Усього на 2023 рік заплановано закупівлю МВ для пацієнтів з БЕ за 20 найменуваннями на загальну суму майже 120 млн грн. За офіційними даними ДП «Медичні закупівлі України», за кошти Державного бюджету на 2023 рік за бюджетною програмою КПКВК 2301400 «Забезпечення медичних заходів окремих державних програм та комплексних заходів програмного характеру» за напрямом «Закупівля лікарських засобів (в т. ч., тих, що підлягають закупівлі відповідно до договорів керованого доступу), імунобіологічних препаратів (вакцин), МВ та допоміжних засобів до них» у частині «Медичні вироби для громадян, які страждають на бульозний епідермоліз» наразі закуплено 1 152 од. Гель для ран Prontosan® X, туба 250 г (Б. Браун Медикал АГ, Швейцарія) за ціною 3 027,34 грн; 1 од. Розчин для іригації ран Prontosan®, флакон 350 мл (Б.Браун Медикал АГ, Швейцарія) за ціною 600,88 грн. Враховуючи те, що перев'язувальні матеріали мають різні особливості, а пацієнти різну потребу в них для виконання конкретних завдань, складно оцінити потребу в цій запланованій частці витрат.

Висновок. Система забезпечення МВ пацієнтів з БЕ для лікування шкіри потребує перегляду підходів в напрямку нормативно-правового врегулювання через особливості самого захворювання, що впливає на річні потреби в ЛЗ та МВ, а саме перегляду номенклатури закупівель.

ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ (ISMS, СУІБ) В МЕДИЧНИХ І ФАРМАЦЕВТИЧНИХ ЗАКЛАДАХ

Пімінов О. Ф., Лебединець В. О., Зарічкова М. В.
Інститут підвищення кваліфікації спеціалістів фармації
Національного фармацевтичного університету
м. Харків, Україна
lebedynets@nuph.edu.ua

Вступ: Кібератаки стають частішими, більш організованими та більш збитковими для державних установ, бізнесу та об'єктів критичної інфраструктури. Згодом вони можуть досягти критичного рівня, який загрожує національному та Євроатлантичному процвітанню, безпеці й стабільності – зазначено у Стратегічній концепції оборони та безпеки НАТО, що була анонсована на саміті НАТО у листопаді 2010 р., м. Лісабон. У світі з 2019 по 2021 рр. кількість кібератак лише на урядові інформаційні системи та мережі зросла майже втричі. Наразі щотижня в світі реєструється понад 255 млн. кібератак, а взагалі проблеми в системах забезпечення комп'ютерної безпеки великих підприємств та урядових установ виявляються кожні 35 хвилин. Збитки від кібератак у 2020 р. становили понад 375 млрд. дол. США, а витрати на кібербезпеку у 2020 р. склали понад 54,5 млрд. дол. США. За прогнозами експертів збитки бізнесу від кібератак найближчими роками можуть перевищити 6 трильйонів доларів, якщо підвищення дієвості системи кіберзахисту не носитиме кардинального характеру.

Серед глобальних ризиків і загроз для України можна назвати збільшення кількості масштабних дезінформаційних кампаній (кампаній, інспірованих активістами радикальних рухів для маніпулювання свідомістю окремих людей та груп населення), інформаційну політику країни-агресора (вплив на ключові демократичні інституції, посилення внутрішніх протирічь в Україні тощо), збільшення впливу соціальних мереж на внутрішню і зовнішню суспільно-політичну ситуацію, а також недостатній рівень медіаграмотності (медіакультури) населення України.

За твердженням багатьох фахівців, на сьогодні кіберпростір повинен розглядатись як п'ята сфера ведення бойових дій, поряд з наземною, повітряною, морською та космічною. Кібератаки є одним із шляхів та засобів вирішення державних і недержавних проблем.

Виходячи з цього, питання пошуку ефективних способів, методів і засобів забезпечення інформаційної безпеки взагалі та у закладах галузі охорони здоров'я (зважаючи на її стратегічне значення для країни) зокрема є актуальним завданням сьогодення.

Мета: обґрунтувати актуальність забезпечення інформаційної безпеки та висвітлити основні етапи впровадження систем управління інформаційною безпекою в медичних і фармацевтичних закладах відповідно до вимог стандарту ISO/IEC 27001.

Методи: для досягнення мети були використані методи наукового дослідження: аналіз статистичних даних, огляд нормативно-правових актів, державних програм, стратегій, положень та інших документів стосовно інформаційної безпеки; структурний та логічний аналіз для угрупування та систематизації інформаційних матеріалів.

Результати. Система управління інформаційною безпекою (СУІБ) – це набір політик і процедур для систематичного управління конфіденційними даними організації з метою мінімізації ризику та забезпечення безперервності бізнесу шляхом проактивного обмеження впливу на безпеку. СУІБ зазвичай стосується поведінки і дій працівників, а також даних і технологій. СУІБ може бути націлена на певний тип даних, як-от інформація про замовників, клієнтів, споживачів (що актуально, зокрема, для медичних і аптечних закладів, для дистриб'юторів лікарських засобів і медичних виробів, які повинні забезпечувати простежуваність продукції), або може бути реалізований комплексним способом, який стане частиною культури компанії.

Мета впровадження СУЫБ – забезпечити потрібний організації рівень інформаційної безпеки, тобто збереження конфіденційності, цілісності і доступності інформації. Крім того, можуть бути поставлені й інші задачі, зокрема, забезпечити автентичність, підзвітність, незаперечність і надійність інформації. У цьому контексті під конфіденційністю слід розуміти забезпечення доступу до даних на основі розподілу прав доступу, захист від несанкціонованого ознайомлення (дані можуть бути *відкриті*, коли право доступу мають усі користувачі, з *обмеженим* доступом, коли має доступ тільки певна група людей, а також *особисті*, до яких доступ може мати тільки одна людина). Доступність – забезпечення постійного доступу до даних відповідним категоріям користувачів і захист цих даних від блокування

зловмисниками. Цілісність – захищеність даних від їх зловмисного або випадкового знищення чи спотворення

Інформаційна безпека включає в себе комплекс заходів, які повинні забезпечити захищеність даних від несанкціонованого доступу, використання, оприлюднення, внесення змін чи знищення. Види загроз інформаційній безпеці:

- отримання доступу до секретних або конфіденційних даних;
- порушення або припинення роботи інформаційної системи;
- отримання доступу до керування роботою інформаційної системи;
- знищення або спотворення даних.

Методи та засоби забезпечення інформаційної безпеки дуже різні. Зокрема, їх прийнято класифікувати на технічні, адміністративні (організаційні) та фізичні. Технічні засоби захисту – це, перш за все, міжмережеві екрани, антивірусні програми, системи автентифікації та шифрування, системи контрольованого доступ до інформаційних об'єктів як для груп, так і для кожного окремого користувача. Адміністративні та правові заходи захисту – це звід правил користування даними і комп’ютерною інфраструктурою, зокрема ліцензування діяльності у сфері забезпечення інформаційної безпеки та атестація об'єктів інформатизації. До фізичних засобів захисту належать охоронні конструкції, замки, сейфи, камери спостереження тощо.

Комплексне керування всіма цими заходами й засобами в організації доцільно здійснювати згідно із міжнародними стандартами захисту та управління даними, такими як ISO 27001.

Стандарт ISO/IEC 27001:2022 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Вимоги – це загальноприйнятий на міжнародному рівні стандарт з управління інформаційною безпекою, розробленим Міжнародною організацією зі стандартизації (ISO) разом з Міжнародною комісією з електротехніки (IEC). Стандарт встановлює вимоги для створення, впровадження, підтримки та постійного вдосконалення СУІБ.

ISO/IEC 27001:2022 встановлює принципи й вимоги, що допомагають організаціям ефективно керувати ризиками для інформаційної безпеки, визначає процедури ідентифікації, аналізування та управління ризиками для конфіденційності, цілісності та доступності інформації.

Стандарт з'явився як відповідь на зростання кількості кібератак та збільшення загроз інформаційній безпеці на світовому рівні, збільшення потреб у надійному захисту конфіденційної інформації, запобігання витоку даних, забезпечення безперервності та збільшення довіри до бізнесу й державних структур. Перше видання стандарту ISO/IEC 27001 з'явилося ще у 2005 р. Відтоді були видані оновлені версії у 2013 та 2017 рр., а остання актуалізація відбулася у 2022 р. з метою адаптації до змін у технологічному середовищі та врахування нових загроз і викликів, пов'язаних з безпекою інформації.

Етапи впровадження СУІБ можна визначити таким чином:

Ініціювання проєкту впровадження СУІБ

Встановлюються цілі впровадження системи, визначаються терміни, ресурси, очікувані результати. Формується команда, відповідальна за реалізацію проєкту. Встановлюються інформаційні активи та процеси СУІБ.

Виконання контекстного аналізу

Аналізуються зовнішні та внутрішні фактори, що впливають на інформаційну безпеку в організації. Виявляються зацікавлені сторони, їхні вимоги й очікування стосовно інформаційної безпеки (наприклад, інвестори, кредитори, партнери, власники, замовники тощо).

Розробка політики інформаційної безпеки компанії

Визначаються й декларуються загальні засади, принципи й цілі, пов'язані з інформаційною безпекою в межах організації.

Встановлення процесів управління ризиками

Описуються процедури ідентифікації, оцінювання, аналізування та керування ризиками для інформаційної безпеки.

Забезпечення відповідності вимогам

Визначаються вимоги стандартів та законодавства, яким повинна відповідати організація в контексті забезпечення інформаційної безпеки.

Реалізація дій з керування ризиками

Визначаються потенційні загрози для інформаційної безпеки та їхні можливі наслідки, а також ймовірність реалізації ризиків (настання небажаної ситуації). Визначаються заходи для мінімізації чи усунення ризиків, включаючи технічні, організаційні, правові тощо.

Впровадження заходів із забезпечення інформаційної безпеки

Організаційні: встановлюються політики, процедури та розподіляється відповідальність для забезпечення безпеки інформації. Проводиться навчання й підготовка персоналу щодо додержання вимог з інформаційної безпеки. Технічні: заходи із фізичного захисту носіїв інформації.

Моніторинг, оцінювання результативності та покращення

Визначаються показники (характеристики, індикатори), що дозволяють вимірювати ефективність СУІБ. Проводяться внутрішні аудити та оцінювання відповідності встановленим вимогам. На основі отриманих результатів вносяться корективи та вживаються коригувальні й запобіжні дії з удосконалення СУІБ.

Сертифікація СУІБ на відповідність вимогам стандарту ISO/IEC 27001:2022 здійснюється за необхідності.

Ключові аспекти функціонування СУІБ можна стисло описати так:

- Застосування політики інформаційної безпеки організації (політика інформаційної безпеки визначає правила, процедури та відповідальності щодо захисту інформації, включаючи правила доступу до конфіденційної інформації, використання інформаційних мереж та систем, роз’яснення ризиків для безпеки працівникам організації).
- Інформування й навчання працівників (персонал має бути належно навчений правилам та процедурам інформаційної безпеки, включаючи виявлення фішингу, проявам соціальної інженерії, безпечного використання паролів та інших аспектів безпеки).