров'я;

б) методології псевдонімізації особистої інформації про здоров'я (див. Бібліографію для короткого опису Технічної специфікації, яка стосується саме цієї теми);

в) якість обслуговування мережі та методи вимірювання доступності мереж, що використовуються для медичної інформатики;

г) якість даних (на відміну від цілісності даних).

Варто зауважити, що версія ISO 27799:2016 є нині актуальною. Наступна версія ще в проекті [75].

2.2.3. Огляд передумов імплементації ISO 27799: відповідність запланованим заходам щодо реалізації Концепції розвитку електронної охорони здоров'я.

Проведемо аналіз регламентуючої документації, на підставі якої ЗОЗ розглядають імплементацію безпекових стандартів. До уваги візьмемо два документи: Розпорядження Кабінету Міністрів України, від 28.12.2020р. №1671-р. «Про схвалення концепції розвитку електронної охорони здоров'я» [14] та Розпорядження Кабінету Міністрів України, від 29.09.2021р. №1175-р. «Про затвердження плану заходів щодо реалізації Концепції розвитку електронної охорони здоров'я» [15]. Тавтологічність розгляду обумовлена потребою відповідності як на етапі формування проекту [14] так й на етапі вибору діючого стандарту [15].

Відповідно до [14], проблеми серед ЗОЗ наступного характеру:

1. Низька ефективність системи охорони здоров'я, яка, зокрема, характеризується:

А) відсутністю своєчасної та стандартизованої інформації про пацієнта у лікарів, що призводить до дублювання консультацій, лабораторних досліджень, інших медичних послуг на різних рівнях надання медичної допомоги та до нераціональних витрат ресурсів;

Б) використанням медичними працівниками та закладами охорони здоров'я неефективних інструментів, пов'язаних з веденням великої кількості паперових форм медичної документації та збиранням статистичної інформації, яка потребує перегляду та оцінки з точки зору впливу на ефективність функціонування системи охорони здоров'я;

В) екстенсивна форма ведення медичної документації та недостатність інформації про стан здоров'я пацієнта.

2. Інформація про стан здоров'я пацієнта є фрагментованою, первинна медична інформація зберігається у різних надавачів медичних послуг переважно у паперовій формі, що призводить до адміністративного навантаження на медичних працівників та значних часових затрат, недоступності інформації для медичного персоналу поза закладом, високу вірогідність її втрати, низьку можливість для проведення моніторингу, контролю та управління якістю надання медичних послуг;

3. Обмежена доступність медичних послуг. У регіонах України спостерігається неоднорідність покриття мережею закладів охорони здоров'я, нестача кваліфікованого медичного персоналу, непропорційний територіальний розподіл спеціалістів (концентрація у великих містах, недостатність у сільській місцевості), що формує запит на надання медичної допомоги з використанням засобів дистанційного зв'язку;

4. Непрозорість системи охорони здоров'я, недостовірні дані та корупція. Унаслідок того, що практично усі процеси збирання первинних медичних даних та формування медичної статистики пов'язані з паперовим документообігом, в Україні відсутні дієві механізми збору якісної інформації для ухвалення ефективних рішень органами управління системи охорони здоров'я та запобігання зловживанням у цій сфері, у тому числі щодо управління лікарськими засобами, медичними виробами та медичним обладнанням, контролю за доступністю та якістю надання медичної допомоги пацієнтам, зменшення кількості лікарських помилок та зловживань. Збирання та формування медичної статистики розірвані в процесі між собою, відсутня достовірна валідація і верифікація первинних даних, що використовуються для формування статистичної звітності;

5. Недостатньо розвинена національна медична інфраструктура інформатизації, зокрема кадрова спроможність і рівень цифрової компетентності медичних працівників, стан комп'ютеризації закладів охорони

здоров’я. У частині розвитку електронної системи охорони здоров’я та інших інформаційно-комунікаційних систем у сфері охорони здоров’я потребують розв’язання такі проблеми:

А) потреба в забезпеченні сумісності (інтероперабельності) інформаційно-комунікаційних систем у сфері охорони здоров’я, а також елементів загальнонаціональної інтероперабельності та стандартів поширеного єдиного цифрового ідентифікатора особи, єдиного довідника адрес;

Б) екстенсивна форма ведення медичної документації та недостатність інформації про стан здоров’я пацієнта (частина первинної медичної інформації зберігається в різних надавачів медичних послуг в паперовій формі, що призводить до адміністративного навантаження на працівників сфери охорони здоров’я та часових затрат; недостатність інформації в електронній формі про стан здоров’я пацієнта призводить до погіршення якості медичної допомоги).

Відповідно до цих пунктів, досягнення мети цієї Концепції [14] повинно базуватися на таких основних підходах і принципах:

1. Нормування єдиної державної політики щодо розвитку е-здоров’я, забезпечення її ефективної реалізації;

2. Досягнення завдань та індикаторів Цілей сталого розвитку “Забезпечення здорового способу життя та сприяння благополуччю для всіх у будь-якому віці”;

3. Консолідація та координація ресурсів, зусиль та дій державних органів, надавачів медичних послуг, громадян та бізнесу щодо розвитку е-здоров’я;

4. Сприяння наданню усіх видів медичної допомоги та підвищенню якості охорони здоров’я;

5. Управління якістю шляхом використання моделі безперервного поліпшення процесів “плануй - роби - перевіряй - впливай”;

6. Використання передових міжнародних медичних та інформаційних стандартів;

7. Формування єдиного медичного інформаційного простору як сукупності баз та банків даних, технологій їх ведення та використання,

інформаційно-комунікаційних систем та мереж, що функціонують на основі єдиних принципів і загальних правил, що забезпечує інформаційну взаємодію різних сторін і задоволення їх інформаційних потреб, а також інтероперабельність, інтегрованість та гармонійний взаємозв'язок із суміжними сферами;

8. Розвиток національної медичної інфраструктури інформатизації, що, зокрема, включає в себе кадрову спроможність, інформаційні ресурси, технології, продукти і послуги;

9. Створення умов для справедливої конкуренції та розвитку ринку;

10. Використання переваг обробки великих даних та інтелектуальних систем для прогнозування потреб охорони здоров'я, планування ресурсів у сфері;

11. Дебюрократизація та адміністративне спрощення для надавачів медичних послуг;

12. Прозорість та публічна доступність узагальнених даних щодо розвитку е-здоров'я;

13. Забезпечення інформаційної безпеки та захисту інформації і персональних даних, зокрема з урахуванням вимог Законів України "Про захист інформації в інформаційно-комунікаційних системах", "Про захист персональних даних", інших нормативно-правових актів у вказаній сфері, а також Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних), міжнародних стандартів ISO/IEC, інших міжнародних документів та вимог в цій сфері;

14. Орієнтованість електронної системи охорони здоров'я на пацієнта, залучення громадян до піклування про власне здоров'я, контролю за якістю отриманих послуг, зокрема шляхом надання доступу до власних медичних даних та розпорядження ними, а також зручного доступу до актуальних знеособлених відкритих даних;

15. Забезпечення доступу осіб з інвалідністю до послуг у сфері охорони здоров’я.

У підсумку, відповідність ISO 27799 даним вимогам [14] щодо пунктів: **5, 6, 7, 12, 13, 14.**

Відповідно до [15], план заходів потребує:

1. Забезпечення нормативно-правового регулювання переходу від паперових форм первинно-облікової медичної документації, надання форм звітності до ведення електронних медичних записів та формування деперсоналізованих агрегованих звітів на їх підставі;

2. Розроблення дорожньої карти пріоритетних розробок у сфері е-здоров’я;

3. Визначення переліку реєстрів та довідників, які необхідно розробити, з урахуванням вимог до кожного з них;

4. Проведення інвентаризації та оцінки існуючих інформаційно-комунікаційних систем е-здоров’я з метою їх оновлення та інтеграції до єдиного медичного інформаційного простору;

5. Гармонізація національних стандартів з поширеними у світі стандартами та класифікаторами, впровадження міжнародно визнаних і поширених стандартів в Україні для подальшої інтеграції із світовим інформаційним простором;

6. Створення технічних можливостей (PI, спеціалізованих баз з агрегованими знеособленими даними) для доступу до знеособлених агрегованих великих даних (Big Data) в е-здоров’я та прозорих правил їх використання для інститутів громадянського суспільства, вчених, бізнесу, у тому числі з комерційними цілями;

7. Розширення функціональних можливостей електронної системи охорони здоров’я та розвиток інструментів для продовження реформи фінансування системи охорони здоров’я;

8. Розроблення та впровадження ініціатив щодо державно-приватного партнерства з метою розвитку е-здоров’я;

9. Залучення міжнародної технічної допомоги та ресурсів з інших джерел, не заборонених законодавством, на проекти з розвитку е-здоров'я;

10. Розроблення концепції стратегічних напрямів розвитку кібербезпеки;

11. Здійснення заходів щодо впровадження стандартів кібербезпеки на основі стратегічних напрямів розвитку кібербезпеки е-здоров'я, у тому числі проведення моніторингу, захисту та аналізу можливих втручань, втрат, пошкоджень;

12. Створення експериментального середовища для тестування та розвитку інновацій на ринку надання послуг у сфері охорони здоров'я;

13. запровадження функціонування програм та платформ, необхідних для пошуку вразливостей у системах, програмах, реєстрах е-здоров'я, а також проведення постійного моніторингу кіберзагроз в умовах їх стрімкого розвитку;

14. Розвиток цифрових компетентностей, інформаційної культури, цифрової грамотності (цифрової освіченості), кібербезпеки серед медичних працівників і пацієнтів, у тому числі з адаптацією для осіб з інвалідністю з порушеннями зору, слуху, опорно-рухового апарату, мовлення та інтелектуального розвитку, а також з різними комбінаціями порушень;

15. Проведення заходів інформаційного характеру, зокрема опублікування на офіційному веб-сайті МОЗ та НСЗУ узагальнених даних щодо розвитку е-здоров'я;

16. Проведення інформаційних та просвітницьких кампаній із популяризації е-здоров'я, у тому числі з адаптацією для осіб з інвалідністю з порушенням зору, слуху, опорно-рухового апарату, мовлення та інтелектуального розвитку, а також з різними комбінаціями порушень;

17. Забезпечення доступності е-здоров'я для користувачів - пацієнтів з порушеннями зору, слуху, опорно-рухового апарату, мовлення та інтелектуального розвитку, а також з різними комбінаціями порушень відповідно до ДСТУ EN 301 549:2022 (EN 301 549 V3.2.1 (2021-03), IDT) "Інформаційні технології. Вимоги щодо доступності продуктів та послуг ІКТ";

18. Розширення функціональності Єдиного державного веб-порталу електронних послуг “Портал Дія” та його мобільного додатка;

19. Впровадження надійної та безпечної електронної ідентифікації та автентифікації лікарів у сфері е-здоров’я за допомогою інтегрованої системи електронної ідентифікації;

20. Розвиток систем підтримки клінічних рішень, персоналізованої медицини, телемедицини, систем для обробки великих даних (Big Data), штучного інтелекту - інженерної обробки, використання та отримання нових знань, використовуючи модель та дані електронної системи охорони здоров’я і супутніх систем.

У підсумку, відповідність ISO 27799 даним вимогам [14] щодо пунктів: **6, 10, 11, 13, 14, 19** безпосередньо, а також дає змогу реалізувати пункти: **1, 2, 4, 5, 7, 8, 9, 18** та **20** шляхом консолідації джерел інформації через уніфіковані безпекові стандарти.

Як результат, перевага ISO 27799 у більшій відповідності запитам та кращу пристосованість до використання у галузі охорони здоров’я. Подібну орієнтацію на [14; 15] можна простежити і в роботах [77 – 79].

2.3 Огляд наявних шаблонів для впровадження кіберстандартів у медичних закладах

В цілях допомоги ЗОЗ, на сайті Міністерства Охорони Здоров'я України було запропоновано [1] перелік шаблонів.

Цитуючи даний інформаційний портал [1], наданий пакет документів містить у своєму складі:

– політики (Що?), які декларативно визначають стан безпеки відповідно до вимог законодавства, стандартів та найкращих світових практик кібербезпеки;

– процедури (Як?), що описують дії, які треба виконати, щоб досягти стану безпеки, визначеного Політикою інформаційної безпеки, та підтримувати його на рівні, також визначеному цією Політикою;

– посадові обов'язки (Хто?), котрі описують компетенції, якими повинні володіти люди, відповідальні за втілення політик у життя;

– технічні завдання (Чим?), які встановлюють вимоги до інструментів реалізації політик.

Для ефективного використання – було запропоновано використати посібник [80] (див. таблиця 2.3).

Таблиця 2.3

Шаблони для впровадження кіберстандартів у медичних закладах від МОЗ України

Файл, назва документу	Опис документу
Анкета самооцінки	Залежно від низки чинників, які впливають на кібербезпеку закладу охорони здоров'я, є два варіанти шаблонів Політики інформаційної безпеки: «Базовий» (Категорія 1) та «Просунутий» (Категорія 2). Використовуйте Анкету самооцінки для того, щоб визначити, який шаблон Політики інформаційної безпеки обрати для вашого закладу

Продовження табл. 2.3

Файл, назва документу	Опис документу
Шаблон політики ІБ закладу, 1 категорія	Шаблон Політики інформаційної безпеки для закладу охорони здоров'я Категорії 1 (рівень вимог «Базовий» відповідно до Анкети самооцінки). Відредагуйте обраний шаблон Політики інформаційної безпеки таким чином, щоб він відображав поточну ситуацію в закладі. Мінімально обов'язковий рівень редагування вимагає заповнення тексту, позначеного червоним кольором, та перегляд на відповідність тексту, позначеного жовтим кольором. Додатково адаптуйте будь-який інший текст відповідно до застосованої термінології та поточної ситуації в закладі
Шаблон Політики ІБ закладу, 2 категорія	Шаблон Політики інформаційної безпеки для закладу охорони здоров'я Категорії 2 (рівень вимог «Просунутий» відповідно до Анкети самооцінки). Відредагуйте обраний шаблон Політики інформаційної безпеки таким чином, щоб він відображав поточну ситуацію в закладі. Мінімально обов'язковий рівень редагування вимагає заповнення тексту, позначеного червоним кольором, та перегляд на відповідність тексту, позначеного жовтим кольором. Додатково адаптуйте будь-який інший текст відповідно до застосованої термінології та поточної ситуації в закладі
Шаблон посадової інструкції відповідального за інформаційну безпеку	Шаблон Посадової інструкції відповідального за інформаційну безпеку
Процедура управління вразливостями	Шаблон Процедури управління вразливостями
Процедура з експлуатації	Шаблон процедури з експлуатації технічного (ІТ) обладнання

технічного (IT) обладнання	

Продовження табл. 2.3

Файл, назва документу	**Опис документу**
Політика управління ризиками ІБ	Шаблон політики управління ризиками інформаційної безпеки. Адаптуйте і затвердіть Політику управління ризиками інформаційної безпеки. Для всіх інформаційних активів закладу виконайте оцінку ризиків та оберіть запобіжні заходи і процедури з переліку затвердженої Політики інформаційної безпеки. Залишкові ризики, які не покриваються запобіжними заходами з переліку Політики інформаційної безпеки, погоджено та прийнято власниками інформаційних активів. Для мінімізації організаційних та технічних ризиків використовуйте наведені нижче шаблони, які допоможуть закладу у впровадженні запобіжних заходів
Процедура планування відновлення після аварій	Шаблон Процедури планування відновлення після аварій
Процедура управління змінами, 1 категорія	Шаблон Процедури управління змінами (Категорія 1)
Процедура управління змінами, 2 категорія	Шаблон Процедури управління змінами (Категорія 2)
Шаблон А3, 1 категорія	Шаблон Політики антивірусного захисту (Категорія 1)
Шаблон А3, 2 категорія	Шаблон Політики антивірусного захисту (Категорія 2)
Шаблон ТЗ закупівлі АПЗ	Шаблон Технічних вимог до закупівлі антивірусного програмного забезпечення
Шаблон ПК доступу, 1 категорія	Шаблон Політики контролю доступу

	(Категорія 1)

Закінчення табл.2.3

Файл, назва документу	**Опис документу**
Шаблон ПК доступу, 1 категорія	Шаблон Політики контролю доступу (Категорія 2)
Шаблон політики використання мереж і послуг мережі, 1 категорія	Шаблон Політики використання мереж і послуг мережі (Категорія 1)
Шаблон політики використання мереж і послуг мережі, 2 категорія	Шаблон Політики використання мереж і послуг мережі (Категорія 2)
Шаблон ПКЗ, 1 категорія	Шаблон Політики криптографічного захисту (Категорія 1)
Шаблон ПКЗ, 2 категорія	Шаблон Політики криптографічного захисту (Категорія 2)
Процедури роботи з персональними даними	Шаблон Процедури роботи з персональними даними
Процедура управління ВД	Шаблон Процедури управління віддаленим доступом
Вимоги до каналів зв’язку між закладом та МІС	Вимоги до каналів зв’язку між закладом охорони здоров’я та МІС
Шаблон ЧС	Шаблон Політики чистого столу/екрана
Шаблон ПУІБ, 1 категорія	Шаблон Політики управління інцидентами інформаційної безпеки (Категорія 1)
Шаблон ПУІБ, 2 категорія	Шаблон Політики управління інцидентами інформаційної безпеки (Категорія 2)
Порядок самооцінки	Шаблон Порядку проведення самооцінки заходів кібербезпеки

Джерело: складено на основі офіційних даних МОЗ України [1].

Посібником запропоновані наступні кроки щодо впровадження політики інформаційної безпеки в ЗОЗ (орфографічні помилки джерела виправлено):

Крок 1. Оберіть шаблон політики інформаційної безпеки відповідно до рівня вимог закладу охорони здоров'я:

– Залежно від ряду факторів, які впливають на кібербезпеку ЗОЗ, створено два варіанти ПІБ: "Базовий" (Категорія 1) та "Просунутий" (Категорія 2);

– Використовуйте Анкету самооцінки, для того, щоби визначитись з тим, який шаблон ПІБ обрати для Вашого закладу.

Запропоновані матеріали:

– Посилання на Анкету самооцінки;

– Посилання на шаблон ПІБ для рівня «Базовий» (Категорія 1);

– Посилання на шаблон для рівня «Просунутий» (Категорія 2).

Крок 2. Адаптуйте шаблон політики інформаційної безпеки відповідно до поточної ситуації у закладі:

– Відредагуйте обраний шаблон політики інформаційної безпеки таким чином, щоби він відображав поточну ситуацію в закладі;

– Мінімально обов'язковий рівень редагування вимагає заповнення тексту, відміченого червоним кольором та перегляд на відповідність тексту, відміченого жовтим кольором.

– Додатково, адаптуйте будь-який інший текст відповідно до застосованої термінології та поточної ситуації закладу.

Запропоновані матеріали:

– Посилання на матеріали навчального вебінару "Впровадження політики інформаційної безпеки в ЗОЗ"

Крок 3. Затвердіть політику інформаційної безпеки у керівника закладу охорони здоров'я:

– Надайте заповнену політику інформаційної безпеки на затвердження керівнику закладу.

Крок 4. Створіть план оброблення ризиків інформаційної безпеки:

– Для всіх інформаційних активів закладу виконайте оцінку ризиків і оберіть запобіжні заходи та процедури з переліку затвердженої ПІБ.;

– Залишкові ризики, які не покриваються запобіжними заходами з переліку ПІБ погоджені та прийняті власниками інформаційних активів.;

– Для всіх заходів та процедур визначені відповідальні за їх виконання;

– Відповідальні отримали необхідні для виконання своїх обов'язків: а) навчання, б) повноваження, в) ресурсне та технічне забезпечення;

– Для управління ризиками інформаційної безпеки адаптуйте та затвердіть Політику управління ризиками інформаційної безпеки;

– Для мінімізації організаційних та технічних ризиків, використовуйте наступні шаблони, які допоможуть закладу у впроваджені запобіжних заходів (шаблони недоступні).

Запропоновані матеріали:

– Посилання на матеріали навчального вебінару "Політика управління ризиками інформаційної безпеки";

– Посилання на шаблон Політики управління ризиками ІБ;

– Посилання на матеріали навчального вебінару "Відповідальний за інформаційну безпеку в ЗОЗ";

– Посилання на шаблон Посадової інструкції відповідального за інформаційну безпеку;

– Посилання на матеріали навчального вебінару "Управління вразливостями";

– Посилання на шаблон Процедури управління вразливостями;

– Посилання на шаблон Процедури з експлуатації технічного (ІТ) обладнання;

– Посилання на шаблон Процедури планування відновлення після аварій;

– Посилання на шаблон Процедури управління змінами (Категорія 1);

– Посилання на шаблон Процедури управління змінами (Категорія 2);

– Посилання на шаблон Політики антивірусного захисту (Категорія 1);

– Посилання на шаблон Політики антивірусного захисту (Категорія 2);

– Посилання на шаблон Технічних вимог до закупівлі антивірусного програмного забезпечення;

– Посилання на шаблон Політики контролю доступу (Категорія 1);

– Посилання на шаблон Політики контролю доступу (Категорія 2);

– Посилання на шаблон Політики використання мереж і послуг мережі (Категорія 1);

– Посилання на шаблон Політики використання мереж і послуг мережі (Категорія 2);

– Посилання на шаблон Політики криптографічного захисту (Категорія 1);

– Посилання на шаблон Політики криптографічного захисту (Категорія 2);

– Посилання на шаблон Процедури роботи з персональними даними;

– Посилання на шаблон Процедури управління віддаленим доступом;

– Посилання на Вимоги до каналів зв’язку між ЗОЗ та МІС;

– Посилання на шаблон Політики чистого столу/екрану;

– Посилання на шаблон Політики управління інцидентами інформаційної безпеки (Категорія 1);

– Посилання на шаблон Політики управління інцидентами інформаційної безпеки (Категорія 2).

Продовження, після матеріалів, кроку 4: Оберіть відповідний шаблон, адаптуйте його та додайте його до плану оброблення ризиків.

Крок 5. Створіть план самоперевірки інформаційної безпеки:

– Визначте хто, коли і яким чином перевіряє виконання плану оброблення ризиків інформаційної безпеки.

Запропоновані матеріали:

– Посилання на матеріали навчального вебінару "Порядок проведення самооцінки заходів кібербезпеки"

– Посилання на шаблон Порядку проведення самооцінки заходів кібербезпеки

Крок 6. Проведіть самоперевірку інформаційної безпеки:

– Відповідно до плану самоперевірки, проведіть перевірку стану виконання плану оброблення ризиків інформаційної безпеки.

– По результатах перевірки визначте відповідальних за усунення недоліків та впровадження змін і удосконалень.

Крок 7. Створіть план перспективного розвитку системи управління інформаційною безпекою:

– На підставі поточної ситуації створіть план перспективного розвитку для побудови в закладі сталої системи управління інформаційною безпекою.

Більшість документів в посібнику мають статус 404 (недоступні, вилучені, видалені; наявний доступ до окремих з них через вебархів). Окремі з них, на приклад, в кроці №5 – потребує запит. Результат переходу за посиланням на більшість матеріалів з посібника продемонстровано на рисунку (вони типові для кожного з посилань, див рис. 2.2):

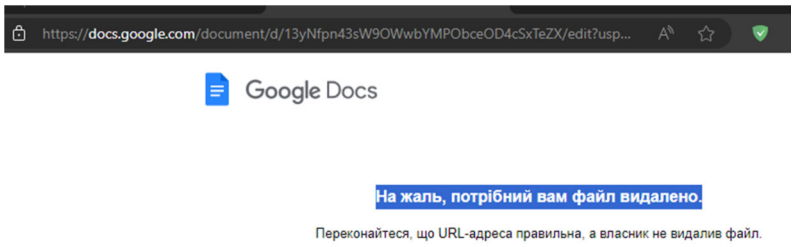


Рис. 2.2 Усі документи відсутні по вказаних в посібнику посиланнях

Варто зауважити, що даний посібник розроблено відповідно до Проекту US□ID – Підтримки реформи охорони здоров'я «Від Американського Народу».

Оглянувши перелік даних шаблонів – можна зробити наступні висновки:

1. Якість даних шаблонів неоднорідна;
2. Орієнтація чи аргументація щодо використання безпекового стандарту (версія, пункт) – не інтуїтивна;
3. Окремі документи мають статус 404 (відсутній доступ);
4. Рекомендації імплементації мають значний поріг входження.

Даний список можна продовжити, але на меті не стоїть знецінити роботу, навпаки – ці напрацювання, багато в чому, недосяжні – так як будуть проігноровані без чітких вказівок (наказів та розпоряджень) на виконання.

Подібні документи (політики безпеки, імплементація безпекових стандартів) – мають характер сценаріїв усіх ймовірних безпекових процесів – а значить мають відповідати галузі. Поліпшити цю справу могли б єдині інструкції щодо застосування даних політик.

Підсумовуючи – наявність даних шаблонів є позитивною динамікою, і свідчить про розвиток галузі eHealth загалом.

Висновки до Розділу 2

Провівши аналіз особливих потреб безпеки інформації в секторі ЗОЗ, вказано, що технологічний процес у секторі охорони здоров'я сприяв відповідності потреб кіберзахисту медичної сфери – іншим галузям, а значить і сприянню успішної імплементації стандартів сімейства ISO 27000. Однак, специфічні вимоги щодо СУІБ ЗОЗ змушує звернути увагу саме на стандарт ISO 27799, як крок щодо уніфікації потреб медичної галузі єдиним сімейством ISO 27000.

Дослідивши досвід діджиталізації системи охорони здоров'я в Україні, можна зробити висновок, що існують різні моделі за якими вони працюють, а саме: централізовані – коли влада та прийняття рішень зосереджені в центральному органі; децентралізовані – коли влада та відповідальність розподілені між різними рівнями або локальними підрозділами та гібридні – коли поєднуються перші дві моделі.

Розглядаючи модель цифровізації медицини України, доцільно зазначити, що вона реалізується на основі дворівневої моделі, а саме гібридної «центроцентричної». Прямим відображенням цього є і «рушії» імплементації «підвищення рівня кібербезпеки» в окремо-взятому ЗОЗ: КП «РОКЛ ім. Семенюка» РОР.

А саме: Наказ №02ОД/6 від 04.01.2024, що має на меті реалізувати «Виконання Плану заходів щодо реалізації Концепції розвитку електронної охорони здоров'я, затвердженого розпорядженням Кабінету міністрів України від 29.09.2021 року № 1175-р та з метою підвищення рівня кібербезпеки» [15], а саме: затвердити Політику інформаційної безпеки, призначити відповідального, затвердити склад Робочої групи з інформаційної безпеки та доручити даній групі забезпечити функціонування інформаційного захисту підприємства, з моніторингом та аудитом. Даний крок не має чітких вказівок.

Як результат: при імплементації можуть знехтувати безпековим стандартом ISO 27799. Відсутність вказівок зі сторони Законів України

підтверджується глибоким аналізом нормативно-правового забезпечення з першого розділу.

Провівши аналіз відповідності запитів щодо Розпоряджень Кабінету Міністрів України [14] та [15], з точки зору проектного бачення [14] та практичних рекомендацій [15] – було підтверджено відповідність цільовому призначенню ISO 27799 як рекомендованому до імплементації, в більшій мірі ніж ISO 27002, задля можливостей сертифікації згідно ISO 27001 [2 – 4; 10].

Провівши аналіз наявних матеріалів у форматі запропонованих шаблонів – сформовано висновок щодо складності їх імплементації з одного боку, але хорошої динаміки розвитку галузі з іншого. В наступному розділі буде проведено аналіз ефективних заходів та запропонованих окремих політик з ресурсу МОЗ України та розглянуто типові сценарії імплементації стандартів ISO 27002 та ISO 27799, як приклад реалізації безпекового стандарту на підприємстві типу ЗОЗ.

РОЗДІЛ 3
ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ В ЗАКЛАДІ ОХОРОНИ ЗДОРОВЯ

3.1. Рекомендації використання безпекових стандартів сімейства ISO 27000

Провівши аналіз Розпоряджень щодо Концепції розвитку eHealth та планів заходів щодо його реалізації [14; 15]. Провівши аналіз нормативно-правового забезпечення, окресливши вимоги щодо безпекових стандартів з

Результатом аналітичного огляду стану рівня кібербезпеки в ЗОЗ та методів його підвищення є сформована пропозиція:

1. У відповідності до діючих розпоряджень щодо підвищення рівня кібербезпеки та інших заходів, що стосуються реалізації концепції розвитку електронної охорони здоров'я і стосуються безпеки інформації – найбільш ефективним рішенням буде імплементація типового набору політик безпеки у відповідності до практичних рекомендацій відповідно до ISO 27002 та ISO 27799.

1.1. Зокрема ISO 27799 є більш відповідною версією ISO 27002, орієнтованою саме на заклади охорони здоров'я, але й вимагаючи дещо більший рівень знань щодо імплементації.

2. Другою підставою проходження відповідної імплементації безпекового стандарту – діючі умови сертифікації та акредитації згідно з міжнародних нормативно-правових документів та діючих співпраць [10; 11].

3. Кількісний характер імплементації політик має бути результатом запиту конкретного ЗОЗ.

3.1 Дане рішення має бути сформовано на підставі висновку та безпосередньо роботи Робочої групи з інформаційної безпеки закладу, на базі якого планується здійснити імплементацію безпекового стандарту.

4. Рішення щодо імплементації має бути в середині робочого життєвого циклу процесу «забезпечення безпеки на підприємстві».

4.1 Даний цикл має починатись із аудитних заходів та складання пропозиції у форматі проекту, закінчуватись верифікацію усіх процесів щодо їх ефективності, реалізації поставлених завдань та прозорості виконання та починатись заново, після проходження повного моніторингу виконання усіх політик на місці імплементації.

Безпека – це не продукт.

Безпека – це процес.

3.2. Рекомендаційні конфігурації Міністерства охорони здоров'я України робочих місць закладів охорони здоров'я, що стосується кібербезпеки

Окремо варто розглянути ефективні рекомендації з сайту МОЗ України. Ці заходи чудово доповнюють загальні політики й можуть мати демонстраційний характер опису процедур. Приклад політик буде розглянуто в розділі 3.4.

3.2.1. Формування кібергігієни на робочому місці ЗОЗ.

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

Реалізовуючи правила кібергігієни на робочому місці – не прямо, виконуються політики безпекових стандартів, що і регулюють дані правила в тому числі. Розглянемо ті з них, які рекомендовані інформаційним порталом МОЗ України.

3.2.2. Правила роботи з паролями на робочому місці закладу охорони здоров'я.

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.

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 МОЗ України [1]: 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 упродовж 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.

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

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 МОЗ України [1]: Змінюйте паролі регулярно – принаймні один раз на рік для паролей від важливих службових програм, якщо частіший період не рекомендовано керівництвом закладу.

Якщо 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.

Примітка МОЗ України [1]: 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;

– не залишайте паролі в інших місцях, де з ними можуть ознайомитися сторонні люди;

– не зберігайте паролі в електронному вигляді у комп'ютері або смартфоні.

Використання мережевих сервісів (продуктів), текстових редакторів та програм для нотаток загального призначення для зберігання паролів **категорично не рекомендується** [1].

3.2.3. Використання двофакторної автентифікації на робочому місці закладу охорони здоров’я.

Двофакторна автентифікація (2F□) є процесом, що вимагає від користувача подання двох різних форм ідентифікації для отримання доступу до облікового запису. Це часто використовується як додатковий захисний етап для захисту ваших облікових записів і онлайн-сервісів. 2F□ є важливою, оскільки вона додає додатковий рівень безпеки до вашого облікового запису, що ускладнює процес незаконного доступу. Навіть якщо зловмисник знає ваш

пароль, він все одно не зможе увійти в систему, оскільки він потребує другого фактору автентифікації.

Як працює 2FA: шляхом використання двох з трьох можливих "факторів": щось, що ви знаєте (наприклад, пароль), щось, що ви маєте (наприклад, смартфон), або щось, що ви є (наприклад, ваш відбиток пальця). Деякі поширені приклади двофакторної автентифікації включають SMS-повідомлення з кодом, яке відправляється на ваш телефон після введення пароля, мобільні додатки, що генерують коди, та біометричні фактори, такі як відбитки пальців або розпізнавання обличчя.

Рекомендовані мобільні додатки для 2FA:

Google □uthenticator – це одна з найпопулярніших програм для двофакторної автентифікації, що створює коди автентифікації на вашому мобільному пристрої.

Microsoft □uthenticator – це інший широко використовуваний сервіс для двофакторної автентифікації, який також дозволяє використовувати багатофакторну автентифікацію.

□uthy – це служба двофакторної автентифікації, яка працює з багатьма веб-сайтами і сервісами. □uthy надає різні опції для отримання кодів 2F□, включаючи SMS, дзвінки та мобільні програми.

Переваги 2FA:

Збільшена безпека: додавання ще одного рівня автентифікації значно знижує ризик несанкціонованого доступу до облікового запису. Захист даних: 2F□ є важливим інструментом для захисту вашої особистої та фінансової інформації. Зменшення шансів крадіжки ідентичності: навіть якщо ваш пароль став відомим, зловмисники все одно не зможуть отримати доступ до ваших облікових записів без другого фактору автентифікації. Важливо пам'ятати, що 2F□ є лише одним з компонентів загальної безпеки в Інтернеті. Це не повинно замінити інші важливі заходи безпеки, такі як використання складних паролів, регулярна зміна паролів і недопущення передачі своїх паролів іншим.

3.2.4. Безпечна робота в мережі Інтернет на робочому місці ЗОЗ.

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

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).

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 – індикація використання https трафіку та відповідного сертифікату безпеки (див. рис. 3.1, 3.2, 3.3, залежно від використаного браузера).

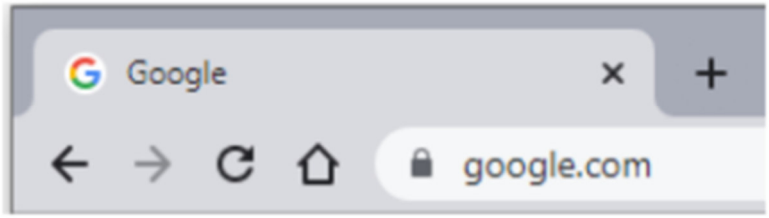


Рис. 3.1 Іконка замкненого замка у веб-браузері Google Chrome

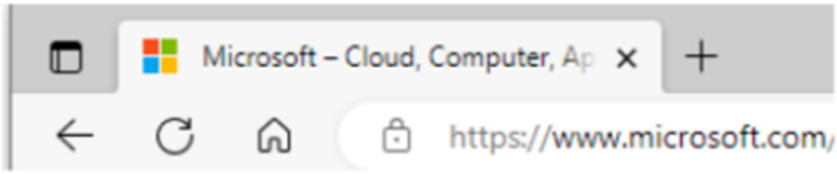


Рис. 3.2 Іконка замкненого замка у веб-браузері Microsoft Edge

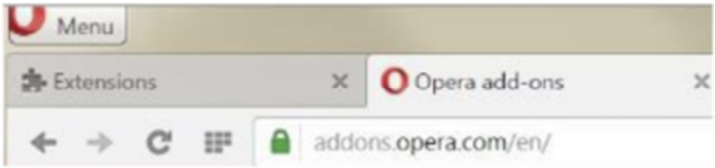


Рис. 3.3 Іконка замкненого замка у веб-браузері Opera

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. 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. Скопіювати адресу веб-сайту, репутацію якого треба перевірити, в «буфер обміну». Для цього виділіть текст адреси. Після чого, одночасно натисніть дві клавіші на клавіатурі: «Ctrl» та «c».

Крок 2. Відкрити веб-сервіс Url Scan за допомогою посилання https://urlscan.io/ (див. рис. 3.4):

Рис. 3.4 Фрагмент головної сторінки веб-сервісу Url Scan

Крок 3. Ввести адресу сайту у веб-сервіс Url Scan (див. рис. 3.5):

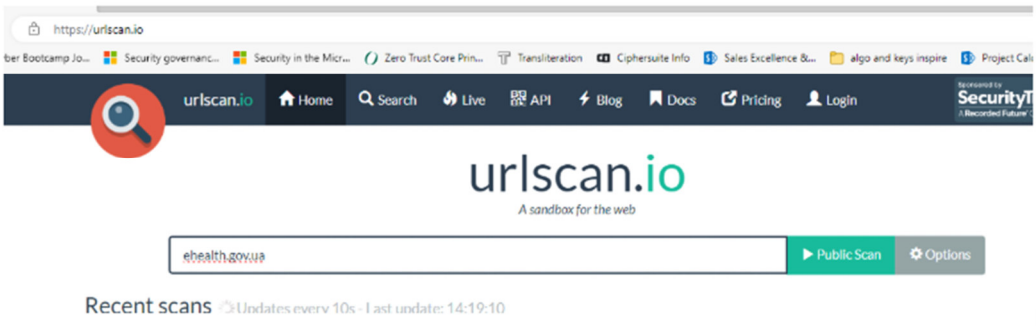


Рис. 3.5 Перевірка адреси сайту у веб-сервісі Url Scan

Крок 4. Натиснути зелену кнопку «Public Scan» (див. рис. 3.6):

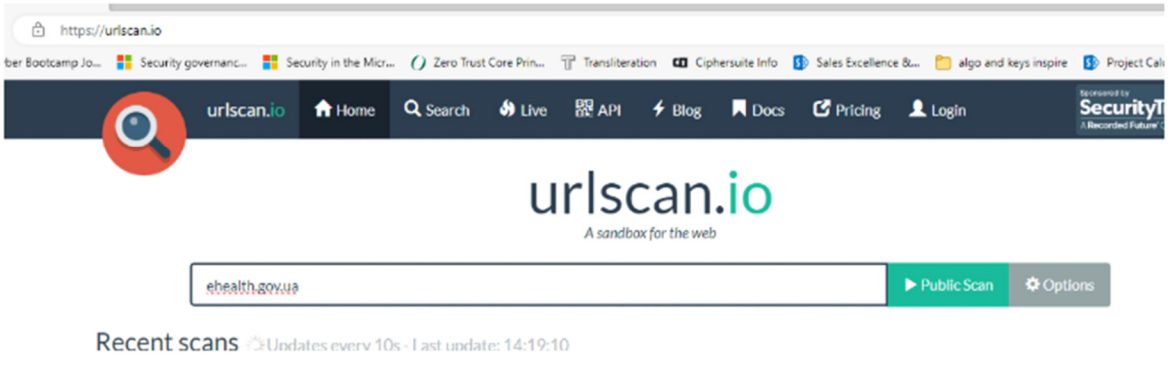


Рис. 3.6 Перевірка адреси сайту у веб-сервісі Url Scan

Крок 5. Проаналізувати аналіз сканування (див. рис. 3.7, 3.8):

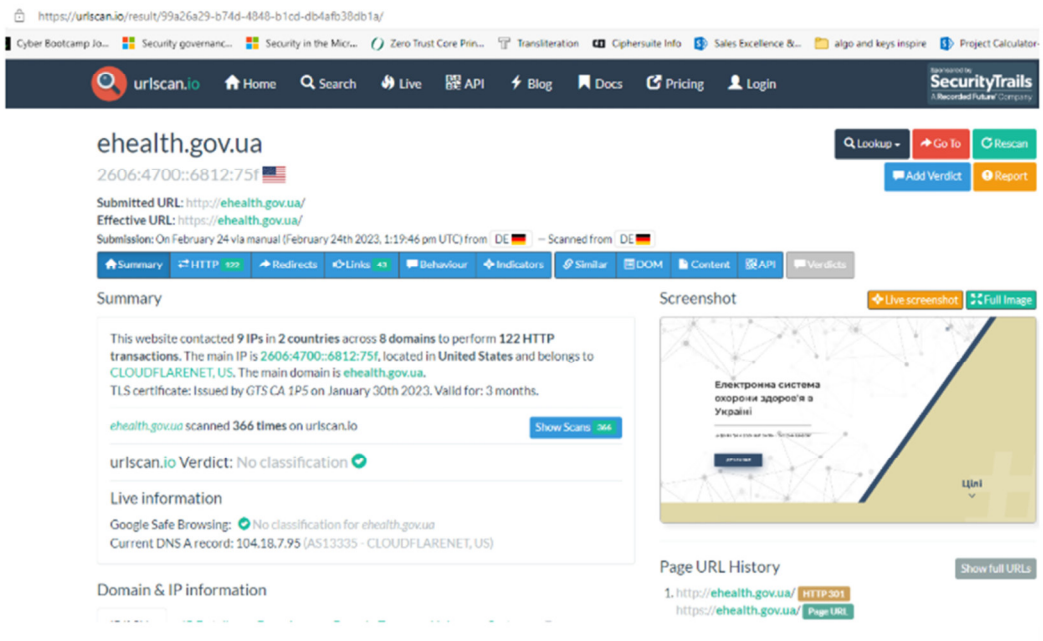


Рис. 3.7 Приклад результатів сканування

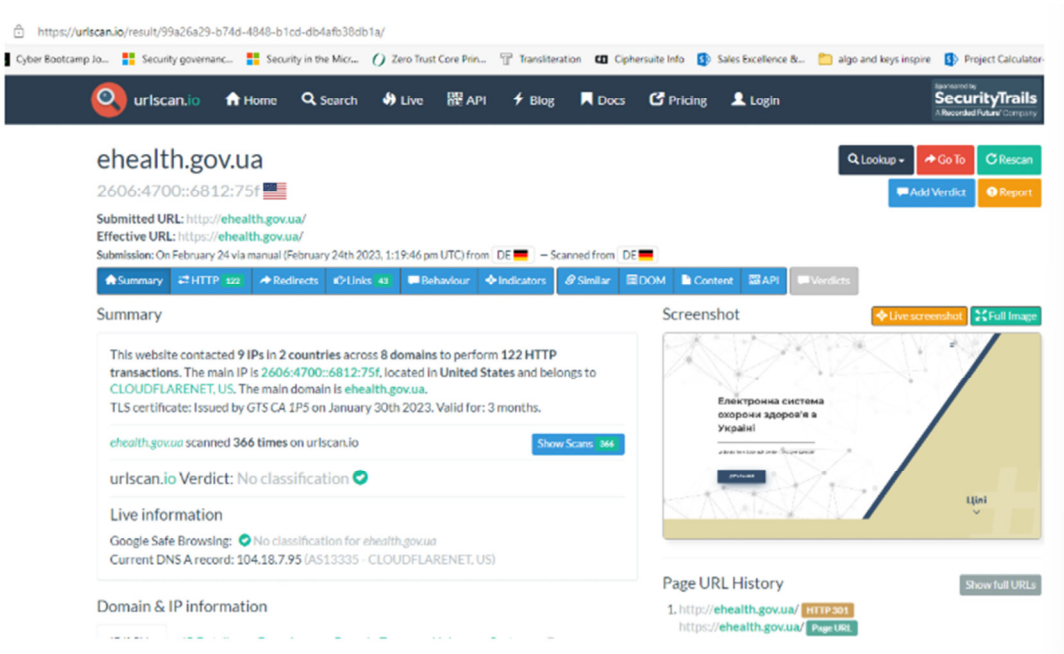


Рис. 3.8 Приклад результатів сканування

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 кібербезпеки.

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.

Необхідна обережність 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.

Не рекомендується [1]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.

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.

3.2.5. Рекомендації при роботі з WiFi мережею в ЗОЗ.

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

Категорично не рекомендується [1] 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.

3.2.6. Рекомендації по роботі з електронною поштою

Наступні рекомендації покликані зменшити ризик витоку конфіденційних даних через кіберзагрози, пов'язані з використанням робочої електронної пошти [1]**:**

– не використовувати 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;

– 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 зберігати 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;

– остерігатися фішингових листів;

– 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;

– остерігатися листів, що можуть містити файли зі шкідливим програмним забезпеченням.

Примітка МОЗ України [1]: 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.

Окремої уваги варте нагадування, що запуск документу у розширенні, для прикладу, *.doc та *.docx – аналогічно, по наслідку, від запуску застосунку з розширенням *.exe, тощо, так як вищезгадані документи запускаються у середовищі Microsoft Word, по замовчуванню, а дане середовище може виконувати приховані скрипти за аналогією шкідливого ПЗ типу «вірус», «троян», тощо.

3.2.7. Правило порожнього робочого столу на комп’ютері в ЗОЗ.

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.

3.2.8. Рекомендаційні заходи щодо протидії фішингу на робочому місці ЗОЗ від МОЗ України.

У кожному секторі економіки і в кожній країні працює правило: «користувач – це найбільш вразлива ланка ланцюга захисту інформації в організації» [1] 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 із жертвою зазвичай встановлюється через електронну пошту, соціальні мережі або месенджери.

Як було зазначено, кінцева мета фішингу – це отримання конфіденційних даних. Нижче наводиться короткий огляд інформації, яка є пріоритетною для зловмисників [1].

Варто зауважити, що фішинг базується на соціальній інженерії типу «загроза по замовчуванню». Це модель поведінки, при якій необхідно діяти згідно протоколам безпекових стандартів та політик безпеки, адже все що за межами їх – може загрожувати інформаційній безпеці працівника, а тому й всьому закладу.

Хорошою практикою щодо формування політик безпеки, на етапі проектної пропозиції робочою групою з інформаційної безпеки є ідентифікація загроз. Саме загрози є підґрунтям щодо потреби в кіберзахисті. І вони ж піддаються моніторингу та їх стан кібербезпеки піддається верифікації. Аби успішно ідентифікувати загрози – корисно буде ідентифікувати дані, за якими «полюють» зловмисники.

У більшості випадків зловмисників найбільше цікавить наступна інформація закладів охорони здоров'я:

– 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 закладу, телефони співробітників (в тому числі, внутрішні телефонні номери);

– технічні засоби і програмно-апаратне забезпечення закладу;

– інформація про підрядників закладу;

– вся інформація, що Ви публікуєте особисто або Ваші друзі/колеги публікують про Вас у мережі Інтернет, може бути використана зловмисникам проти Вас. Чим більше інформації має злодій, тим вища ймовірність успіху в реалізації злочину.

Рекомендаційні заходи щодо боротьби з фішингом відповідно до порад МОЗ України щодо кібергігієни на робочому місці [1]:

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: *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* [1].

Окрім того, варто зауважити ефективність «зворотної» соціальної інженерії (знову ж таки, ідентифікація ймовірних загроз): 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:

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

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.

Сором: сором зізнатися в недостатності комп'ютерних знань і, як результат, несвоєчасне звернення за кваліфікованою допомогою.

Доброта: надмірна доброта і альтруїзм можуть спонукати людину надати допомогу, поступаючись звичайними правилами безпеки або втрачаючи пильність.

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.

3.3.10. Кібергігієна щодо використання інтернет-посилань в електронних листах на робочому місці комп’ютера в ЗОЗ.

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 в пункті 3.3.4. Безпечна робота в мережі Інтернет на робочому місці закладу охорони здоров’я). 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». Поширеною 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 закладу не завжди можуть бути впевнені в тому, що пацієнт, який зайшов до їхнього 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”.

3.3. Приклад конфігурацій політик безпеки відповідно до безпекового стандарту ISO 27001

Другим результатом магістерської роботи, окрім аналітичного огляду із супровідними рекомендаціями щодо застосування ISO 27799 – є сформований пакет політик безпеки, типового зразку, що масштабований для підприємства типу заклад охорони здоров'я, відповідно до розглянутого раніше випадку щодо реалізації Наказу КП «РОКЛ ім. Ю. Семенюка» РОР «Про Впровадження політики інформаційного захисту» №02ОД/6 від 04.01.2024р. Даний пакет політик розміщено в повній мірі в межах додатку до магістерської роботи (див. додаток А). Дані політики мають навмисно-загальний характер відображення в цілях дотримання інформаційної гігієни. З іншої сторони, типовість форми, в котрій вони розміщені – дають змогу масштабувати дані політики на будь який інший заклад охорони здоров'я.

В межах згаданого наказу було вказано наступні наказові пункти: затвердити політику інформаційної безпеки КП «РОКЛ ім. Ю. Семенюка» РОР, Призначити відповідального за інформаційну безпеку, затвердити склад Робочої групи з інформаційної безпеки, доручити даній групі забезпечити функціонування інформаційного захисту підприємства, з моніторингом та аудитом ІТ та ПЗ.

Відповідно до даного завдання, слідуючи методиці розробки та життєвого циклу імплементації безпекового стандарту – запропоновано проектне рішення для розгляду та використання. Перелік наведених політик наведено в таблиці (див. таблиця 3.1).

Як видно з переліку політик та опису – в даній магістерській роботі було оглянуто конкретні приклади щодо даних політик у форматі правил та рекомендацій [75; 77]. Звісно, сертифікаційні переваги не єдина «сильна» сторона використання безпекових стандартів сімейства ISO 27000, а ще – гнучкість, масштабованість, типовість, інтуїтивність.

Єдиним недоліком – необхідний поріг входження щодо:

А) розуміння що ISO 27000 сімейство існує;

Б) розуміння які процеси дане сімейство стандартів регламентує;

В) розуміння як це застосувати;

Г) знання, що для ЗОЗ є стандарт ISO 27799 в межах даного сімейства.

Найбільш важливим в роботі є не лише перелік та напрацьовані політики, що додані до додатку А (див. додаток А), а вказування їх доцільності (перша перевага), а також вказування на можливість та ефективність використання спеціалізованого стандарту ISO 27799 на відміну від типового ISO 27002 (друга перевага).

Таблиця 3.1

Пропоновані політики безпеки для типового ЗОЗ, відповідно до додатку А

Назва політики безпеки	**Призначення**
□cceptable Use Policy (□UP)	Загальні правила
Bring Your Own Device (BYOD)	Щодо особистих пристроїв
Clear Desk and Clear Screen Policy (CDCS)	Щодо екранів, робочих столів
Encryption Policy	Шифрування даних
Information Classification Policy	Класифікація інформації
Information Security Policy	Інформаційна безпека
Internet and Email Usage Policy	Інтернет та електронна пошта
Malware Protection Policy	Щодо шкідливого ПЗ
Network Security Policy	Мережеві аспекти
Password Policy	Безпека паролів
Physical and Environmental Security Policy	Фіз. та екологічна безпека
Software Installation Procedure	Встановлення ПЗ
System and □pplication □ccess Control Policy	Управління доступом

Опанувати стандарт значно простіше, коли є відомості що він існує та вартий уваги. Найкращий сценарій, підсумовуючи проведену роботу –

продовжувати робити посібники та методичні матеріали та вебінари для закладів ЗОЗ зі сторони МОЗ України.

Це величезний крок вперед.

Лишилось підтримати ініціативу не лише на централізованому рівні, виправдовуючи центроцентричну систему, а й на рівні департаментів – займатись допомогою в імплементації, або, хоча б, теоретично-методичним супроводом до даного процесу.

Варто зауважити, що результатом даного розділу є формування політик безпеки, котрі ніяким чином не можуть бути розміщені в дипломній роботі, через їх обсяг, але будуть прикріплені у форматі додатку до роботи.

Дані висновки отримують підґрунтя серед наступних досліджень: [86-95].

Окремо варто звернути увагу до попередні дослідження [81-84], в котрих виконано перші етапи роботи щодо формування даного твердження.

Висновки до Розділу 3

Розглянувши рекомендації використання безпекових стандартів сімейства ISO 27000 було аргументовано підтвердження ефективність запропонованих МОЗ України рекомендацій та правил щодо формування кібергігієни на робочому місці.

З подальшого розділу стало зрозумілим, що це інтерпретація політик безпеки типового характеру з ISO 27000 сімейства. Й разом з тим, вони не втрачають свою актуальність, але втрачають централізацію, єдність та фундаментальність.

Дані безпекові стандарти мають бути імплементовані цілісно на підприємство, аби комплексно задіяти власні можливості. І саме ця риса не реалізована якщо на дані політики дивитись лишень як на правила. А отже й значно падає ефективність.

Окрім того, варто відзначити практичний вміст рекомендацій МОЗ. Варто зауважити, що саме в такому формфакторі рекомендації та політики найкраще можна імплементувати при використанні серед працівників ЗОЗ із браком кваліфікації в сфері кіберзахисту (найбільш вірогідний сценарій при кожному ЗОЗ). З негативного – більшість документів із пропонованого в посібнику списку – недоступні. Важко перевірити ефективність пропозицій, все ж таки, як політик безпеки, а не лише деталізованих та якісних рекомендацій.

Звісно, ідеальний сценарій – це ефективна робота Робочої групи на підприємстві, котра з проекту сформує подібні деталізовані та інструкційно пророблені сценарії кожного із аспектів, що регламентовані стандартом (більшість з них наведені в таблиці 3.1).

ВИСНОВКИ

В роботі оглянуто питання кібербезпеки в сфері електронної охорони здоров’я, як окремих компонентів ЗОЗ, так і частини екосистеми Е-здоров’я.

Оглянуті нормативно-правові матеріали та методики імплементації безпекових стандартів, окремо оглянуто підґрунтя кібербезпеки як такої, в цілях орієнтації на захист як на процес, а не продукт.

Проведено аналіз сфери питання кібербезпеки в сфері охорони здоров’я. Визначено сутність захисту інформації та роботи з персональними даними у закладі здоров’я. Досліджено організаційно-правове забезпечення сфери захисту інформації та роботи з персональними даними в закладах охорони здоров’я. Проведено паралелі щодо взаємозв’язків кібербезпеки та діджиталізації.

Окремо оглянуто зміни в сфері стандартів кібербезпеки через призму нового стандарту ISO 27799 та його місця в сфері охорони здоров’я.

Проведено аналіз ефективності імплементації як рекомендаційних політик, окремого характеру по кожному із питань, так і цілісного підходу щодо погляду на безпекові політики як частину безперервного життєвого циклу процесу «кібербезпеки». Проведено аналіз перспектив та потреб імплементації стандарту ISO 27799 – як через критичність медичної інфраструктури так й через відповідні Розпорядження щодо схвалення Концепції розвитку електронної охорони здоров'я.

Варто зауважити, що імплементація політик безпеки у будь якому з оглянутих виглядів – матиме не лише виконавчу функцію щодо Розпоряджень, а й посприяє ефективному розвитку ЗОЗ локального характеру.

Виокремлено думку, що задля підтримки ініціативи МОЗ України – подібні процедури популяризації та допомоги з імплементацією безпекових стандартів варто перейняти й регіональним департаментам, в цілях покращення регіональної ситуації.

Окремо варто зауважити, що хоч заклад, на базі якого проводилось дослідження імплементації безпекового стандарту не відповідає класичному дослідженню напряму державного управління, але проведено паралелі з державною службою в межах охорони здоров’я, котрі, до всього, пролили світло на зв'язок структури даної галузі як впливу на результативність імплементації безпекових стандартів загалом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кібербезпека. Міністерство охорони здоров'я України – офіційний вебсайт. URL: https://moz.gov.ua/uk/kiberbezpeka (дата звернення: 09.10.2024).

2. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems - Requirements. [Чинний від 2022-09-03]. URL: https://www.iso.org/standard/27001 (дата звернення: 09.10.2024).

3. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security controls. [Чинний від 2022-09-03]. URL: https://www.iso.org/standard/75652.html (дата звернення: 09.10.2024).

4. ISO 27799:2016. Health informatics — Information security management in health using ISO/IEC 27002. 2nd edition. [Чинний від 2016-07]. URL: https://www.iso.org/standard/62777.html (дата звернення: 09.10.2024).

5. Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks. URL: https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/ (дата звернення: 09.10.2024).

6. Susukailo V., Opirsky I., Yaremko O. Methodology of ISMS Establishment gainst Modern Cybersecurity Threats. *Lecture Notes in Electrical Engineering. Springer International Publishing.* 2021. С. 257–271. URL: https://doi.org/10.1007/978-3-030-92435-5_15.

7. Sari P. K., Handayani P. W., Hidayanto . N., ji R. F. and Yazid S. Challenges of Inter-organizational Information Security in Healthcare Services: Health Regulator's Perspective. *International Conference on Informatics, Multimedia, Cyber and Information System.* ICIMCIS, Jakarta, Indonesia, 2021. pp. 1-6, https://doi: 10.1109/ICIMCIS53775.2021.9699177.

8. Paul P. C., Loane J., McCaffery F. and Regan G.. Data Security nd Privacy Risk Management Framework For WB N Based Healthcare pplications. *IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events.* PerCom Workshops, Kassel,

Germany, 2021, pp. 704-710, https://doi:10.1109/PerComWorkshops51409.2021.9431069.

9. Premi V. C. G., Solainayagi P., Srinivasan C. and Kuppusamy P. G. Data Privacy and Confidentiality in Healthcare pplications of IoT-Enabled Wireless Sensor Networks. *Second International Conference On Smart Technologies For Smart Nation.* SmartTechCon, Singapore, Singapore, 2023, pp. 610-614, https://doi:10.1109/SmartTechCon57526.2023.10391743.

10. ДСТУ ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements (ISO/IEC 27001:2022, IDT). [Чинний від 2023-08-22]. Вид. офіц. Київ, 2023. 19с.

11. Про прийняття національних стандартів, зміни до національного стандарту та скасування національних стандартів: Наказ Кабінету Міністрів України від 17.08.2023р. № 210. Дата оновлення 28.08.2023р. URL: https://zakon.rada.gov.ua/rada/show/v0210774-23#Text (дата звернення: 09.10.2024).

12. Kurii, Y., & Opirskyy, I. (2023). ISO 27001: Аналіз змін та особливості відповідності новій версії стандарту. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *3*(19), С. 46–55. https://doi.org/10.28925/2663-4023.2023.19.4655

13. Загальний регламент про захист даних (GDPR). Офіційний переклад українською мовою. Джерело: URL: kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf URL: https://gdpr-text.com/uk/ (дата звернення: 09.10.2024).

14. Про схвалення Концепції розвитку електронної охорони здоров'я: Розпорядження Кабінету Міністрів України від 28.12.2020р. № 1671-р. Дата оновлення 06.09.2024р. URL: https://zakon.rada.gov.ua/laws/show/1671-2020-%D1%80#Text (дата звернення: 09.10.2024).

15. Про затвердження плану заходів щодо реалізації Концепції розвитку електронної охорони здоров'я: Розпорядження Кабінету Міністрів України від 29.09.2021р. №1175-р. Дата оновлення 26.03.2024р.

URL: https://zakon.rada.gov.ua/laws/show/1175-2021-%D1%80#Text (дата звернення: 09.10.2024).

16. Про основні засади забезпечення кібербезпеки України: Закон України від 21.06.2018р. № 2469-VIII. Дата оновлення 05.06.2024р. № 3783-IX. URL: https://ips.ligazakon.net/document/view/T172163?an=237&q=кібербезпека (дата звернення: 09.10.2024).

17. WannaCry. Матеріал з Вікіпедії — вільної енциклопедії. URL: https://uk.wikipedia.org/wiki/WannaCry (дата звернення: 09.10.2024).

18. Хакерські атаки на Україну (2017). Матеріал з Вікіпедії — вільної енциклопедії. URL: https://uk.wikipedia.org/wiki/Хакерські_атаки_на_Україну_(2017) (дата звернення: 09.10.2024).

19. Про основні засади забезпечення кібербезпеки України: Закон України від 05.06.2024р. № 3783-IX. *Відомості Верховної Ради України*, 2017р., № 45, ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 09.10.2024).

20. Easttom C. and Butler W. □ Modified McCumber Cube as a Basis for a Taxonomy of Cyber □ttacks. *IEEE 9th Annual Computing and Communication Workshop and Conference.* CCWC, Las Vegas, NV, US□, 2019, pp. 0943-0949, https://doi:10.1109/CCWC.2019.8666559.

21. McCumber, John (2004). Hegel's Epistemology: □ philosophical introduction to the 'phenomenology of spirit'. Continental Philosophy Review 37 (3):367-381.

22. Varela, Martín & Zwickl, Patrick & Reichl, Peter & Xie, Min & Schulzrinne, Henning. From Service Level □greements (SL□) to Experience Level □greements (EL□): The challenges of selling QoE to the user. 2015. https://doi:10.1109/ICCW.2015.7247432.

23. Maximum Tolerable Period of Disruption (MTPOD). BCM Institute. URL: https://www.bcmpedia.org/wiki/Maximum_Tolerable_Period_of_Disruption_(MTPOD) (дата звернення: 09.10.2024).

24. Zhylin □., Beliavsky V. Bakalynsky O. NIST CSF 2.0: New Cybersecurity Framework from the National Institute of Standards and Technology of the United States. *Ukrainian Scientific Journal of Information Security*, 2024, vol. 30, issue 1, pp. 73-76.

25. CYBERSECURITY – NIST. □n official website of the United States government. URL: https://www.nist.gov/cybersecurity (дата звернення: 09.10.2024).

26. RM□N full backup vs. level 0 incremental. Pythian Blog: Technical Track. URL: https://www.pythian.com/blog/technical-track/rman-full-backup-level-0-incrmental (дата звернення: 09.10.2024).

27. Про захист персональних даних: Закон України від 22.02.2024р. № 3585-IX. *Відомості Верховної Ради України*, 2010р., № 34, ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 09.10.2024).

28. Про затвердження Порядку вибору лікаря, який надає первинну медичну допомогу, та форми декларації про вибір лікаря, який надає первинну медичну допомогу: Наказ Міністерства охорони здоров’я України від 19.03.2018р. № 503. Дата оновлення 07.03.2023р. URL: https://zakon.rada.gov.ua/laws/show/z0347-18#Text (дата звернення: 09.10.2024).

29. Деякі питання електронної системи охорони здоров'я: Постанова Кабінету Міністрів України від 25.04.2018р.№ 411. Дата оновлення 04.07.2024. URL: https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#Text (дата звернення: 09.10.2024).

30. Söderström, Eva & Åhlfeldt, Rose-Mharie & Eriksson, Nomie. Standards for information security and processes in healthcare. *J. Systems and IT.* 2009. №11. pp. 295-308. https://doi:10.1108/13287260910983650.

31. Tyali, S. & Pottas, Dalenca. Information security management systems in the healthcare context. *Proceedings of the South African Information Security Multi-Conference*, S□ISMC 2010. pp. 177-187.

32. Про інформацію: Закон України від 10.10.2024р. № 4017-IX. *Відомості Верховної Ради України*, 1992, № 48, ст. 650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 09.10.2024).

33. Цивільний кодекс України від 05.06.2024р. № 3778-IX. *Відомості Верховної Ради України*, 2003, №№ 40-44, ст. 356. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 09.10.2024).

34. Сімейний кодекс України від 29.10.2024р. № 1-р/2024. *Відомості Верховної Ради України*, 2002, №21-22, ст. 135. URL: https://zakon.rada.gov.ua/laws/show/2947-14#Text (дата звернення: 09.10.2024).

35. Основи законодавства України про охорону здоров'я: Закон України від 21.08.2024р. № 3911-IX. *Відомості Верховної Ради України*, 1993, № 4, ст. 19. URL: https://zakon.rada.gov.ua/laws/show/2801-12#Text (дата звернення: 09.10.2024).

36. Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних: Закон України від 03.07.2013р. № 383-VII. *Відомості Верховної Ради України*, 2014, № 14, ст. 252. URL: https://zakon.rada.gov.ua/laws/show/z0001-12#Text (дата звернення: 09.10.2024).

37. Кращі практики управління кібербезпекою. Оглядовий звіт. Комітет з питань цифрової трансформації. URL: https://www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_04.pdf (дата звернення: 09.10.2024).

38. Cybersecurity Capability Maturity Model (C2M2). □n official website of the United States government. URL: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2 (дата звернення: 09.10.2024).

39. Cybersecurity Maturity Model Certification 2.0 Program. □n official website of the United States government. URL: https://www.cisa.gov/resources-tools/resources/cybersecurity-maturity-model-certification-20-program (дата звернення: 09.10.2024).

40. Patel, Pratik & Deshpande, Vivek. □pplication Of Plan-Do-Check-□ct Cycle For Quality □nd Productivity Improvement-□ Review. International Journal for Research in □pplied Science & Engineering Technology. 2017. №5, pp. 197-201.

41. Російські атаки на енергетичну систему України змушують медиків працювати в темряві — звіт. Physicians for Human Rights. 04.12.2024. URL: https://phr.org/news/російські-атаки-на-енергетичну-систе/ (дата звернення: 06.12.2024).

42. За минулий рік українська електронна система охорони здоров'я «відбила» низку цілеспрямованих фішингових та DDoS-атак. Міністерство охорони здоров'я України – офіційний сайт. 24.05.2023р. URL: https://moz.gov.ua/uk/za-minulij-rik-ukrainska-elektronna-sistema-ohoroni-zdorov%E2%80%99ja-vidbila-nizku-cilesprjamovanih-fishingovih-ta-ddos-atak- (дата звернення: 09.10.2024).

43. Маганова Т. В. Щодо забезпечення інформаційної безпеки в медичних освітніх закладах України: виклики війни / Т. В. Маганова, С. В. Приходченко, В. О. Дубина // *Перспективи та інновації науки. Педагогіка. Психологія. Медицина.* - 2023. - N 9. - С. 678-686. https://doi.org/10.52058/2786-4952-2023-9(27)-678-686.

44. Шевчук Р.В. Механізми розвитку Національної системи охорони здоров'я в контексті забезпечення Національної Безпеки в Україні. public-management [інтернет]. 07.12.2022р., №5 (33):127-31. (дата звернення: 06.12.2024).

45. Курепін В. М. Забезпечення трудових прав в умовах воєнного стану // Актуальні проблеми сучасної науки в дослідженнях молодих учених, курсантів та студентів : тези доп. *Всеукр.наук.-практ. конф.* (м. Вінниця, 17 травн. 2023 р.) / МВС України, Харків. нац. ун-т внут. справ, Наук. парк «Наука та безпека». Вінниця : ХНУВС 2023. С. 316-319.

46. Ляшук А. Загрози і виклики для системи кібербезпеки інформаційних систем та реєстрів сфери охорони здоров'я. ПУ [інтернет]. 29, Грудень 2023р., (6):113-21. (дата звернення: 06.12.2024).

47. Савченко Д., Доценко Т. В. Теоретичні аспекти взаємозв'язків кібербезпеки та безпеки охорони здоров'я // *Виклики кібербезпеки індустрії фінансових послуг : матеріали II наукової онлайн-конференції* / за заг. ред. доц.

В. В. Койбічук, м. Суми, 02 липня 2024 р. Суми : Сумський державний університет, 2024. С. 23-26.

48. Кучеренко В., Хожило І. (2024). Безпека медичних установ як напрям глобальної політики у сфері охорони здоров'я. *Матеріали конференцій МЦНД*, (04.10.2024; Ужгород, Україна), 70–73.

49. Тім П. Огляд законодавства ЄС, пов'язаного з громадським здоров'ям. – 2020. – 113 с. [Електронний ресурс] URL: https://eu-ua.kmu.gov.ua/sites/default/files/inline/files/oglyad_zakonodavstva_yes_u_sferi_ohorony_zdorovya.pdf (дата звернення: 06.12.2024).

50. Горбатова Д. І. Форми державного управління у сфері охорони здоров'я. Право і суспільство. – 2019. – № 4. – С. 166–173 [Електронний ресурс] URL: http://pravoisuspilstvo.org.ua/archive/2019/4_2019/26.pdf., с. 166. (дата звернення: 06.12.2024).

51. Про схвалення Стратегії розвитку сфери інноваційної діяльності на період до 2030 року: Розпорядження Кабінету Міністрів України від 10.07.2019р. № 526-р. URL: https://zakon.rada.gov.ua/laws/ show/526-2019-р#Text (дата звернення: 06.12.2024).

52. Про внесення змін до Закону України "Про захист персональних даних": Закон України від 20.11.2012р. № 5491-VI. *Відомості Верховної Ради України*, 2013р. №51, ст.751. URL: https://zakon.rada.gov.ua/laws/show/5491-17/#Text (дата звернення: 06.12.2024).

53. Роз'яснення щодо наслідків незаконного розголошення лікарської таємниці (ЛЖВ). Українська Гельсінська Спілка з прав людини. 12.09.2018р. URL: https://www.helsinki.org.ua/articles/roz-yasnennya-schodo-naslidkiv-nezakonnoho-rozholoshennya-likarskoji-tajemnytsi-lzhv/ (дата звернення: 06.12.2024).

54. Кримінальний кодекс України від 20.11.2024р. № 4074-IX. *Відомості Верховної Ради України,* 2001р., №25-26, ст.131. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 06.12.2024).

55. Про оперативно-розшукову діяльність: Закон України від 18.07.2024р. № 3887-IX. *Відомості Верховної Ради України*, 1992, № 22, ст. 303. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text (дата звернення: 06.12.2024).

56. Про прокуратуру: Закон України від 25.09.2019р. № 1789-XII. URL: https://zakon.rada.gov.ua/laws/show/1789-12#Text (дата звернення: 06.12.2024).

57. Про прокуратуру: Закон України від 23.09.2024р. № 1697-VII. *Відомості Верховної Ради України*, 2015, № 2-3, ст. 12. URL: https://zakon.rada.gov.ua/laws/show/1697-18#Text (дата звернення: 06.12.2024).

58. Про адвокатуру та адвокатську діяльність: Закон України від 15.11.2024р. № 5076-VI. *Відомості Верховної Ради України*, 2013, № 27, ст. 282. URL: https://zakon.rada.gov.ua/laws/show/5076-17#Text (дата звернення: 06.12.2024).

59. Про страхування: Закон України від 08.11.2024р., № 1909-IX. Відомості Верховної Ради України, 2023р., №№ 12-13, ст. 28. URL: https://zakon.rada.gov.ua/laws/show/1909-20#Text (дата звернення: 06.12.2024).

60. Деякі питання електронної системи охорони здоров'я: Постанова Кабінету Міністрів України від 25.04.2018р., № 411. Дата оновлення 04.07.2024р. URL: https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#Text (дата звернення: 06.12.2024).

61. Пояснювальна записка до проєкту розпорядження Кабінету міністрів України «Про схвалення Стратегії розвитку інноваційної діяльності України на період до 2030 року». [Електронний ресурс] URL: https://thedigital.gov.ua/storage/uploads/files/FIN-ПОЯСНЮВАЛЬНА%20ЗАПИСКА.pdf (дата звернення: 06.12.2024).

62. Концепція розбудови електронної охорони здоров'я в Україні. Міністерство охорони здоров'я – офційний сайт. URL: https://moz.gov.ua/uk/koncepciya-rozbudovi-elektronnoyi-ohoroni-zdorov-ya-ukrayini (дата звернення: 06.12.2024).

63. Горбатова Д. І. Форми державного управління у сфері охорони здоров'я. Право і суспільство. – 2019. – № 4. – С. 166–173 URL:

http://pravoisuspilstvo.org.ua/archive/2019/4_2019/26.pdf (дата звернення: 06.12.2024).

64. Вострикова К. С. Публічне адміністрування в сфері охорони громадського здоров'я в Україні умовах реалізації медичної реформи : дип. магістр права. Запоріжжя. – 2020. – 126 с.

65. Борщ В. В. Система охорони здоров'я як структурний елемент національної безпеки України. Науковий вісник Ужгородського національного університету. – 2019. – Вип. 23 (1). – С. 19–23 URL: http://www.visnykeconom.uzhnu.uz.ua/archive/23_1_2019ua/6.pdf (дата звернення: 06.12.2024).

66. Hübner, Ursula Hertha and Marc □. Elmhorst. "eBusiness in healthcare: from eProcurement to supply chain management." (2008).

67. Sullivan, F. and Wyatt, J. Published by Blackwell, 2006. ISBN 10: 0727918508 / ISBN 13: 9780727918505.

68. Hübner, Ursula & Elmhorst, Marc. (2008). eBusiness in Healthcare.

69. Magadi, M.□., Madise, N.J. and Rodrigues, R.N. (2000) Frequency and Timing of □ntenatal Care in Kenya: Explaining the Variations between Women of Different Communities. *Social Science & Medicine*, № 51, pp. 551-561. https://doi.org/10.1016/S0277-9536(99)00495-5.

70. Frangopoulos, E.D., & Eloff, M.M. (2004). □ Comparative Study of Standards and Practices related to Information Security Management. *In: Peer-reviewed Proceedings of the ISSA 2004 Enabling Tomorrow Conference*. 30 June – 2 July 2004, Midrand, South □frica: ISS□. Retrieved May 21, 2008, URL: http://icsa.cs.up.ac.za/issa/2004/Proceedings/Full/033.pdf (дата звернення: 06.12.2024).

71. Siponen, M. Information Security Management Standards: Problems and Solutions. *In: Proceedings of the 7th Pacific Asia Conference on Information Systems*. 10-13 July 2003, □delaide, South □ustralia. Retrieved November 17, 2008. URL: http://www.pacis-net.org/file/2003/papers/security/284.pdf (дата звернення: 06.12.2024).

72. □hlfeldt, R-M. Information security in distributed healthcare domain: Exploring the problems and needs of different healthcare providers. *In Licentiate Thesis*. 2006. № 06-003, Stockholm University. Sweden.

73. Janczewski, L., & Xinli Shi, F. (2002). Development of Information Security Baselines for Healthcare Information Systems in New Zealand. *Computers and Security*, 21(2), 172-192.

74. Експертна думка. HIP□□-compliance в українському контексті: як працювати вітчизняній компанії? Асоціація працівників України – Ukrainian Bar □ssociation. URL: https://uba.ua/eng/news/ekspertna-dumka-hipaacompliance-v-ukrainskomu-kontekst-jak-pracjuvati-vtchiznjanjj-kompani (дата звернення: 06.12.2024).

75. ISO/DIS 27799. Draft international standart. [в розробці] URL: https://www.iso.org/standard/84647.html (дата звернення: 06.12.2024).

76. ISO 27001 vs. ISO 27002: Understanding the difference. Nemko. URL: https://www.nemko.com/iso-27001-vs-iso-27002 (дата звернення: 06.12.2024).

77. Ляшук, А. Загрози і виклики для системи кібербезпеки інформаційних систем та реєстрів сфери охорони здоров'я. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2023. №6, С. 113–121.

78. Коваль Б., Коваль Л., Пойда С. Навчання майбутніх лікарів основам медіаграмотності та кібербезпеки. *Перспективи та інновації науки*. 2023. №8(26). С. 171–183.

79. Трофименко О., Дубовий Я., Логінова Н., Прокоп Ю., Задерейко О. Питання кібербезпеки медичних комп'ютерних систем. *Захист інформації*. 2021. №23(1). С. 30–39.

80. Шаблони для впровадження кіберстандартів у медичних закладах. Міністерство охорони здоров'я України – офіційний сайт. URL: https://moz.gov.ua/uk/shabloni-dlja-vprovadzhennja-kiberstandartiv-u-medichnih-zakladah (дата звернення: 06.12.2024).

81. Бабич С.В., Цецик Я.П., Красномовець О.І. Виклики електронного урядування: перспективи через досвід. *Актуальні питання у сучасній науці. Серія: Державне управління*, 2024, № 11(29). С. 287-301.

82. Бабич С.В., Тихончук Л.Х. Глобальна ініціатива. *Big Data Earth: планетарна діджиталізація. Серія: Економічні науки.* Вип. 4(104), 2023. С. 36-56.

83. Цецик Я.П., Бабич С.В., Проказюк І.С. Міжнародний досвід впливу якості цифрових комунікацій в сфері медичних послуг на результативність їх надання. *Наукові перспективи.* 2024, № 11(53). С. 408-424.

84. Бабич С.В., Цецик Я.П. Проблеми кібербезпеки та тенденції використання штучного інтелекту в сфері охорони здоров'я. *Успіхи і досягнення у науці.* 2024, №9(9). С. 357-374.

85. Бабич С.В. Технології та алгоритми обману для боротьби з кібератаками. Кваліфікаційна робота на здобуття освітнього ступеня «Магістр» зі спеціальності 125 - Кібербезпека. Тернопіль: ЗУНУ, 2022, 81 с.

86. Трохимчук, В. В., С. Г. Убогов. Науково-практичні підходи до формування інтегрованих систем управління на оптових та роздрібних фармацевтичних підприємствах». 2018.

87. Панченко, Олег. Інформаційна складова національної безпеки. Вісник Національної академії Державної прикордонної служби України. Серія: державне управління, 2019, 3.

88. Левківський, В. Л. Аналіз структури та функціональних можливостей медичних інформаційних систем україни. Вісник Херсонського національного технічного університету, 2023, 3 (86): С. 111-118.

89. Недбайло, Ю. Розробка пропозицій щодо удосконалення системи управління якістю фармацевтичного підприємства АТ «Лубнифарм». Харків, 2024. 87 с.

90. Макогонський В. В. Використання інформаційних технологій для розвитку діяльності закладу охорони здоров'я (на прикладі КНП "Старосинявська ЦРЛ", смт. Стара Синява, Хмельницька обл.) : дипломна

робота магістра : 073 Менеджмент.Хмельниц. нац. ун-т. Хмельницький, 2021. 73 с.

91. Васюк Н. О., Юрочко Т. П. Публічне управління охороною здоров'я в сучасних умовах реформування в Україні. Державне управління: теорія та практика. 2019. № 1. С. 78-84.

92. Василенко Ю. М. Діджиталізація системи охорони здоров’я: вітчизняний та зарубіжний досвід : кваліфікаційна робота на здобуття освітнього ступеня «магістр» : 281 «Публічне управління та адміністрування». ЧНУ ім. Петра Могили. Миколаїв, 2023. 92 с.

93. Саядов, І. І. Інтеграція потоків даних BSN в єдину хмарну платформу ЕСОЗ (e-health) : магістерська дис. : 122 Комп’ютерні науки. Київ, 2021. 102 с.

94. Даценко О. А. Удосконалення нормативного забезпечення діяльності органу, який здійснює аудит і сертифікацію систем менеджменту відповідно до вимог стандарту ISO/IEC 17021-3 : робота на здобуття кваліфікаційного ступеня магістра : спец. 152 – метрологія та інформаційно-вимірювальна техніка . Суми : Сумський державний університет, 2023. 56 с.

95. Цимбал В. С. Захист персональних даних: особливості правового регулювання та практики застосування в Україні та країнах ЄС : кваліфікаційна робота магістра спеціальності 081 «Право». Запоріжжя : ЗНУ, 2020. 125 с.

Додаток А

Конфігуровані політики безпеки для закладів охорони здоров'я

Відповідно до розділу 3.3 – в даному додатку запропоновані типові конфігуровані політики для закладів охорони здоров'я (див табл. А 1.1):

Таблиця А 1.1

Наведені політики безпеки в додатку А

Додаток	Назва політики	Ст.
Додаток А.1	Політика прийнятного використання	127
Додаток А.2	Політика використання особистих пристроїв	137
Додаток А.3	Політика «чистого робочого столу та екрану»	142
Додаток А.4	Політика шифрування	145
Додаток А.5	Політика класифікації інформації	150
Додаток А.6	Політика інформаційної безпеки	153
Додаток А.7	Політика використання інтернету та електронної пошти	157
Додаток А.8	Політика захисту від шкідливих програм	163
Додаток А.9	Політика захисту в мережі	168
Додаток А.10	Політика використання паролів	172
Додаток А.11	Політика фізичної та екологічної безпеки	177
Додаток А.12	Процедура встановлення програмного забезпечення	182
Додаток А.13	Політика управління доступом	185

Дані політики мають бути масштабовані для обраного ЗОЗ шляхом створення робочої групи та застосування відповідних політик в сферах, які вони регулюють через безпосередню роботу групи та через навчання персоналу. Виконання даних політик зобов'язане супроводжуватись моніторингом та верифікацією їх ефективності та успішності. Політики безпеки, що регулюють напрями інформаційної та робочої діяльності котрі не використовуються в закладі – мають бути спростовані та вилучені.

Додаток А.1

Політика прийнятного використання – Acceptable Use Policy (AUP)

1. Огляд

1.1 Вступ

Ефективна інформаційна безпека є командною роботою, що передбачає участь і підтримку кожного співробітника **ЗОЗ**, який працює з інформацією **ЗОЗ** та її супутніми активами. Відповідальність за знання цих вказівок і відповідну поведінку у своїй діяльності покладається на кожного користувача комп'ютера.

1.2 Мета

Метою цієї Політики є описати прийнятне використання інформації та її супутніх активів, таких як інформаційні обробні засоби та мережеві ресурси в **ЗОЗ**, а також захистити користувачів та **ЗОЗ** від загальних ризиків безпеки.

1.3 Відповідальність

Співробітники та підрядники **ЗОЗ**:

- Відповідальні за дотримання правил цієї Політики та інших підтримуючих політик інформаційної безпеки при роботі з інформацією ЗОЗ та її супутніми активами.
- Відповідальні за виявлення добросовісного судження щодо відповідного використання інформації, інформаційних систем, електронних пристроїв та мережевих ресурсів відповідно до політик і процедур **ЗОЗ**, а також місцевих законів і норм.

2. Положення політики

2.1 Загальне використання та право власності

1. Інформація **ЗОЗ** (включаючи інформацію її клієнтів), збережена в інформаційних системах і обчислювальних пристроях, що належать або орендовані **ЗОЗ**, співробітниками або підрядниками **ЗОЗ** чи третіми особами

(разом далі – "користувачі"), залишається виключною власністю **ЗОЗ**. Усі користувачі повинні забезпечити захист інформації **ЗОЗ** за допомогою організаційних, технічних або юридичних засобів відповідно до встановленої схеми класифікації інформації.

2. Усі користувачі зобов'язані невідкладно повідомляти Системних адміністраторів про крадіжку, втрату чи несанкціоноване розкриття інформації **ЗОЗ**.

3. Користувачі повинні отримувати доступ, використовувати або ділитися інформацією **ЗОЗ** лише в тій мірі, в якій це дозволено та необхідно для виконання їхніх службових обов'язків.

4. З метою безпеки та обслуговування мережі уповноважені особи **ЗОЗ** можуть в будь-який час контролювати обладнання, системи та мережевий трафік.

5. **ЗОЗ** залишає за собою право періодично проводити аудит мереж і систем для забезпечення відповідності цій Політиці.

2.2 Правила фізичної безпеки

1. Співробітникам **ЗОЗ** видаються особисті електронні картки доступу у формі значка, що надає їм відповідний доступ до приміщень починаючи з дати прийому на роботу.

2. Співробітники повинні завжди носити свої картки під час перебування в приміщеннях **ЗОЗ**.

3. Під час звільнення всі співробітники повинні повернути свої картки доступу інженеру з комп’ютерних технологій, відповідальному за це. Такі картки повинні бути заблоковані/деактивовані наприкінці дня звільнення.

4. Ключі та картки доступу не повинні залишатися без нагляду в очевидному місці або носитися так, щоб їх легко було втратити або вкрасти.

5. Користувачі повинні повідомляти Системним адміністраторам про будь-яку потенційну або реальну проблему безпеки, включаючи несанкціонований вхід, крадіжку майна або втрату ключів чи електронних карток.

2.3 Правила класифікації інформації

2.3.1 Класифікація інформації

1. Інформацію **ЗОЗ** слід класифікувати, враховуючи потреби в обміні чи обмеженні інформації, а також правові вимоги.

2. Інформація, що належить, створена, оброблена, збережена або знищена **ЗОЗ**, може бути класифікована в одну з трьох категорій:

а) Загальна - інформація доступна загальному загалу, співробітникам та підрядникам **ЗОЗ**, клієнтам і партнерам через уповноважені канали. Загальна інформація не є чутливою за контекстом чи змістом і не потребує спеціального захисту конфіденційності. Втрата доступності через зупинку системи є прийнятним ризиком. Цілісність важлива, але не критична.

б) Внутрішня / Тільки для внутрішнього використання - інформація доступна співробітникам **ЗОЗ** та іншим уповноваженим підрядникам, які потребують цієї інформації для виконання своїх функціональних обов'язків. Інформація цієї категорії не повинна розкриватися за межами **ЗОЗ** без дозволу. Її розкриття може призвести до негативного впливу на діяльність **ЗОЗ** та рівень наданих послуг або спричинити незначні фінансові втрати для співробітників або **ЗОЗ**. Збереження цілісності та доступності важливе, але не критичне.

в) Конфіденційна - будь-які дані або власна інформація **ЗОЗ** , що не є загальновідомими або ще не були розкриті, незалежно від їхньої матеріальної чи нематеріальної форми. Розкриття конфіденційної інформації обмежується конкретним підрозділом/департаментом **ЗОЗ** і не може розкриватися за межами конкретних груп, уповноважених мати доступ до цієї інформації. Таке розкриття може призвести до значної шкоди конкурентній перевазі, партнерству, відносинам та репутації. Конфіденційна інформація доступна лише особам, які виконують певні функції або ролі. Збереження цілісності, конфіденційності та обмеженої доступності є важливим. Дозвіл є обов'язковим для обміну конфіденційною інформацією. **До даної категорії належить і інформації категорії «державної таємниці» (далі - секретної інформації).**

3. Для прикладів інформації кожної категорії класифікації, будь ласка, зверніться до Політики класифікації інформації.

2.3.2 Маркування інформації

1. Конфіденційна інформація **ЗОЗ** повинна бути промаркована міткою класифікації "Конфіденційно". Маркування внутрішньої інформації є бажаним, але не обов'язковим.

2. Процес маркування застосовується лише до інформації в електронному вигляді. Зокрема, під час створення документів, особливо тих, що будуть надіслані клієнтам та партнерам (наприклад, внутрішні політики та процедури, пропозиції послуг, звіти тощо), слід використовувати корпоративні шаблони з попередньо визначеним форматом і мітками класифікації, коли це можливо.

3. Мітки класифікації повинні з'являтися в заголовку або в нижньому колонтитулі принаймні на першій сторінці документованої інформації; їх також можна додати на кожній наступній сторінці за бажанням.

2.3.3 Правила обробки інформації

1. У деяких випадках внутрішня та конфіденційна інформація можуть вимагати дозволу перед її розповсюдженням внутрішнім чи зовнішнім отримувачам. Розповсюдження означає тут розподіл, копіювання, надсилання або будь-які інші форми надання доступу до інформації чи її супутніх активів для перегляду, копіювання, обробки, модифікації або видалення інформації.

2. Зокрема:

а) внутрішня інформація вимагає дозволу на розповсюдження зовнішньо (включаючи зовнішніх підрядників);

б) конфіденційна інформація вимагає дозволу на розповсюдження:

I. зовнішньо (включаючи зовнішніх підрядників);

II. внутрішньо з членами іншого підрозділу/відділу.

3. Дозвіл на розповсюдження внутрішньої інформації з зовнішніми сторонами не потрібен, якщо ці сторони зазначені в розділі "Цільова аудиторія" документа.

4. Дозвіл на розповсюдження конфіденційної інформації з членами тієї ж групи (наприклад, підрозділу, проекту тощо) не потрібен.

5. Дозвіл на розповсюдження внутрішньої та конфіденційної інформації може бути отримано відповідно до наступної процедури:

а) дозвіл на розповсюдження документованої інформації має бути отримано від Власника документа;

б) якщо Власник інформації невідомий або через обставини неможливо отримати дозвіл, дозвіл має бути отримано від керівника співробітника, який бажає поділитися інформацією;

в) якщо керівник невідомий, або через обставини неможливо отримати дозвіл, або керівник має сумніви щодо надання дозволу на розповсюдження інформації, запит на розповсюдження має бути направлений до члена Керівної команди, відповідального за підрозділ/відділ, з якого надійшов запит;

г) якщо жоден із визначених затверджувачів недоступний або якщо у них є сумніви щодо надання дозволу на розповсюдження інформації, дозвіл має бути наданий СТО.

6. Дозвіл на розповсюдження може бути наданий у наступних форматах:

а) усний дозвіл може бути наданий для розповсюдження внутрішньої інформації як внутрішньо, так і зовнішньо;

б) усний дозвіл може бути наданий для розповсюдження конфіденційної інформації внутрішньо;

в) письмовий дозвіл (наприклад, через електронну пошту) є обов'язковим для розповсюдження конфіденційної інформації зовнішньо.

7. Внутрішня та конфіденційна інформація повинні зберігатися в безпечному місці (наприклад, в закритих офісних приміщеннях), щоб запобігти несанкціонованому доступу. Доступ до цієї інформації має контролюватися фізичними та/або логічними засобами контролю доступу і повинен бути обмежений для співробітників **ЗОЗ** та уповноважених підрядників. Зокрема:

а) інформація в електронному вигляді має зберігатися в корпоративних інформаційних системах (наприклад, SharePoint) або на мережевих ресурсах, затверджених **ЗОЗ**

б) інформація в паперовому вигляді повинна зберігатися в замкнених сейфах або шафах для документів.

8. Співробітники та підрядники **ЗОЗ** повинні забезпечити, щоб жодна інформація **ЗОЗ** не зберігалася виключно на їхніх локальних робочих станціях.

9. Більше правил щодо належної обробки інформації **ЗОЗ** можна знайти в Політиці класифікації інформації.

2.4 Правила безпеки робочої станції

1. Користувачам рекомендується використовувати виключно робочі станції, надані **ЗОЗ** , для робочих завдань.

2. Як виняток, співробітникам **ЗОЗ** може бути надано дозвіл використовувати свої особисті пристрої для роботи, якщо для цього є обґрунтоване обґрунтування відповідно до Політики використання особистих пристроїв.

3. Для забезпечення безпеки інформації **ЗОЗ** корпоративні робочі станції оснащені попередньо встановленим програмним забезпеченням для захисту від шкідливих програм та програмним забезпеченням для управління мобільними пристроями (MDM). Адміністратори системи відповідають за установку цього програмного забезпечення на робочих станціях.

4. Користувачі повинні переконатися, що їхні робочі станції використовують ліцензійні та підтримувані версії авторизованих операційних систем (OS) та програмних додатків з останніми доступними оновленнями та виправленнями відповідно до Списку стандартного програмного забезпечення.

5. Користувачам забороняється перевстановлювати спочатку встановлену операційну систему (OS) на їхніх робочих станціях. Якщо така необхідність виникає, перевстановлення ОС на робочих станціях (включаючи пристрої BYOD) має бути узгоджено з адміністраторами системи, щоб забезпечити відповідність вимогам безпеки після перевстановлення ОС.

6. Користувачі не повинні намагатися змінити або вимкнути будь-які налаштування безпеки, застосовані до робочої станції адміністраторами системи.

7. Якщо користувач вважає, що корпоративна робоча станція або пристрій BYOD можуть бути заражені вірусом, трояном, шпигунським програмним забезпеченням або іншою загрозою шкідливого програмного забезпечення, він/вона повинні негайно повідомити адміністраторам системи в письмовій формі про потенційний інцидент безпеки інформації.

8. Якщо користувач втратив або загубив корпоративну робочу станцію або пристрій BYOD, він/вона повинні негайно повідомити адміністраторам системи в письмовій формі про потенційний інцидент безпеки інформації.

2.5 Правила безпеки паролів

2.5.1 Використання секретної аутентифікаційної інформації

1. Секретна аутентифікаційна інформація користувача, така як паролі, повинна залишатися конфіденційною, забезпечуючи, щоб її не розголошували іншим сторонам, включаючи інших співробітників, адміністраторів системи, менеджерів та осіб, які мають повноваження. Групова (наприклад, спільна) секретна аутентифікаційна інформація повинна зберігатися виключно серед членів групи.

2. Секретна аутентифікаційна інформація не повинна зберігатися в запису (наприклад, написана на папері, збережена в програмному файлі або знімку екрана) без попередньої авторизації. Зокрема:

а) паролі повинні відповідати критеріям безпеки (мінімум 12 символів, комбінація великих і малих літер, цифр і спеціальних символів;

б) не повинні бути простими, поширеними словами, такими як "пароль" або "123456");

в) паролі, використовувані для роботи з обліковими записами, повинні бути унікальними та не використовуватися для особистих облікових записів.

3. Співробітники зобов'язані використовувати унікальні паролі для своїх робочих облікових записів, уникаючи використання одного й того ж пароля для особистих облікових записів.

2.5.2 Захист секретної аутентифікаційної інформації

1. Співробітники не повинні зберігати секретну аутентифікаційну інформацію у неперевірених форматах (наприклад, зберігання паролів у браузері без паролів, використовуючи текстовий документ або електронну таблицю), крім схвалених безпечних сховищ, наприклад, за допомогою "сховища паролів", дозволених **ЗОЗ**.

2. Функція браузера "Запам'ятати пароль" дозволяється лише за певних умов, що стосуються корпоративних облікових записів, які розроблені, щоб зменшити ризик витоку.

3. У разі підозри на те, що пароль може бути скомпрометований, співробітники зобов'язані негайно зв'язатися з адміністраторами системи та змінити пароль.

2.6 Правила установки програмного забезпечення

1. Встановлення несанкціонованого програмного забезпечення заборонено.

2. Встановлення програмного забезпечення яке дозволено:

а) оновлення стандартного програмного забезпечення, затвердженого для встановлення та використання на робочих станціях співробітників;

б) програмне забезпечення, яке було попередньо схвалено клієнтом.

3. Будь-яке програмне забезпечення, яке викликає підозри, має бути подане на перевірку адміністраторам системи.

2.7 Правила використання Інтернету та електронної пошти

2.7.1 Використання Інтернету

1. Співробітники повинні використовувати Інтернет для робочих завдань, а не для особистих цілей. Зокрема, надмірне використання особистих ресурсів в Інтернеті заборонено.

2. Корпоративні мережі повинні використовуватися для виконання робочих завдань; особисті пристрої мають бути використані, зокрема, для перевірки електронної пошти, за умови, що це управлінське рішення. Використання особистих пристроїв для виконання завдань, що вимагають використання інформації **ЗОЗ** , обмежене.

3. **ЗОЗ** залишає за собою право перевіряти та моніторити Інтернет-трафік, дані та електронну пошту.

4. Усі користувачі повинні дотримуватися професіоналізму в усіх онлайн-комунікаціях.

5. Заборонені дії включають:

а) завантаження та використання піратського програмного забезпечення;

б) неналежне спілкування (неетичні, неприязні або загрозливі повідомлення) чи будь-яка спроба передати конфіденційну інформацію за межі **ЗОЗ**.

2.7.2 Використання електронної пошти

1. Співробітники повинні використовувати корпоративні електронні адреси виключно у робочих цілях.

2. Співробітники повинні уникати використання сторонніх систем електронної пошти для ділових комунікацій, якщо це можливо.

3. Користувачі повинні негайно повідомляти та видаляти підозрілі електронні листи.

2.8 Оцінка відповідності

1. **ЗОЗ** залишає за собою право перевіряти відповідність цій Політиці та підтримуючим політикам інформаційної безпеки ЗОЗ різними методами, включаючи, але не обмежуючись, періодичними перевірками, внутрішніми та зовнішніми аудитами, а також зворотним зв'язком для Керівної команди.

2. Порушення політик і правил **ЗОЗ** може мати серйозні наслідки для **ЗОЗ** , співробітників та підрядників **ЗОЗ**, такі як репутаційні збитки, цивільна, адміністративна чи кримінальна відповідальність, а також санкції, накладені державними органами.

3. **ЗОЗ** очікує, що її співробітники та підрядники повністю дотримуватимуться правил і політик ЗОЗ. **ЗОЗ** проводить моніторинг і аудити дотримання внутрішніх політик. Порушення політик **ЗОЗ** може призвести до дисциплінарних заходів, аж до припинення відносин, компенсації збитків тощо.

Додаток А.2

Політика використання особистих пристроїв – Bring Your Own Device (BYOD)

1. Огляд

1.1 Вступ

Типовою проблемою для організацій сьогодні є те, що їхні співробітники не усвідомлюють, що особисті пристрої, які використовуються для роботи, представляють загрозу інформаційній безпеці ЗОЗ. У результаті вони часто не застосовують ті ж самі процедури безпеки та захисту інформації, як це робили б для корпоративних робочих станцій. Тому ЗОЗ **ЗОЗ** необхідно встановити належні правила використання та контролю особистих пристроїв, які використовуються для роботи, а також визначити, які кроки слід дотримуватись під час ініціювання та завершення використання пристроїв.

1.2 Мета

Метою цієї Політики є описання кроків, яких повинні дотримуватися **ЗОЗ** та її співробітники при використанні особистих пристроїв для робочих завдань.

1.3 Відповідальність

Співробітники **ЗОЗ**:

● Відповідальні за запит на дозвіл використання особистого пристрою для роботи.

● Відповідальні за забезпечення того, щоб їхні особисті пристрої відповідали вимогам безпеки, викладеним у цій Політиці.

Менеджерський склад / менеджери підрозділів/відділів:

● Відповідальні за надання дозволу на використання особистих пристроїв для роботи.

Системні адміністратори:

● Відповідальні за періодичний аудит налаштувань безпеки на особистих пристроях, що використовуються для роботи.

2. Положення політики

2.1 Принципи використання пристроїв BYOD у ЗОЗ

1. Співробітникам **ЗОЗ** рекомендується використовувати для робочих завдань виключно робочі станції, надані **ЗОЗ**. Як виняток, співробітникам **ЗОЗ** може бути надано дозвіл на використання особистих пристроїв для роботи, якщо на це є вагомі ділові підстави.

2. Використання особистого пристрою для роботи має бути письмово схвалене менеджером користувача.

3. **ЗОЗ** залишає за собою право відкликати цей дозвіл, якщо співробітник не виконує положення, викладені в цій Політиці, або з будь-якої іншої причини, яку **ЗОЗ** вважає розумною.

4. **ЗОЗ** виплачує співробітникам грошові виплати або компенсації за використання їхніх особистих пристроїв для роботи.

5. Для роботи можуть використовуватися лише ті пристрої, які відповідають технічним та програмним вимогам **ЗОЗ**.

6. Співробітник погоджується з тим, що з моменту, коли пристрій введено в експлуатацію, він підлягає тим же правилам і нормам, що застосовуються до пристроїв, що належать організації та надані **ЗОЗ** своїм співробітникам, якщо в цій Політиці не вказано інше.

7. Користувачі несуть особисту відповідальність за всі витрати, пов’язані з їхніми пристроями.

8. **ЗОЗ** не несе відповідальності за зберігання або пошкодження пристроїв і не покриває витрати, пов’язані з ремонтом пристроїв.

9. По можливості **ЗОЗ** забезпечує обробку (встановлення/оновлення/видалення) програмного забезпечення, необхідного для виконання обов’язків та завдань користувачів або надання послуг.

10. Співробітник може попросити компанію керувати налаштуваннями безпеки пристроїв BYOD. У цьому випадку команда IT **ЗОЗ** повинна забезпечити співробітника корпоративними засобами управління мобільними пристроями (MDM) та програмним забезпеченням для забезпечення безпеки

кінцевих точок та налаштувати пристрої відповідно до корпоративних стандартів і політик **ЗОЗ** . В іншому випадку співробітник повинен забезпечити відповідність своїх пристроїв BYOD вимогам Розділу 2.3 Вимоги до безпеки пристроїв BYOD.

11. Пристрої BYOD, якими **ЗОЗ** не управляє, можуть підлягати періодичному аудиту. Власників активів можуть попросити надати детальну інформацію про налаштування активу та допомогти аудиторам у зборі необхідних доказів.

2.2 Процедура ініціювання та завершення використання пристроїв BYOD

1. Перед введенням пристрою в експлуатацію має бути отримано письмове схвалення відповідного менеджера відповідно до розділу 2.1(2) цієї Політики.

2. У разі переходу в новий підрозділ або відділ співробітник має отримати нове схвалення.

3. Користувач несе особисту відповідальність за забезпечення того, щоб особистий пристрій, що використовується для роботи, відповідав наведеним нижче технічним вимогам. Системні адміністратори мають право перевіряти, чи сумісний пристрій із технічними вимогами на вибірковій основі.

4. Припинення використання пристрою може бути ініційовано **ЗОЗ** або співробітником, зокрема під час припинення відносин.

5. Якщо користувач відключає, готує до повернення або інакше припиняє використання особистого пристрою, який був авторизований для роботи, він повинен повідомити Системних адміністраторів, що пристрій більше не буде використовуватися для підключення до ресурсів, систем і мереж ЗОЗ та обробки інформації **ЗОЗ** .

6. Користувачі несуть відповідальність за видалення з пристрою всього програмного забезпечення та інформації, наданої **ЗОЗ** .

7. Системні адміністратори несуть відповідальність за блокування всіх облікових записів користувачів у день припинення відносин.

2.3 Вимоги до безпеки для пристроїв BYOD

1. Від співробітників **ЗОЗ** очікується, що вони використовуватимуть свої особисті пристрої етично в будь-який час і дотримуватимуться правил і норм інформаційної безпеки **ЗОЗ** , зокрема тих, що викладені в цій Політиці.

2. Користувачі несуть відповідальність за забезпечення того, щоб жодна інша особа (включаючи членів родини та друзів) не мала доступу до особистого пристрою, що використовується для роботи (навіть якщо ці користувачі мають окремі облікові записи).

3. Користувачі несуть відповідальність за забезпечення того, щоб їхні особисті пристрої, що використовуються для роботи, відповідали наступним вимогам інформаційної безпеки:

а) пристрій повинен працювати під управлінням ліцензійної та актуальної версії авторизованої операційної системи (OS) відповідно до Переліку стандартного програмного забезпечення;

б) пристрій повинен бути захищений засобами безпечного механізму аутентифікації, за потреби. Паролі, що використовуються для захисту особистих пристроїв, які використовуються для роботи, повинні відповідати вимогам, викладеним у Політиці паролів;

в) пристрій повинен підтримувати та мати увімкнене повне шифрування диска;

г) пристрій повинен бути налаштований на автоматичне блокування, коли він неактивний більше п’яти (5) хвилин;

д) на пристрої повинна бути встановлена система захисту від шкідливих програм;

е) на пристрої повинні бути ліцензовані та підтримувані версії додатків з останніми доступними оновленнями та патчами. Користувачі нестимуть особисту відповідальність за будь-які наслідки (включаючи юридичну

відповідальність) у зв'язку з використанням неліцензованого програмного забезпечення;

є) на пристрої не повинно бути жодного забороненого, неліцензованого, шкідливого або будь-якого іншого програмного забезпечення чи контенту, який може загрожувати конфіденційності або публічному іміджу **ЗОЗ** (наприклад, торрент-клієнти, відеоігри тощо).

4. Зберігання внутрішньої та конфіденційної інформації **ЗОЗ** на особистих пристроях, що використовуються для роботи, не рекомендується і повинно бути уникнено, коли це можливо. Користувачі повинні зберігати будь-яку робочу інформацію в корпоративних інформаційних системах (наприклад, корпоративний SharePoint, Confluence) або на мережевих ресурсах, схвалених **ЗОЗ**.

5. Якщо користувач вважає, що особистий пристрій, що використовується для роботи, може бути інфіковано вірусом, трояном, шкідливим програмним забезпеченням або будь-якою іншою загрозою, він/вона повинен/повинна негайно повідомити Системних адміністраторів про можливий інцидент інформаційної безпеки.

6. Якщо користувач втрачає або ненавмисно залишає особистий пристрій, що використовується для роботи, він/вона повинен/повинна негайно повідомити Системних адміністраторів про можливий інцидент інформаційної безпеки.

Додаток А.3

Політика «чистого робочого столу та екрану» –
Clear Desk and Clear Screen Policy (CDCS)

1. Огляд

1.1 Вступ

Політика чистого столу та чистого екрану (далі - "Політика") спрямована на забезпечення того, щоб вся конфіденційна інформація була видалена з робочих місць та заблокована, коли предмети не використовуються або коли користувачі залишають свої робочі місця.

1.2 Мета

Мета цієї Політики полягає у встановленні мінімальних вимог для підтримки чистоти столів та екранів, а також у забезпеченні того, щоб конфіденційна інформація ЗОЗ **ЗОЗ** була заблокована та не потрапляла в поле зору, коли не використовується.

1.3 Відповідальність

Співробітники та підрядники ЗОЗ - відповідають за дотримання правил, встановлених у цій Політиці, під час роботи з конфіденційною інформацією.

Системні адміністратори - відповідають за впровадження технічних засобів безпеки, необхідних відповідно до цієї Політики.

2. Положення політики

2.1 Правила чистого столу

1. Користувачі зобов'язані забезпечити, щоб вся конфіденційна інформація в паперовій або електронній формі була в безпеці в їхньому робочому просторі в кінці робочого дня та коли вони планують залишити своє робоче місце на тривалий час.

2. Робоче місце користувача повинно містити лише документи, необхідні для роботи в даний момент. В інший час робочі документи слід зберігати в

спеціально відведеному місці. В кінці робочого дня необхідно прибрати всі зайві предмети з робочого місця, а також документи, що містять конфіденційну інформацію.

3. По можливості паперові та комп'ютерні носії, такі як USB-накопичувачі, мобільні телефони та планшети, що містять конфіденційну інформацію, повинні бути прибрані зі столу та зберігатися в підходящих закритих сейфах, шафах або іншій меблі, коли не використовуються, особливо поза робочими годинами.

4. Серверні кімнати та робочі приміщення повинні залишатися закритими, якщо їх залишили без нагляду.

5. Зона рецепції може бути особливо вразливою для відвідувачів. Ця зона повинна бути якомога чистішою в будь-який час. Ніяка конфіденційна інформація не повинна зберігатися на столах, які можуть бути в межах досяжності або видимості відвідувачів.

6. Ключі для доступу до конфіденційної інформації не повинні залишатися на незайнятому столі.

7. Обладнання та носії, що вивезені за межі підприємства, не повинні залишатися без нагляду в громадських місцях.

8. Паролі не повинні бути написані та зберігатися в доступному місці.

9. Усі принтери повинні бути очищені від паперів відразу після їх друку; надруковані документи, що містять конфіденційну інформацію, повинні бути негайно прибрані з принтера. Це допомагає забезпечити, щоб чутливі документи не залишалися в лотках принтера для неналежної особи.

10. При утилізації чутливі документи повинні бути знищені в шредерах.

11. Конфіденційна інформація не повинна залишатися в загальних конференц-залах або кімнатах для зустрічей.

12. Після кожної зустрічі біла дошка, що містить конфіденційну інформацію, повинна бути стерта.

13. Потрібно забезпечити безпеку всіх офісних приміщень, коли вони не використовуються. Потрібна процедура "остання особа виходить", щоб кожен

розумів свої обов'язки щодо закриття дверей, закриття вікон та налаштування охоронних сигналізацій.

2.2 Правила чистого екрану

1. Користувачі зобов'язані забезпечити, щоб комп'ютерні робочі місця та мобільні пристрої були заблоковані, коли робоче місце не зайняте. Користувачі повинні виходити з системи або блокувати свої машини, коли покидають кімнату.

2. Користувачі повинні завжди враховувати видимість дисплея на своєму робочому місці. Скільки можливо, слід забезпечити, щоб екран не був видимий для неавторизованих осіб під час використання.

3. Користувачі зобов'язані блокувати свій екран, коли залишають комп'ютер без нагляду.

4. Автоматичне блокування екрана повинно бути активоване, змушуючи дисплей блокуватися через п'ять (5) хвилин бездіяльності. Робоча станція повинна бути захищена паролем для повторної активації.

5. Користувачі зобов'язані забезпечити, щоб їхні комп'ютери були вимкнені та заблоковані в безпечному місці в кінці робочого дня.

6. Користувачі завжди повинні бути в курсі, коли отримують доступ до конфіденційної інформації, чи можуть інші бачити інформацію, що відображається на їхньому екрані.

7. Екрани комп'ютерів повинні бути нахилені так, щоб не бути видимими неавторизованими особами. Це може включати зовнішні та внутрішні вікна та головні двері. Це особливо важливо при використанні ноутбука в громадському місці.

8. У разі використання публічного ПК/ноутбука для зустрічі, семінару чи презентації після завершення користувачі повинні переконатися, що дані повністю видалені з цього ПК/ноутбука, включаючи кошик.

9. Правила чистого столу та чистого екрану, викладені в цій Політиці, також застосовуються до дистанційної роботи та використання активів **ЗОЗ** за межами підприємства.

Додаток А.4

Політика шифрування – Encryption Policy

1. Огляд

1.1 Вступ

Шифрування перетворює інформацію в іншу форму або код, так що тільки особи з доступом до секретного ключа (офіційно називаного ключем дешифрування) або пароля можуть її прочитати. Наразі шифрування є одним з найпопулярніших і найефективніших методів інформаційної безпеки, які використовуються організаціями. Метою шифрування є захист конфіденційності цифрової інформації під час її зберігання на комп'ютерних системах та передачі через Інтернет або інші комп'ютерні мережі.

1.2 Мета

Метою цієї Політики є встановлення вимог до застосування шифрування до інформації та обладнання як засобу захисту конфіденційності та цілісності інформації **ЗОЗ**.

1.3 Обов'язки

Співробітники та підрядники **ЗОЗ**: - відповідають за впровадження криптографічних контролів на своїх особистих пристроях.

Системні адміністратори - відповідають за налаштування та впровадження технологій та протоколів шифрування

2. Положення політики

2.1 Загальні положення

1. Для зменшення ризику розкриття або підробки конфіденційної інформації **ЗОЗ** через перехоплення, втрату або крадіжку інформації або обладнання, **ЗОЗ**, а також його співробітники та підрядники повинні впроваджувати відповідні криптографічні засоби безпеки у поєднанні з процедурами, які керують відповідними ключами шифрування.

2. Для шифрування інформації в спокої та в русі повинні використовуватися загальноприйняті міжнародні стандарти та алгоритми шифрування.

2.2 Інформація

1. Внутрішня та конфіденційна інформація **ЗОЗ** повинні, бажано, створюватися та зберігатися в авторизованих інформаційних системах, які управляються компанією.

2. Однак, коли така інформація передається за межі авторизованої системи, вона повинна бути зашифрована під час передачі.

3. Шифрування під час передачі може включати шифрування файлу, надісланого електронною поштою, шифрування портативного жорсткого диска, що використовується для передачі інформації, або використання зашифрованих протоколів передачі, таких як TLS.

4. Всі бездротові точки доступу повинні бути налаштовані з використанням потужного шифрування (□ES WP□2 щонайменше) для аутентифікації та передачі перед авторизацією їх використання.

2.3 Пристрої

2.3.1 Пристрої, що належать організації

1. Де це вважається доцільним, і пристрій здатний до шифрування пристроїв, застосування шифрування є обов'язковим. Може бути проведено оцінку ризиків для оцінки ризиків, пов'язаних з використанням активу, та ухвалення рішення щодо застосовності криптографічного захисту.

2. Всі робочі станції, що використовуються співробітниками та підрядниками **ЗОЗ** (включаючи BYOD-пристрої), повинні бути зашифровані за допомогою повного шифрування диска. Користувачам не дозволяється вивозити свої робочі станції за межі офісних приміщень, якщо повне шифрування диска не включено та не реалізоване.

3. Якщо це застосовано і вимагається результатами оцінки ризиків, власники активів відповідають за забезпечення захисту активів, що

перебувають під їх відповідальністю, за допомогою шифрування, за необхідності.

4. Якщо потрібно, користувачі можуть подати запит на виключення з правил, що стосуються повного шифрування диска робочих станцій. Запит на виключення повинен бути надісланий СТО через корпоративну електронну пошту та містити чітке обґрунтування такого виключення. СТО повинен переглянути та ухвалити рішення щодо надання дозволу на запит. Дозвіл може бути наданий лише в письмовій формі через корпоративну електронну пошту.

2.3.2 Особисті пристрої

1. Персональні комп'ютери не завжди мають увімкнені функції безпеки, еквівалентні контрольованим робочим станціям ЗОЗ. Крім того, ними можуть користуватися кілька осіб, не всі з яких можуть бути працівниками ЗОЗ, і, ймовірно, вони можуть бути передані іншим членам сім'ї, продані приватно або утилізовані. Крім того, будучи портативними, вони підлягають ризику втрати або крадіжки. Як такі, ці пристрої становлять високий ризик для безпеки інформації, яку вони зберігають.

2. Коли можливо, користувачі не повинні створювати або зберігати будь-яку внутрішню або конфіденційну інформацію **ЗОЗ** на особистих пристроях (наприклад, ноутбуках, смартфонах тощо), включаючи використання інструментів синхронізації файлів. Несуттєва інформація не повинна зберігатися на пристрої, якщо копія також не зберігається в системі, що належить ЗОЗ.

3. **ЗОЗ** визнає, що певні програми, такі як електронна пошта або синхронізація файлів, можуть автоматично завантажувати інформацію без явної дії користувача, і тому, коли такі інструменти використовуються на особистих пристроях, тоді шифрування повинно бути застосовано. Крім того, користувач повинен забезпечити захист пристрою відповідно до політики **ЗОЗ**.

4. Користувач, що обробляє інформацію ЗОЗ, несе повну відповідальність за застосування відповідних контролів безпеки та за забезпечення безпеки інформації протягом її життєвого циклу.

5. Користувачі, що використовують авторизовані особисті пристрої для роботи (пристрої BYOD), несуть відповідальність за забезпечення безпечного видалення інформації **ЗОЗ** з пристрою перед його утилізацією.

2.3.3 Смартфони та планшети

1. Коли смартфони, планшети або інші розумні пристрої використовуються для роботи (незалежно від власності), рекомендується застосовувати шифрування на цих пристроях.

2.3.4 Інші пристрої

1. Особлива увага повинна бути приділена фізичній безпеці інших портативних пристроїв з меншими вбудованими функціями безпеки, таких як цифрові камери, зовнішні жорсткі диски, USB-накопичувачі та записуючі пристрої.

2. Якщо шифрування пристроїв доступне, воно повинно бути використане, а відповідні відновлювальні паролі або ключі повинні зберігатися на стороні ЗОЗ в безпеці.

3. Використання цих пристроїв для зберігання конфіденційної інформації слід уникати, де це можливо, але якщо їх потрібно використовувати для збору конфіденційної інформації, ця інформація не повинна зберігатися на пристрої довше мінімально необхідного часу для передачі цієї інформації в безпечне місце, таке як безпечний ноутбук або інформаційна система ЗОЗ.

4. Поки пристрій містить конфіденційну інформацію, ця інформація повинна бути захищена або за допомогою шифрування пристрою, або за допомогою шифрування файлів.

5. Усі записи конфіденційної інформації повинні бути безпечно видалені з пристрою негайно після успішної передачі, а пристрій слід утилізувати безпечно, коли він більше не потрібен ЗОЗ.

2.4 Інструменти синхронізації та обміну файлами

1. Користувачі не повинні наражати на ризик розкриття конфіденційність чутливої інформації або втрату критичної інформації **ЗОЗ** шляхом використання

незахищених інструментів і методів (такі як несанкціоновані програми та системи) і/або особистих електронних поштових рахунків.

2. Зокрема, користувачам не дозволяється зберігати внутрішню або конфіденційну інформацію в Інтернеті за допомогою особистих публічних сховищ (наприклад, особистий Google Drive, Dropbox тощо).

3. Якщо внутрішня або конфіденційна інформація повинна бути передана через незахищені зовнішні системи або служби, для захисту інформації слід розглянути шифрування на рівні файлу. Ключі, паролі або інші секрети повинні бути передані **ЗОЗ** безпечними засобами, щоб **ЗОЗ** змогла відновити інформацію за потреби.

2.5 Вимоги до управління криптографічними ключами

1. Якщо криптографічні ключі управляються з боку **ЗОЗ**, для захисту криптографічних ключів повинні бути впроваджені спеціальні контролі безпеки.

2. Криптографічні алгоритми, довжини ключів та практики використання повинні обиратися відповідно до найкращих практик.

3. Криптографічні ключі повинні бути захищені від модифікацій та втрати. Секретні та приватні ключі повинні бути захищені від несанкціонованого використання, а також розкриття. Для зберігання ключів шифрування настійно рекомендується використовувати сейфи.

4. Генерація ключів повинна базуватися на стандартному генераторі випадкових чисел (RNG).

5. Ключі шифрування повинні бути змінені не рідше одного разу протягом 3-річного періоду.

6. Криптографічні ключі повинні бути захищені так, щоб тільки авторизовані користувачі та програми могли отримати доступ до ключів.

7. Якщо це застосовано, використання криптографічних ключів повинно бути зафіксовано, щоб забезпечити аудиторський слід.

8. Втрата, крадіжка або потенційне несанкціоноване розкриття ключа шифрування повинні бути негайно повідомлені системним адміністраторам, які повинні вжити заходів для відкликання/деактивації ключів за потреби.

Додаток А.5

Політика класифікації інформації – Information Classification Policy

Огляд

1.1 Вступ

Інформація є стратегічно важливим активом ЗОЗ **ЗОЗ** та її клієнтів. Усі співробітники та підрядники **ЗОЗ** несуть відповідальність за захист конфіденційності, цілісності та доступності інформації **ЗОЗ** та клієнтів, яка створюється, обробляється, модифікується, передається, зберігається або знищується, незалежно від носія, на якому ця інформація зберігається, і незалежно від її формату (наприклад, електронний, паперовий або інші фізичні форми).

1.2 Мета

Метою цієї Політики є встановлення структури для класифікації інформації на основі її чутливості, цінності та важливості для організації, щоб інформація **ЗОЗ** та клієнтів могла бути належним чином захищена.

1.3Відповідальність

Співробітники та підрядники **ЗОЗ**:

Відповідають за дотримання правил цієї Політики та інших підтримуючих політик інформаційної безпеки **ЗОЗ** під час роботи з інформацією та інформаційними активами **ЗОЗ**.

Власники активів/документів:

- Забезпечують належну класифікацію та захист активів і документованої інформації.
- Визначають та періодично переглядають обмеження доступу та класифікацію активів і документованої інформації, що перебувають у їхньому володінні.

Команда з інформаційної безпеки:

•Періодично контролює дотримання цієї Політики.

2. Положення політики

2.1 **Класифікація інформації**

1. Інформація **ЗОЗ** має бути класифікована з урахуванням робочих потреб щодо обміну або обмеження інформації, а також юридичних вимог.

2. Інформація, що належить, створюється, обробляється, зберігається або знищується **ЗОЗ**, може бути класифікована в одну з трьох категорій:

а) **Публічна** - інформація доступна загальній аудиторії, співробітникам і підрядникам **ЗОЗ**, клієнтам та партнерам через авторизовані канали. Публічна інформація не є чутливою за контекстом чи змістом і не вимагає спеціального захисту конфіденційності. Втрата доступності через простої системи є прийнятним ризиком. Цілісність важлива, але не критична;

б) **Внутрішня / Тільки для внутрішнього використання** - інформація доступна співробітникам **ЗОЗ** та іншим уповноваженим підрядникам, які потребують цієї інформації для виконання своїх функціональних обов'язків. Інформація цієї категорії не повинна розкриватися за межами **ЗОЗ** без дозволу. Її розкриття може негативно вплинути на продуктивність ЗОЗ та рівень наданих послуг або призвести до незначних фінансових втрат для співробітників або **ЗОЗ**. Збереження цілісності та доступності є важливим, але не критичним;

в) **Конфіденційна** - будь-які дані або власна інформація **ЗОЗ**, які не є загальновідомими або ще не були розкриті, незалежно від того, в матеріальній чи нематеріальній формі. Розкриття конфіденційної інформації обмежується в межах конкретного підрозділу/відділу **ЗОЗ** і не може бути розкрито за межами конкретних груп, уповноважених мати доступ до цієї інформації. Таке розкриття може завдати значної шкоди конкурентним перевагам, партнерству, відносинам і репутації. Конфіденційна інформація доступна лише особам, які виконують конкретні функції або ролі. Збереження цілісності, конфіденційності та обмеженої доступності є важливим. Дозвіл є обов'язковим для обміну конфіденційною інформацією.

3. Команда управління **ЗОЗ** несе відповідальність за класифікацію інформації.

4. Призначена мітка класифікації інформації та її пов'язаних активів повинні періодично переглядатися та оцінюватися для забезпечення їх адекватності. Результати класифікації повинні бути оновлені відповідно до змін у цінності, чутливості та критичності інформації протягом її життєвого циклу.

5. Оцінка призначеної мітки класифікації повинна проводитися відповідним власником активу в таких випадках:

а) за вказівкою Команди управління;

б) під час оновлення інформації про актив в інвентарі;

в) під час перегляду документованої інформації;

г) за ініціативою власника активу.

2.2 Маркування інформації

1. Конфіденційна інформація **ЗОЗ** повинна бути промаркована міткою «Конфіденційна». Маркування внутрішньої інформації є бажаним, але не обов'язковим.

2. Процес маркування застосовується лише до інформації в електронному вигляді. Зокрема, під час створення документів, особливо тих, які будуть розподілені клієнтам і партнерам (наприклад, внутрішні політики та процедури, пропозиції послуг, звіти тощо), слід використовувати корпоративні шаблони з попередньо визначеним форматом і мітками класифікації, коли це можливо.

3. Мітки класифікації повинні з’являтися в заголовку або в нижньому колонтитулі принаймні на першій сторінці документованої інформації; їх також можна додати на кожній наступній сторінці за бажанням.

4. Спливаючі банери, які з’являються під час входу в інформаційну систему, можуть бути використані, щоб зробити користувачів обізнаними про рівень класифікації інформації, до якої вони отримують доступ.

Додаток А.6

Політика інформаційної безпеки –
Information Security Policy

1. Огляд

1.1 Вступ

Інформація є найважливішим активом у всіх сучасних організаціях. Вона відіграє критичну роль у функціонуванні **ЗОЗ**, її співробітників та клієнтів. Тому ресурси **ЗОЗ**, включаючи інформацію, інформаційні системи, фізичні активи, мережі та обладнання, повинні бути належним чином захищені, щоб забезпечити збереження конфіденційності, цілісності, доступності інформації та безперервного функціонування операційних процедур.

Цей документ визначає Політику інформаційної безпеки ЗОЗ. **ЗОЗ** на рівні керівництва визнає необхідність забезпечення безперебійної роботи ЗОЗ на благо своїх клієнтів, акціонерів та інших зацікавлених сторін. Щоб забезпечити такий рівень безперервної роботи, **ЗОЗ** впровадила набір заходів інформаційної безпеки для вирішення своїх сприйнятих ризиків.

1.2 Мета

Метою цієї політики є встановлення основних вимог до інформаційної безпеки для функціонування **ЗОЗ** та опис системи управління інформаційною безпекою (ISMS), що була створена для виконання цих вимог.

1.3 Відповідальність

Команда інформаційної безпеки:

- Відповідальна за розробку цієї політики та створення умов для її реалізації;
- Відповідальна за координацію впровадження, документування та функціонування.

ISMS в межах ЗОЗ.

Команда управління:

- Відповідальна за забезпечення відповідності політик інформаційної безпеки та цілей інформаційної безпеки стратегічному напрямку ЗОЗ;
- Відповідальна за забезпечення наявності ресурсів, необхідних для ISMS;
- Відповідальна за регулярний перегляд ефективності ISMS, щоб гарантувати досягнення запланованих результатів ISMS;
- Відповідальна за керівництво та підтримку осіб, які сприяють ефективності ISMS та просувають постійне покращення.

Співробітники та підрядники **ЗОЗ**:

- Відповідальні за дотримання правил, викладених у цій політиці, а також у супутніх політиках та процедурах інформаційної безпеки.

2. Положення політики

2.1 Загальна інформація

1. **ЗОЗ** пропонує прозору службу, яка підбирає програмістів відповідно до специфічних потреб клієнтів, організовує операції команди, а потім передає право власності компаніям.

2. Політика інформаційної безпеки є невід'ємною частиною стратегії ЗОЗ, оскільки є ключовим фактором у якості надійного партнера.

2.2 Вимоги до інформаційної безпеки

1. Метою Політики інформаційної безпеки в **ЗОЗ** є забезпечення дотримання наступних вимог:

а) Інформація, яку клієнти надають **ЗОЗ**, використовується виключно для надання послуг, які вони замовили у ЗОЗ;

б) Конфіденційність, цілісність і доступність інформації, яку клієнти надають **ЗОЗ**, належним чином захищені;

в) Інформація, яку клієнти надають **ЗОЗ**, обробляється відповідно до застосовного міжнародного законодавства та регламентів;

г) Конфіденційність, цілісність і доступність усієї інформації, яка не є публічно доступною про **ЗОЗ** або яку вона володіє, належним чином захищені;

д) Співробітники та підрядники **ЗОЗ** дотримуються застосовного законодавства та регламентів у частині інформаційної безпеки;

е) Конфіденційність, цілісність і доступність інформації, що належить співробітникам та підрядникам **ЗОЗ**, належним чином захищені.

2. Щоб задовольнити вищезгадані вимоги, **ЗОЗ** впровадила та задокументувала **Систему управління інформаційною безпекою (ISMS)**, яка складається з набору політик, процедур, процесів та систем для управління ризиками для активів ЗОЗ з метою мінімізації ризику для щоденних операцій у всіх відповідних підрозділах.

3. ISMS **ЗОЗ** визначена з урахуванням внутрішніх і зовнішніх питань, а також вимог зацікавлених сторін, і створена відповідно до визнаного міжнародного стандарту ISO/IEC 27001:2013.

4. ISMS **ЗОЗ** затверджена Командою управління, відповідає стратегічному напрямку ЗОЗ, доведена до відома відповідних зацікавлених сторін, адекватно забезпечена ресурсами та відповідає чинному законодавству, регламентам та іншим вимогам.

5. ISMS **ЗОЗ** оновлюється щонайменше раз на рік або в разі суттєвих змін в оточенні.

2.3 Покращення інформаційної безпеки

1. Політика ЗОЗ щодо постійного покращення полягає в тому, щоб:

а) Постійно покращувати ефективність заходів інформаційної безпеки;

б) Збільшити рівень проактивності щодо інформаційної безпеки в межах ЗОЗ;

в) Зробити процеси та заходи інформаційної безпеки більш вимірювальними, щоб надати надійну основу для обґрунтованих рішень;

г) Отримувати ідеї для покращення через регулярні зустрічі та інші форми комунікації з зацікавленими сторонами;

д) Переглядати ідеї для покращення на регулярних управлінських зустрічах для пріоритизації та оцінки термінів і вигод.

2. ISMS **ЗОЗ** активно контролюється, переглядається та оновлюється, щоб забезпечити виконання цілей ISMS.

3. **ЗОЗ** проводить незалежні аудити ISMS щонайменше раз на рік, щоб визначити його продовжувальну придатність, адекватність та ефективність.

4. **ЗОЗ** постійно покращує ефективність ISMS через регулярний перегляд політик та процедур інформаційної безпеки, вимірювання та аналіз цілей інформаційної безпеки, результати аудитів, аналіз контрольованих подій, коригувальні та запобіжні дії, а також управлінський перегляд.

2.4 Області політики інформаційної безпеки

1. **ЗОЗ** визначає стратегію інформаційної безпеки в різноманітних сферах, пов'язаних з інформаційною безпекою, які детально описані в комплексному наборі документації, що супроводжує цю загальну Політику інформаційної безпеки.

2. ISMS **ЗОЗ** вимагає впровадження заходів безпеки в наступних областях:

2.1 Політика безпеки;

2.2 Організація інформаційної безпеки;

2.3 Безпека людських ресурсів;

2.4 Контроль доступу;

2.5 Криптографія;

2.6 Фізична та екологічна безпека;

2.7 Безпека комунікацій;

2.8 Придбання, розробка та обслуговування інформаційних систем;

2.9 Управління інцидентами інформаційної безпеки;

2.10 Управління безперервністю роботи;

2.11 Відповідність.

3. Кожна з політик інформаційної безпеки ЗОЗ визначається та узгоджується однією або кількома особами з компетенцією в цій сфері та, після формального затвердження, доводиться до відома відповідної аудиторії, як внутрішньо, так і зовні ЗОЗ.

Додаток А.7

Політика використання інтернету та електронної пошти – Internet and Email Usage Policy

1. Огляд

1.1 Вступ

Інтернет і електронна пошта широко використовуються в майже всіх галузях і є основними інформаційними та комунікаційними ресурсами в ЗОЗ. Водночас неналежне використання Інтернету та електронної пошти може спричинити численні юридичні, приватні та безпекові ризики, тому важливо, щоб користувачі розуміли правильне використання Інтернету та електронних комунікацій.

1.2 Мета

Метою цієї Політики є забезпечення належного використання Інтернету та електронної пошти та ознайомлення користувачів з тим, що компанія **ЗОЗ** вважає прийнятним і неприпустимим при використанні Інтернету та електронної пошти.

1.3 Обов'язки

Співробітники та підрядники **ЗОЗ**:

• Відповідальні за дотримання правил цієї Політики та інших супутніх політик інформаційної безпеки під час роботи з інформацією ЗОЗ та інформаційними активами.

• Відповідальні за вживання обґрунтованих заходів щодо належного використання інформації, засобів обробки інформації, електронних пристроїв та мережевих ресурсів відповідно до політик та процедур **ЗОЗ**, а також місцевих законів і норм.

2. Положення політики

2.1 Використання Інтернету

1. Всі користувачі повинні використовувати Інтернет відповідально та продуктивно; як ресурс для виконання своїх обов’язків і підтримки цілей ЗОЗ.

2. Надмірне особисте використання Інтернету ЗОЗ під час робочих годин не дозволяється, проте разове та розумне особисте використання є прийнятним, якщо:

а) легковажне використання Інтернету не заважає продуктивності користувача, включаючи якість виконаної роботи та інші показники ефективності;

б) особисте використання Інтернету не порушує жодних інших правил, зазначених у цьому документі;

в) особисте використання не завдає надмірних негативних наслідків для корпоративної мережі шляхом споживання надмірної кількості обмеженої доступної пропускної здатності. Прикладами є, але не обмежуються, завантаженням/вивантаженням непропорційно великих файлів та переглядом високоякісних потокових відео;

г) користувачі не використовують майно ЗОЗ для виконання комерційних послуг поза завданнями та проектами, призначеними компанією.

3. Доступ до Інтернету в **ЗОЗ** має надаватися через спеціалізовані мережі. Кабельне з’єднання повинно використовуватися лише корпоративними пристроями. Корпоративна Wi-Fi мережа може використовуватися як корпоративними, так і особистими пристроями співробітників.

4. **ЗОЗ** залишає за собою право контролювати Інтернет-трафік і моніторити та отримувати доступ до даних, що складаються, надсилаються або отримуються через її онлайн-з'єднання.

5. При використанні веб-браузерів слід дотримуватися таких правил:

а) для перегляду Інтернету слід використовувати лише авторизовані браузери;

б) заборонено використовувати профілі браузерів (профіль Chrome, профіль Edge, профіль Firefox тощо), зареєстровані з особистою електронною адресою для робочих цілей; тільки профілі браузера, прив'язані до електронної

адреси **ЗОЗ**, можуть використовуватися на робочих станціях користувачів для виконання робочих обов’язків. Окремі профілі браузера, прив’язані до особистої електронної адреси, можуть використовуватися користувачами для особистого використання на робочих станціях.

6. Всі сайти та завантаження можуть контролюватися та/або блокуватися **ЗОЗ**, якщо вони вважаються шкідливими та/або непродуктивними для роботи.

7. Користувачі повинні бути обережними при завантаженні файлів з Інтернету. Коли це можливо, слід використовувати лише надійні джерела та веб-сайти для завантаження файлів. Де це можливо, рекомендується сканувати файли, завантажені з Інтернету, на наявність шкідливих програм за допомогою програмного забезпечення для захисту від шкідливих програм. Під час сканування файлів на наявність шкідливих програм програмне забезпечення повинно бути оновлено до останньої версії. Якщо в завантажених файлах виявлено шкідливий код, користувач повинен видалити його та негайно повідомити системних адміністраторів у разі зараження.

8. Використання будь-яких несанкціонованих зовнішніх публічних служб для виконання робочих завдань повинно бути заздалегідь затверджене менеджером користувача та командою системного адміністрування відповідно до Процедури встановлення програмного забезпечення. Приклади таких служб включають програми миттєвих повідомлень, соціальні мережі, служби обміну файлами тощо.

9. Користувачі повинні вести себе професійно, відповідально та етично під час спілкування через усі канали з клієнтами, партнерами, постачальниками або іншими співробітниками **ЗОЗ**, незалежно від того, чи йдеться про робочі чи не робочі чати, канали та групи.

10. Неприпустиме використання Інтернету користувачами включає, але не обмежується:

10.1 доступом до інформації **ЗОЗ**, яка не є в межах обов'язків користувача. Це включає несанкціоноване читання інформації про облікові записи клієнтів,

несанкціонований доступ до інформації файлів інших користувачів і доступ до інформації, яка не потрібна для належного виконання службових функцій;

10.2 створенням, публікацією, передаванням або добровільним отриманням будь-якого незаконного, образливого, наклепницького, загрозливого, переслідувального матеріалу, включаючи, але не обмежуючись, коментарями, заснованими на расі, національному походженні, статі, сексуальній орієнтації, віці, інвалідності, релігії чи політичних переконаннях;

10.3 використанням комп'ютерів для вчинення будь-яких форм шахрайства та/або піратства програмного забезпечення, фільмів або музики;

10.4 крадіжкою, використанням або розкриттям пароля без дозволу;

10.5 завантаженням, копіюванням або піратством програмного забезпечення та електронних файлів, що є авторським правом або без дозволу, включаючи використання Torrent-клієнтів;

10.6 завантаженням файлів з неперевірених джерел;

10.7 розподілом внутрішньої або конфіденційної інформації **ЗОЗ**, комерційних таємниць або власної інформації за межами ЗОЗ;

10.8 використанням, передаванням, дублюванням або добровільним отриманням матеріалів, які порушують авторські права, торговельні марки, комерційні таємниці чи патентні права будь-якої особи або ЗОЗ;

10.9 створенням особистих профілів або використанням особистих адрес електронної пошти для роботи, що може спричинити несанкціоновану передачу конфіденційної інформації або порушення захисту конфіденційності **ЗОЗ**;

10.10 відвідуванням сайтів або завантаженням інформації, яка не є необхідною для виконання службових обов'язків;

10.11 відвідуванням сайтів, які містять небезпечні матеріали, такі як порнографія, расизм, насильство чи екстремізм, або участю в обговореннях на ці теми;

10.12 здійсненням дій, які можуть спричинити фізичні або юридичні наслідки для **ЗОЗ** або її співробітників.

2.2 Використання електронної пошти

1. Користувачі повинні використовувати електронну пошту відповідально та в межах виконання своїх обов'язків.

2. Неприпустиме використання електронної пошти користувачами включає, але не обмежується:

а) створенням, публікацією, передаванням або добровільним отриманням будь-якого незаконного, образливого, наклепницького, загрозливого, переслідувального матеріалу, включаючи, але не обмежуючись, коментарями, заснованими на расі, національному походженні, статі, сексуальній орієнтації, віці, інвалідності, релігії чи політичних переконаннях;

б) використанням електронної пошти для розсилки небажаних комерційних повідомлень (спаму);

в) використанням електронної пошти для обговорення політичних або релігійних питань;

г) використанням електронної пошти для обговорення особистих фінансів, політики, сімейних чи особистих проблем;

д) використанням електронної пошти для обміну особистими зображеннями або матеріалами, що не стосуються робочих питань;

е) пересиланням електронних листів, що містять особисту інформацію про співробітників або клієнтів, без їх явної згоди;

є) використанням електронної пошти для обміну інформацією, що містить конфіденційні дані або комерційні таємниці **ЗОЗ**;

ж) використанням особистих електронних поштових скриньок для робочих повідомлень;

з) використанням електронної пошти для обговорення або розповсюдження особистої інформації, яка є небезпечною для ЗОЗ або її співробітників.

3. Всі електронні листи, надіслані з корпоративних облікових записів, є власністю **ЗОЗ** і можуть бути перевірені.

4. Користувачі повинні використовувати шаблони електронних листів, розроблені **ЗОЗ**, для підтримки професійності та однозначності комунікацій.

5. Всі електронні листи, що містять конфіденційну інформацію, повинні містити відповідні попередження про конфіденційність та безпеку, якщо це необхідно.

6. Користувачі не повинні відкривати електронні листи або вкладення з невідомих або ненадійних джерел. Якщо є сумніви, рекомендується звернутися до відділу інформаційних технологій для перевірки.

7. Всі корпоративні електронні листи повинні мати професійний тон і стиль, що відповідає стандартам **ЗОЗ**, і містити правильні дані про відправника та отримувача.

2.3 Покарання за порушення

1. Неправильне використання Інтернету та електронної пошти може призвести до дисциплінарних дій, які можуть включати, але не обмежуються, письмовим зауваженням, звільненням або кримінальним переслідуванням.

2. Кожен випадок буде розглядатися індивідуально, з урахуванням важливості порушення, історії роботи та обставин, що призвели до порушення.

3. Прикінцеві положення

1. Ця Політика підлягає перегляду щорічно або за потреби в будь-який час.

2. Кожен співробітник **ЗОЗ** зобов'язується дотримуватися цієї Політики, і її недотримання може мати серйозні наслідки.

Додаток А.8

Політика захисту від шкідливих програм – Malware Protection Policy

1. Огляд

1.1 Вступ

Зараження шкідливим програмним забезпеченням є витратною для **ЗОЗ** і часто займає багато часу для осіб. Це може проявлятися у втраті інформації або доступу до ІТ-систем, витратах часу співробітників на відновлення уражених систем або затримках чи втраті важливої роботи. Крім того, шкідливе програмне забезпечення може поширюватися з зараженої системи, що може призвести до серйозних збоїв у наданні послуг, можливих репутаційних збитків або навіть штрафів.

Шкідливе програмне забезпечення є постійно еволюціонуючою загрозою, тому **ЗОЗ** застосовує контроль для захисту інформації та її супутніх активів від усіх форм шкідливого ПЗ.

Контроль проти шкідливого програмного забезпечення повинні базуватися на програмному забезпеченні для захисту від шкідливого ПЗ, обізнаності щодо інформаційної безпеки, а також відповідних контролях доступу до системи та управлінні змінами.

1.2 Мета

Метою цієї Політики є сприяння використанню програмного забезпечення для захисту від шкідливого ПЗ та навчання користувачів правилам, які широко дотримуються для захисту від різних типів шкідливого програмного забезпечення.

1.3 Відповідальність

Співробітники та підрядники **ЗОЗ**:

• Відповідають за оновлення операційної системи, встановлених програм і програмного забезпечення для захисту від шкідливого ПЗ відповідно до останніх оновлень і патчів;

• Відповідають за повідомлення про підозри на зараження шкідливим програмним забезпеченням системним адміністраторам;

Системні адміністратори:

• Відповідають за встановлення, налаштування та обслуговування програмного забезпечення для захисту від шкідливого ПЗ на корпоративних робочих станціях та компонентах інфраструктури, за потреби.

2. Положення політики

2.1 Загальні положення

1. **ЗОЗ** повинна забезпечити, щоб її інформація та інформаційні системи були захищені та не підлягали неналежному використанню. Ця Політика встановлює відповідальність усіх користувачів, включаючи користувачів персональних та BYOD пристроїв, що підключаються до об'єктів **ЗОЗ**, щодо шкідливого програмного забезпечення. Ці заходи не гарантують безпеки, але вони допоможуть значно зменшити ризик поширення шкідливого ПЗ в **ЗОЗ**.

2. Слово "шкідливе ПЗ" (malware), скорочення від "шкідливе програмне забезпечення", використовується колективно для позначення багатьох типів програмного забезпечення, включаючи віруси, програмне забезпечення-вимагачі, черв'яки, трояни, макроси, "поштові бомби", руткіти та інші шкідливі комп'ютерні програми, які хакери використовують для завдання шкоди та отримання доступу до чутливої інформації. Шкідливе ПЗ є загальним терміном для позначення будь-якого програмного забезпечення, призначеного для завдання шкоди окремому комп'ютеру, серверу або комп'ютерній мережі.

3. Існує багато потенційних джерел шкідливого програмного забезпечення, включаючи веб-сайти, соціальні мережі, USB-накопичувачі, електронну пошту, а також програмне забезпечення або документи, скопійовані через мережі або Інтернет.

2.2 Контролі проти шкідливого ПЗ

1. Робочі станції **ЗОЗ**, корпоративні мобільні пристрої, BYOD-пристрої та сервери, які підключені до мережі **ЗОЗ** або інакше використовують інформаційні системи **ЗОЗ**, повинні працювати з авторизованим та актуальним програмним забезпеченням для захисту від шкідливого ПЗ, яке безперервно контролює наявність шкідливого програмного забезпечення, за потреби.

2. Якщо виникає потреба у використанні програмного забезпечення для захисту від шкідливого ПЗ, яке не входить до списку рекомендованих програм, його використання повинно бути погоджено зі системними адміністраторами.

3. Програмне забезпечення для захисту від шкідливого ПЗ повинно сканувати комп'ютери, сервери, носії та інші пристрої як запобіжний захід або на регулярній основі.

4. Робочі станції, корпоративні мобільні пристрої, BYOD-пристрої та сервери, підключені до мережі **ЗОЗ** або інакше використовують інформаційні системи **ЗОЗ**, повинні працювати з авторизованою та підтримуваною версією операційної системи та встановлених програм із застосуванням останніх доступних оновлень та патчів.

5. Персональні пристрої, що використовуються для віддаленого підключення до корпоративної мережі через VPN/RDP сесію, повинні мати встановлене та активоване відповідне програмне забезпечення для захисту від шкідливого ПЗ, завантажене з надійного джерела.

6. Програмне забезпечення для захисту від шкідливого ПЗ повинно бути налаштоване на сканування при доступі, включаючи завантаження або відкриття файлів, папок на знімних або віддалених носіях, сканування вкладень електронної пошти перед доставкою та сканування веб-сторінок.

7. Програмне забезпечення для захисту від шкідливого ПЗ повинно регулярно оновлюватися. Оновлення програмного забезпечення для захисту від шкідливого ПЗ повинні виконуватися щойно оновлення для певного продукту стають доступними. У разі невдач автоматичного оновлення програмного

забезпечення для захисту від шкідливого ПЗ, оновлення повинно виконуватися вручну.

8. Програмне забезпечення для захисту від шкідливого ПЗ повинно бути налаштоване на виконання регулярних (принаймні раз на кілька днів) швидких сканувань.

9. Користувачі повинні бути позбавлені доступу до відомих шкідливих веб-сайтів або за допомогою програмного забезпечення для захисту від шкідливого ПЗ, або через функцію фільтрації контенту.

10. Особливу увагу слід звертати на файли та програмне забезпечення, отримані з зовнішніх мереж або через будь-який інший носій. Користувачі несуть відповідальність за забезпечення того, щоб їх знімні носії були вільні від будь-якого шкідливого програмного забезпечення. Якщо це застосовано, знімні носії повинні бути перевірені програмним забезпеченням для захисту від шкідливого ПЗ перед їх використанням.

11. Заборонено (за винятком крайніх випадків уповільнення комп'ютера) відключати або видаляти програмне забезпечення для захисту від шкідливого ПЗ. Будь-які повідомлення, які свідчать про те, що захист від шкідливого ПЗ був вимкнений, повинні бути повідомлені системним адміністраторам і терміново розслідувані. Якщо необхідно тимчасово вимкнути програмне забезпечення для захисту від шкідливого ПЗ, користувач повинен отримати дозвіл від інженера з комп’ютерних технологій.

12. Якщо користувачі зіткнулися з труднощами з рекомендованим програмним забезпеченням для захисту від шкідливого ПЗ, запити на технічну підтримку можуть бути зроблені до системних адміністраторів.

13. **ЗОЗ** забороняє будь-яку діяльність, спрямовану на створення та/або розповсюдження шкідливого коду (наприклад, вірусів, черв'яків тощо) в корпоративній мережі або інформаційних системах. Однак, якщо це потрібно за вимогою системних адміністраторів Команди інформаційної безпеки для сприяння розслідуванням, користувачі можуть надсилати підозрюване шкідливе ПЗ за допомогою методу, який не дозволяє шкідливому ПЗ розповсюджуватися.

14. **ЗОЗ** залишає за собою право відключити будь-який пристрій від мережі, якщо буде виявлено чи підозрюється на зараження. Пристрій буде відключено до видалення зараження та встановлення відповідних профілактичних інструментів на пристрій.

15. Якщо користувачі підозрюють, що пристрій заражено шкідливим програмним забезпеченням, вони повинні якомога швидше повідомити про інцидент системним адміністраторам.

Додаток А.9

Політика захисту в мережі –
Network Security Policy

1. Огляд

1.1 Вступ

Політика безпеки мережі забезпечує захист цінної інформації від випадкового або ненавмисного розкриття, а також несанкціонованих змін у мережі.

1.2 Мета

Мета цієї Політики — встановити правила та принципи управління мережею, щоб запобігти несанкціонованому доступу до мережі та активів **ЗОЗ** і потенційній втраті конфіденційної інформації.

1.3 Відповідальність

Адміністратори систем:

• Відповідають за управління компонентами мережі **ЗОЗ**;

• Відповідають за впровадження контролю безпеки мережі.

2. Положення політики

2.1 Загальні положення

1. Мережа **ЗОЗ** повинна управлятися та контролюватися для захисту інформації в системах і додатках.

2. Мережа **ЗОЗ** є невід'ємною частиною загальної інфраструктури ЗОЗ та призначена для передачі інформації в внутрішній мережі, надання доступу користувачів до зовнішніх мереж і забезпечення доступу користувачів та клієнтів до відповідних активів **ЗОЗ**.

3. Мережа **ЗОЗ** складається з наступних компонентів:

а) телекомунікаційна інфраструктура (структурована кабельна система);

б) мережеве обладнання:

I. Комутатори;

II. Маршрутизатори;

III. Точки доступу Wi-Fi.

в) служби;

I. DNS;

II. DHCP;

III. VPN-сервер (тільки для IT-відділу).

г) робочі станції з мережевими адаптерами.

4. Ризики інформаційної безпеки та контролю для зазначених компонентів мережі **ЗОЗ** описані в Реєстрі ризиків **ЗОЗ**.

5. Значні зміни та переналаштування в мережі з технологічних причин здійснюються відповідно до Політики управління змінами.

2.2 Вимоги до безпеки мережі та контролі

1. Доступ до мережі **ЗОЗ** надається через захищене з'єднання мережевих клієнтів (робочих станцій, мобільних пристроїв тощо) і серверів до локальної мережі або віддаленого доступу.

2. Місцевий доступ до мережі **ЗОЗ** надається або за допомогою кабельного Ethernet-з'єднання, або бездротового з'єднання.

3. Користувачі, які використовують віддалене з'єднання для доступу до мережі **ЗОЗ**, повинні забезпечити, щоб:

а) пристрої, підключені до мережі **ЗОЗ**, працювали на авторизованій та підтримуваній версії операційної системи та встановлених додатків з останніми доступними оновленнями та патчами;

б) програмне забезпечення для захисту від шкідливих програм від авторитетного джерела було встановлено та працювало на пристроях, підключених до мережі **ЗОЗ** відповідно до Політики захисту від шкідливих програм;

в) на пристроях, підключених до мережі **ЗОЗ**, не було встановлено та запущено жодного шкідливого або потенційно шкідливого програмного забезпечення (наприклад, клієнтів Torrent);

4. У всіх користувачів повинна бути активована брандмауер на їхніх робочих станціях (включаючи BYOD-пристрої).

5. Користувачам заборонено використовувати програми безпеки або утиліти, які виявляють слабкості в безпеці системи (наприклад, програми для злому, пакетні аналізатори, інструменти для картографування мережі або сканери портів), підключаючись будь-яким чином до мережі **ЗОЗ**, за винятком випадків, коли використання таких систем авторизовано та обґрунтоване оперативними потребами.

6. Захист мережі **ЗОЗ** реалізується на основі таких запобіжних заходів:

а) брандмауер маршрутизатора є єдиною точкою входу та виходу з мережі **ЗОЗ** до Інтернету;

б) VPN-з'єднання можуть використовуватися працівниками для віддаленого доступу до мереж клієнтів;

в) системна документація, яка описує топологію, конфігурацію та принципи роботи мережі ЗОЗ, є закритою та захищена від несанкціонованого доступу;

г) доступ до конфігурації мережевого обладнання обмежується відповідно до принципу “найменших прав” і надається тільки адміністраторам систем;

д) доступ до компонентів мережі **ЗОЗ** контролюється через механізм захищеної аутентифікації. Секретна аутентифікаційна інформація, що використовується для доступу до компонентів інфраструктури мережі, відповідає Password Policy.

2.3 Сегрегація в мережі

1. Доступ до Інтернету в межах **ЗОЗ** забезпечується через виділені мережі. З'єднання кабелем повинні використовуватися тільки корпоративними пристроями. Корпоративну бездротову мережу можуть використовувати як корпоративні, так і особисті пристрої працівників.

2. Корпоративна бездротова мережа складається з ізольованих підмереж, розділених за наступними правилами:

а) Різні VL□N для корпоративних і гостьових пристроїв;

б) Різні підмережі;

в) Різні SSID.

2.4 Передача інформації

1. Формальні правила та вимоги для захисту передачі інформації через використання різних видів комунікаційних засобів описані в Політиці класифікації інформації та Політиці використання Інтернету та електронної пошти.

2. Крім того, потреба ЗОЗ в захисті інформації визначається та документується в угодах про нерозголошення, підписаних усіма працівниками та підрядниками перед початком співпраці.

Додаток А.10

Політика використання паролів –
Password Policy

1. Огляд

1.1 Вступ

Паролі є важливим аспектом комп'ютерної безпеки. Погано обраний пароль може призвести до несанкціонованого доступу до інформації ЗОЗ **ЗОЗ** та/або її використання. Усі співробітники та підрядники **ЗОЗ**, які мають доступ до інформації та інформаційних систем **ЗОЗ**, відповідають за вжиття належних заходів, викладених нижче, для вибору та захисту своїх паролів.

1.2Мета

Метою цієї політики є встановлення стандарту для створення надійних паролів і захисту цих паролів.

1.3Обов'язки

Співробітники та підрядники **ЗОЗ**:

• Відповідають за вибір надійних паролів та забезпечення їх конфіденційності.

2. Положення політики

2.1 Передача секретної аутентифікаційної інформації

1. Розподіл секретної аутентифікаційної інформації має контролюватися.

2. Загалом слід уникати наступних каналів для передачі секретної аутентифікаційної інформації:

а) усі види соціальних мереж (наприклад, Facebook, LinkedIn, X, Instagram);

б) Skype, Telegram, Viber, Whats□pp або будь-який інший месенджер, не керований **ЗОЗ**;

в) поштову скриньку, відмінну від корпоративної, як для відправлення, так і для отримання секретної аутентифікаційної інформації.

3. Секретна аутентифікаційна інформація спільних ідентифікаторів користувачів має передаватися одним із наступних способів:

а) за допомогою спеціального програмного забезпечення або систем, прийнятих у **ЗОЗ**(наприклад, сховища паролів, Confluence);

б) записана на папері та передана особисто; папір має бути знищено після першого використання пароля;

в) продиктована по телефону.

4. Секретна аутентифікаційна інформація неперсональних ідентифікаторів користувачів, які не можуть або не повинні змінюватися після першого використання, має передаватися за допомогою методів передачі секретної аутентифікаційної інформації спільних ідентифікаторів користувачів.

5. Секретна аутентифікаційна інформація неперсональних ідентифікаторів користувачів, які повинні змінюватися після першого використання, повинні переважно передаватися за допомогою методів передачі секретної аутентифікаційної інформації спільних ідентифікаторів користувачів. Однак така секретна аутентифікаційна інформація також може бути надіслана за допомогою будь-якої поштової скриньки **ЗОЗ**, особистої поштової скриньки користувача або SMS за допомогою особистого мобільного пристрою користувача. Як відправник, так і отримувач повинні видалити електронний лист/повідомлення із секретною аутентифікаційною інформацією якомога швидше. SMS слід використовувати лише як останній засіб, коли немає доступних інших методів.

6. Користувачі повинні підтвердити отримання секретної аутентифікаційної інформації принаймні усно та повинні змінити тимчасову секретну аутентифікаційну інформацію під час першого входу до системи. Якщо підтвердження не було надано своєчасно, надана секретна аутентифікаційна інформація вважається скомпрометованою, і необхідно вжити відповідних заходів безпеки.

7. Власники систем та сервісів або інші уповноважені особи повинні перевірити особу користувача перед наданням нової, замінної або тимчасової

секретної аутентифікаційної інформації. У випадку, якщо правдоподібна перевірка неможлива, секретна аутентифікаційна інформація не може бути надана за жодних обставин.

2.2 Використання секретної аутентифікаційної інформації

1. Секретна аутентифікаційна інформація користувача, така як паролі, повинна зберігатися в конфіденційності, щоб не розголошуватися жодним іншим сторонам, включаючи інших співробітників, системних адміністраторів, керівників і посадових осіб. Групова (наприклад, спільна) секретна аутентифікаційна інформація повинна зберігатися виключно серед членів групи.

2. Секретна аутентифікаційна інформація не повинна зберігатися в записах (наприклад, записана на папері, збережена в програмному файлі або на знімному носії) безпосередньо, якщо вона не може зберігатися безпечно, і метод зберігання був затверджений **ЗОЗ** (наприклад, сховище паролів).

3. Коли паролі використовуються як секретна аутентифікаційна інформація, слід використовувати лише сильні, якісні паролі, які відповідають наступним вимогам:

а) паролі повинні бути легкими для запам'ятовування (якщо тільки вони не зберігаються безпечно у записах);

б) паролі повинні містити принаймні дванадцять (12) символів;
в) пароль повинен містити принаймні 3 з 4 можливих груп символів: великі літери, малі літери, цифри та символи;

г) паролі не повинні базуватися на будь-чому, що інша особа може легко вгадати або отримати, використовуючи інформацію про особу, наприклад, імена, номери телефонів, дати народження тощо;

д) пароль не повинен складатися з одного слова, наприклад, пароля, або загальновживаної фрази;

е) паролі не повинні містити загальні слова або шаблони з клавіатури (наприклад, пароль, картинка, iloveyou, qwerty, abcdefg тощо);

є) паролі не повинні містити послідовності цифр за порядком;

ж) паролі не повинні бути суто числовими або лише алфавітними символами;

з) якщо паролі безпечно зберігаються у записах (наприклад, у системі управління паролями або на зашифрованому жорсткому диску), вони повинні мати достатню довжину і бути абсолютно випадковими;

и) різні паролі не повинні слідувати одному й тому ж шаблону, оскільки це дозволить вгадати пароль, якщо будь-який із паролів, що слідують за шаблоном, буде скомпрометований;

і) якщо тимчасові паролі, їх слід змінити під час першого входу.

4. Користувачі повинні використовувати окремий, унікальний пароль для кожного з їх робочих облікових записів.

5. Користувачі повинні використовувати окремий, унікальний пароль для кожної системи або сервісу.

6. Користувачі не повинні використовувати жодних робочих паролів для своїх особистих облікових записів.

7. Користувачам не дозволяється ділитися окремою або спільною секретною аутентифікаційною інформацією, якщо вони не є власниками системи або сервісу та не мають на це право відповідно до відповідних процедур.

8. Дозволено використовувати біометричні технології як секретну аутентифікаційну інформацію на робочих системах, якщо ці технології не можуть бути зламані, і використання біометричних технологій не суперечить нормативним актам **ЗОЗ**.

2.3 Захист секретної аутентифікаційної інформації

1. Секретна інформація автентифікації повинна розглядатися як конфіденційна інформація і не повинна передаватися нікому, в тому числі іншим співробітникам, системним адміністраторам, керівників та осіб, наділених владними повноваженнями, якщо інше не передбачено політикою та процедурами **ЗОЗ.**

2. Секретну інформацію для автентифікації корпоративного облікового запису Microsoft (адреса електронної пошти та пароль) слід запам'ятати і не зберігати в жодному вигляді.

3. Користувачам рекомендується використовувати авторизовані системи керування паролями (сховища паролів) для зберігання своєї секретної автентифікаційної інформації. сховища) для зберігання своїх секретних даних автентифікації.

4. Використання функції «Запам'ятати пароль» веб-браузерів для зберігання секретної автентифікаційної інформації для зберігання секретної автентифікаційної інформації дозволяється лише за наступних умов:

а) профіль браузера прив'язаний до корпоративної електронної адреси ЗОЗ;

б) профіль браузера, прив'язаний до корпоративної електронної адреси **ЗОЗ**, не повинен використовуватися на будь-якому пристрої, що не належить або не орендується **ЗОЗ**, щоб уникнути синхронізації між профілем браузера та некерованими незахищеними пристроями.

5. Будь-який користувач, який підозрює, що його пароль був скомпрометований, повинен повідомити про інцидент системним адміністраторам і негайно змінити всі скомпрометовані паролі.

6. Після десяти (10) невдалих спроб введення пароля обліковий запис користувача повинен бути примусово заблокований на п'ятнадцять (15) хвилин.

2.4 Зміна та відновлення секретної автентифікаційної інформації

1. Користувачі не зобов'язані змінювати свої паролі за заздалегідь визначеним розкладом, якщо вони увімкнули багатофакторну автентифікацію.

2. Паролі для облікових записів без увімкненої багатофакторної автентифікації слід змінювати кожні 12 (дванадцять) місяців.

3. Всі користувачі зобов'язані змінювати секретну автентифікаційну інформацію користувача, якщо є будь-які ознаки її можливої компрометації.

4. Усі паролі, встановлені постачальником за замовчуванням, повинні бути змінені після інсталяції системи або програмного забезпечення.

2.5 Багатофакторна аутентифікація (MFA)

Багатофакторна автентифікація (MF□) настійно рекомендується і повинна використовуватися, коли це можливо як для робочих, так і для особистих акаунтів.

Додаток А.11

Політика фізичної та екологічної безпеки – Physical and Environmental Security Policy

1. Огляд

1.1 Вступ.

Політика фізичної та екологічної безпеки (далі "Політика") описує правила та процедури для контролю фізичного доступу до робочих зон приміщень **ЗОЗ** та запобігання пошкодженням і втручанням в інформацію організації та пов’язані з нею активи.

1.2 Мета.

Метою цієї Політики є визначення основних процедур для запобігання несанкціонованому фізичному доступу, пошкодженням та втручанню в інформацію організації та її активи.

1.3 Відповідальність

Співробітники **ЗОЗ**:

- Відповідальні за дотримання правил цієї Політики та інших правил і положень інформаційної безпеки **ЗОЗ** під час доступу до приміщень **ЗОЗ** та роботи в робочих зонах.

2. Положення Політики

2.1 Захищені зони

2.1.1 Контроль фізичного доступу

1. **ЗОЗ** відповідальна за забезпечення того, щоб зони, які містять конфіденційну або внутрішню інформацію та пов’язані з нею активи, були визначені та належним чином захищені.
2. Усі співробітники та підрядники **ЗОЗ** повинні дотримуватися правил контролю фізичного доступу, зазначених у політиках і процедурах.

3. Доступ до об'єктів і робочих зон обмежується лише для уповноваженого персоналу. Усі співробітники та підрядники **ЗОЗ** повинні входити до будівлі через визначений вхід.

4. Доступ до основної будівлі та робочих зон контролюється за допомогою:

а) системи доступу за картками;

б) звичайних замків;

в) системи відеоспостереження;

г) системи сигналізації.

2.1.2 Електронні картки доступу

1. Співробітники **ЗОЗ** отримують персональні електронні картки доступу у формі бейджа, який надає їм відповідний доступ до об'єктів з дати прийняття на роботу.

2. Співробітники повинні завжди носити видані картки під час перебування на території **ЗОЗ**.

3. Після звільнення всі співробітники повинні повернути свої картки доступу офіс-менеджеру або системному адміністратору. Такі картки повинні бути заблоковані в кінці дня звільнення.

4. Ключі та картки доступу не повинні залишатися без нагляду на видному місці або переноситися таким чином, що їх легко втратити або вкрасти.

5. Користувачі повинні повідомляти офіс-менеджера або інженера з комп’ютерних технологій про будь-які потенційні або фактичні проблеми з безпекою, включаючи несанкціонований вхід, крадіжку майна або втрату ключів чи електронних карток.

6. У разі втрати персональної електронної картки доступу **ЗОЗ** відбувається її блокування. Користувач повинен негайно повідомити про втрату картки офіс-менеджеру або системному адміністратору, який повинен забезпечити її негайне блокування.

2.1.3 Доступ для відвідувачів

1. Відвідувач — це будь-яка особа, яка не є співробітником **ЗОЗ**, а саме: зовнішні консультанти, кандидати на вакансію, клієнти, гості, постачальники, зовнішній персонал для обслуговування тощо.

2. Відвідувачі можуть отримувати тимчасові електронні картки доступу для гостей.

3. Відвідувачі повинні бути супроводжені відповідальним співробітником протягом усього часу їхнього перебування на території **ЗОЗ**.

4. Відвідувачам надається доступ лише для конкретних, санкціонованих цілей, і їм надаються інструкції щодо вимог безпеки зони.

5. Співробітник **ЗОЗ** особисто несе відповідальність за відвідувача та забезпечує дотримання ним внутрішніх правил і збереження майна **ЗОЗ**, супроводжуючи відвідувача протягом усього часу його присутності.

2.1.4 Робота в захищених зонах

1. Захищені зони — це кімнати на об’єкті, доступ до яких обмежений для осіб, які потребують його для виконання своїх обов’язків (наприклад, серверна кімната, склад тощо).

2. Доступ до захищених зон надається лише на основі потреби відповідно до функціональних обов’язків.

3. Робота в захищених зонах має контролюватися. Робота без нагляду в цих зонах повинна уникатся як з міркувань безпеки, так і для запобігання можливим зловмисним діям.

4. Слід контролювати та регулювати такі екологічні умови, як температура та вологість, які можуть негативно вплинути на функціонування в захищених зонах.

2.2 Захист від зовнішніх та екологічних загроз

1. Головний технічний директор (CTO) відповідає за впровадження, перевірку та тестування контролю фізичного та екологічного захисту, а також за

їх належне функціонування відповідно до чинного законодавства та нормативних актів.

2. Вогнегасники та детектори мають бути встановлені відповідно до чинних місцевих законів і нормативних актів.

3. Контроль екологічного захисту має перевірятися регулярно відповідно до чинних законів і нормативних актів.

2.3 Безпека обладнання

2.3.1 Захист і технічне обслуговування обладнання

1. Обладнання **ЗОЗ** має бути належним чином розташоване і захищене, щоб зменшити ризики від екологічних загроз та мінімізувати неналежний доступ до робочих зон і можливості несанкціонованого доступу.

2. Системи та обладнання, що обробляють конфіденційну інформацію, повинні бути розташовані таким чином, щоб зменшити ризик її перегляду неуповноваженими особами під час використання.

3. Обладнання **ЗОЗ** повинно регулярно обслуговуватися відповідно до визначеного графіка технічного обслуговування, щоб забезпечити його доступність та цілісність. Системні адміністратори відповідають за підтримку графіка технічного обслуговування обладнання. Технічне обслуговування та ремонт повинні проводитися уповноваженим персоналом.

4. Якщо обслуговування виконується зовнішнім персоналом, вони повинні бути супроводжені відповідальним співробітником **ЗОЗ** протягом усього часу, поки треті особи перебувають на території **ЗОЗ**.

5. Перед повторним введенням обладнання в експлуатацію після його технічного обслуговування його слід перевірити, щоб впевнитися, що обладнання не було пошкоджене та не має несправностей.

6. Підтримуючі комунікації повинні регулярно перевірятися та тестуватися (принаймні раз на рік) відповідно до визначеного графіка, щоб забезпечити їхнє належне функціонування.

2.3.2 Безпека обладнання та активів за межами приміщень

1. Спеціалісти **ЗОЗ** можуть вивозити свої корпоративні ноутбуки та настільні комп’ютери за межі офісу без попереднього погодження, за умови, що в них увімкнене повне шифрування диска.

2. Вивезення з офісу інших інфраструктурних активів (наприклад, серверів, мережевого обладнання тощо) дозволено лише спеціалістам з команди системного адміністрування.

3. Коли обладнання та інформація вивозяться з території **ЗОЗ**, користувачі несуть відповідальність за їх безпечне транспортування та зберігання наскільки це розумно практично. Комп’ютерне обладнання та носії даних повинні зберігатися поза полем зору і не повинні залишатися без нагляду, де це можливо. Коли вони зберігаються вдома, вікна та двері повинні бути зачинені, коли житло не зайняте.

4. Користувачі повинні дотримуватися правил «чистого столу» та «чистого екрану» під час використання активів за межами приміщень.

2.3.3 Безпечний ремонт обладнання

1. Якщо обладнання, що містить інформацію **ЗОЗ**, відправляється на ремонт, носії інформації повинні бути або зашифровані, зачищені, або взагалі витягнуті з пристрою.

2.3.4 Безпечна утилізація або повторне використання обладнання

1. Всі предмети обладнання, що містять носії інформації, повинні перевірятися, щоб впевнитися, що будь-які чутливі дані та ліцензоване програмне забезпечення були видалені або безпечно переписані перед утилізацією або повторним використанням.

2. Носії інформації, що містять конфіденційну інформацію, повинні бути безпечно стерті перед повторним використанням, або, якщо їх не можна очистити, повинні бути знищені перед утилізацією.

3. Інформація повинна бути знищена, видалена або переписана за допомогою методів, які роблять первинну інформацію недоступною. Для безпечного видалення інформації можуть використовуватися методи стирання диска або розмагнічування.

4. Окрім безпечного видалення даних з диска, слід виконати повне шифрування диска, якщо це доцільно, щоб зменшити ризик розкриття інформації **ЗОЗ** під час утилізації або повторного використання обладнання.

Додаток А.12

Процедура встановлення програмного забезпечення – Software Installation Procedure

1. Відповідальність

Співробітники та підрядники ЗОЗ:

• Відповідальні за дотримання правил, визначених у цій Процедурі, щодо запитів та затвердження встановлення програмного забезпечення на корпоративні робочі станції.

Системні адміністратори:

• Відповідальні за обробку запитів на встановлення додаткового програмного забезпечення відповідно до робочого процесу, визначеного в цій Процедурі.

• Відповідальні за надання технічної підтримки та допомоги з встановлення програмного забезпечення.

Технічний директор (CTO):

• Відповідальний за оцінку запитів на встановлення додаткового програмного забезпечення та ухвалення рішення щодо його встановлення та використання.

Юридичний консультант:

• Відповідальний за перегляд Умов використання та Ліцензійної угоди для запитаного програмного забезпечення.

2. Вимоги до встановлення програмного забезпечення

1. Встановлення програмного забезпечення користувачами повинно бути обмежене, контрольоване і відповідати принципу найменших привілеїв.

2. Програмне забезпечення може бути встановлено та використовуватися лише у випадку, якщо це не призведе до компрометації існуючих засобів безпеки.

3. Забороняється встановлення та використання несанкціонованого програмного забезпечення.

4. Дозволені типи встановлення програмного забезпечення включають:

а) оновлення та виправлення до Стандартного програмного забезпечення;

б) програмне забезпечення, добре відоме в IT-спільноті (наприклад, популярні браузери, програми для миттєвих повідомлень, безкоштовні утиліти, інструменти, бібліотеки та фреймворки, що добре відомі у спільноті розробників);

в) програмне забезпечення, узгоджене з клієнтом (якщо ліцензія надана клієнтом).

5. Недозволені типи встановлення програмного забезпечення включають:

а) неліцензійне програмне забезпечення;

б) потенційно шкідливе або невідоме програмне забезпечення з неперевірених джерел;

в) програмне забезпечення, яке входить до чорного списку.

3. Процедури встановлення програмного забезпечення на робочі станції

1. Програмне забезпечення, зазначене в пункті 2.4 цієї Процедури, може бути встановлено самостійно користувачами без додаткового затвердження.

2. Якщо користувач сумнівається у безпеці певного програмного забезпечення або його комерційному використанні, він/вона повинен(на) надіслати запит на перегляд програмного забезпечення до Інженера з комп’ютерних технологій.

3. Системний адміністратор повинен переглянути запит і перевірити наявність дозволеного програмного забезпечення, яке може бути використане як альтернатива запитаному (наприклад, якщо користувач запитує встановлення певного редактора документів, Системний адміністратор може запропонувати використання іншого стандартного програмного забезпечення тієї ж категорії).

4. Якщо альтернативи не існує, Системний адміністратор повинен додати СТО та Юридичного консультанта до запиту для оцінки.

5. СТО та Юридичний консультант повинні оцінити запит. На цьому етапі може бути проведена оцінка впливу на інформаційну безпеку для оцінки ризиків, пов'язаних із використанням запитаного програмного забезпечення. Юридичний консультант відповідальний за перегляд Умов використання та Ліцензійної угоди і повідомлення про будь-які виявлені обмеження СТО.

6. На основі результатів оцінки СТО ухвалює рішення щодо використання запитаного програмного забезпечення.

7. Якщо запит на встановлення програмного забезпечення задоволений, користувач може завантажити програмне забезпечення з надійного та перевіреного джерела і встановити його на свою робочу станцію. У разі виникнення проблем із встановленням користувач може звернутися за допомогою до Системних адміністраторів.

Додаток А.13

Політика управління доступом –
System and Application Access Control Policy

1. Огляд

1.1 Вступ

Управління доступом – це техніка безпеки, яка регулює, хто або що може переглядати або використовувати ресурси в обчислювальному середовищі. Це фундаментальне поняття в сфері безпеки, яке знижує ризики під час виконання робочих процесів.

1.2 Мета

Мета цієї Політики – запобігти несанкціонованому доступу до систем і додатків ЗОЗ **ЗОЗ**.

1.3 Відповідальність

Співробітники та підрядники **ЗОЗ**:

● Відповідають за дотримання правил цієї Політики при доступі до систем ЗОЗ;

● Відповідають за дотримання вимог щодо безпечної процедури входу та рекомендацій з управління паролями при розробці систем і додатків.

Системні адміністратори та власники активів:

● Відповідають за налаштування правил контролю доступу відповідно до робочих вимог щодо управління доступом.

2. Положення політики

2.1 Обмеження доступу до інформації

1. Інформаційні системи **ЗОЗ**, як придбані, так і розроблені всередині ЗОЗ, повинні бути реалізовані з відповідними механізмами автентифікації та заходами, які відповідають вимогам ЗОЗ щодо інформаційної безпеки і чутливості даних, до яких здійснюється доступ, та відповідати сучасним кращим практикам щодо прав доступу користувачів.

2. Повинен бути визначений і впроваджений набір дозволів, який дозволяє контролювати, до яких даних мають доступ користувачі та який рівень доступу (наприклад, читання, запис, видалення). Дозволи мають надаватися як окремим користувачам, так і ролі, що відповідає групі користувачів з певними відповідальностями та потребами.

3. Ті додатки і системи, які розроблені всередині ЗОЗ та потребують інтеграції з іншими додатками або системами, повинні інтегруватися через PI, захищені сучасними протоколами автентифікації та авторизації.

4. Сторонні додатки і системи повинні переважно дотримуватися сучасних кращих практик щодо прав доступу користувачів і засобів інтеграції з іншими додатками або системами. Ті додатки і системи, які не дотримуються таких сучасних практик, не повинні використовуватися взагалі або повинні підлягати оцінці ризиків. Можуть бути введені інші заходи безпеки, щоб компенсувати недоліки систем щодо обмеження доступу до інформації.

2.2 Безпечні процедури входу

1. Там, де це доцільно і застосовано, доступ до систем і додатків повинен контролюватися за допомогою безпечної процедури входу.

2. Процедура входу в систему або додаток повинна бути розроблена таким чином, щоб мінімізувати можливість несанкціонованого доступу та розкривати мінімум інформації про систему або додаток, щоб уникнути надання несанкціонованому користувачу зайвої допомоги.

3. Багатофакторна автентифікація (MF) повинна використовуватися в тих випадках, коли необхідна надійна автентифікація та перевірка особи.

4. Там, де застосовано, співробітники і підрядники **ЗОЗ**, залучені до розробки систем і додатків, повинні враховувати наступні вимоги до хорошої процедури входу:

а) не відображати ідентифікатори системи або додатка до успішного завершення процесу входу;

б) відображати загальне попередження, що доступ до системи або додатка дозволено лише авторизованим користувачам;

в) не надавати повідомлення з допомогою під час процедури входу, які можуть допомогти несанкціонованому користувачу;

г) перевіряти інформацію для входу тільки після завершення введення всіх даних. Якщо виникає помилка, система не повинна вказувати, яка частина даних правильна або неправильна;

д) захищати від спроб грубого підбору пароля;

е) реєструвати як невдалі, так і успішні спроби входу;

ж) генерувати подію безпеки, якщо виявлено спробу або успішне порушення контролю входу;

з) після успішного входу відображати наступну інформацію:

I) дату та час попереднього успішного входу;

II) деталі будь-яких невдалих спроб входу з моменту останнього успішного входу.

і) не відображати пароль під час його введення;

к) не передавати паролі у відкритому вигляді по мережі;

л) завершувати неактивні сесії після певного періоду бездіяльності, особливо в місцях з високим ризиком, таких як громадські місця або зовнішні зони поза управлінням безпеки ЗОЗ або на мобільних пристроях;

м) обмежувати час підключення для забезпечення додаткової безпеки для додатків з високим рівнем ризику та зменшення можливості несанкціонованого доступу.

2.3 Вимоги до управління паролями для систем і додатків

1. Паролі та інша секретна інформація для автентифікації в системах і додатках повинні управлятися контрольованим чином. Нижченаведені вимоги повинні бути враховані в наступних випадках:

а) при розробці механізмів контролю доступу для управління паролями для систем і додатків;

б) при виборі/покупці системи або додатку;

в) при впровадженні засобів безпеки для управління паролями в існуючих системах і додатках.