ЗАХИСТ ДАНИХ АВТОМАТИЗОВАНОЇ КОМП'ЮТЕРНОЇ СИСТЕМИ КОНТРОЛЮ УМОВ ЗБЕРІГАННЯ ФАРМАЦЕВТИЧНОЇ ПРОДУКЦІЇ ІМПОРТЕРА ЛІКАРСЬКИХ ЗАСОБІВ

*Лебединець В. О., Чорний Д. С.**
Національний фармацевтичний університет, м. Харків
*ТОВ «Фармацевтична Компанія Віста», м. Київ

Постанова Кабінету Міністрів України від 30.11.2016 № 929 «Про затвердження Ліцензійних умов провадження господарської діяльності з виробництва лікарських засобів, оптової та роздрібної торгівлі лікарськими засобами, імпорту лікарських засобів (крім активних фармацевтичних інгредієнтів)» вимагає здійснювати імпорт лікарських засобів (ЛЗ) наявності діючої ліцензії на імпорт ЛЗ з додержанням вимог настанови СТ-Н МОЗУ 42-5.0:2014 «Лікарські засоби. Належна практика дистрибуції» (GDP) та настанови СТ-Н МОЗУ 42-4.0:2016 «Лікарські засоби. Належна виробнича практика» (GMP) у тій частині, що стосуються діяльності з імпорту лікарських засобів. Таким чином імпортери повинні враховувати вимоги GMP у контексті використання комп'ютеризованих систем (КС) у критичних етапах імпорту та подальшої дистрибуції ЛЗ на території України.

Валідаційні випробування КС проводяться у відповідності до програм та методики, які враховують IT – інфраструктуру, складність та критичність процесів імпорту та дистрибуції, що засновані на менеджменті ризиків для якості, та розробляються кожним імпортером індивідуально. У GDP зазначається конкретна вимога щодо даних утворених в процесі роботи КС – їх слід охороняти фізичним або електронним способом, а резервні дані, які створені шляхом резервних копій, слід зберігати в окремому місці, що охороняється, протягом часу, визначеного чинним законодавством України, але не менше ніж п'ять років. Таким чином імпортери мають прикласти необхідні зусилля для забезпечення захисту та зберігання даних КС протягом щонайменше п'яти років, а в окремих випадках пов'язаних з внутрішніми вимогами імпортера – від п'яти до п'ятнадцяти років.

На сучасних фармацевтичних складах імпортерів для забезпечення цілодобового вимірювання й реєстрації умов зберігання ЛЗ з функцією керування кліматичним обладнанням при необхідності, найчастіше використовують комерційну КС з відповідним програмним забезпеченням (ПЗ). Така система у своїй роботі накопичує велику кількість даних у персональному та/чи іншому архівах, яку у свою чергу слід перевіряти щодо доступності, читабельності та неушкодженості. Має бути забезпечена та випробувана можливість відновлення даних, для доказу спроможності КС виконувати свої функції та надавати свідчення простежуваності критичного процесу.

У одному з меморандумів PFSB/CND, Директором Відділу відповідності та лікарських засобів, Бюро фармацевтичної та харчової безпеки, Міністерства охорони здоров'я, праці та соціального забезпечення Японії, була надана відповідь щодо класифікації категорії відповідно до GAMP 5 «Керівництво, що ґрунтується на підходах з оцінки ризиків до комп'ютеризованих систем GxP», комерційної КС контролю парового стерилізатора високого тиску, температура і час яких встановлюються користувачем і система яких контролюється вбудованою програмою загального призначення. Таку систему класифікували як «Категорія 3 - Неконфігуровані продукти» і якщо система використовуються без перегляду ПЗ, валідація ПЗ може проводитися під час кваліфікації обладнання КС, якщо це необхідно. Таким чином, аналогічно, до «Категорії 3 - Неконфігуровані продукти» можна віднести комерційні КС та ПЗ для забезпечення цілодобового вимірювання й реєстрації умов зберігання ЛЗ, що пропонується постачальниками, як готовий продукт для використання. У таких випадках, на основі задовільної попередньої кваліфікації постачальників комерційних КС та ПЗ з врахуванням

усіх необхідних ризиків, можна застосовувати простий підхід, що складається з одного рівня – тестування та верифікація на відповідність вимогам специфікації користувача. Верифікація зазвичай охоплює: правильну установку; тести, які демонструють придатність та відповідність викладеним вимогам; будь – які подальші випробування в результаті оцінки ризиків та постачальників комерційних КС та ПЗ. Постачальники КС та ПЗ зазвичай виконують необхідну перевірку відповідно до специфікації, надає відповідну документацію та підтримки (технічне обслуговування).

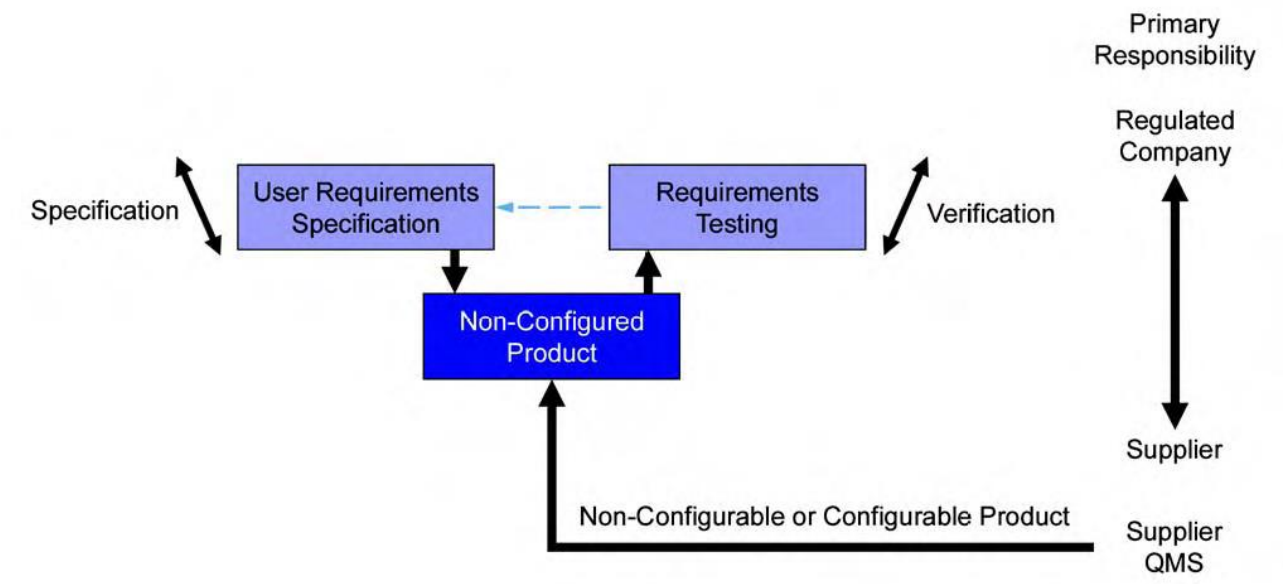

Рисунок 1. Підхід до валідації КС «Категорії 3-Неконфігуровані продукти» за GAMP 5

У цій статті ми розглянемо окремий критичний процес виконуваний КС – захист, збереження, архівування даних та належно захищений доступ до цієї інформації. До компетенції імпортера ЛЗ відноситься ресурси та обладнання, які необхідно виділити для захисту, збереження та архівування даних, що згенерувались у процесі роботи КС для забезпечення цілодобового вимірювання й реєстрації умов зберігання ЛЗ. Для попередження несанкціонованого втручання до КС та ПЗ має бути враховано максимум потенційних ризиків та встановлено фізичне обмеження доступу до апаратної та логічний контроль доступу до програмної частини КС.

Відповідно до рекомендацій GAMP 5 фармацевтичне підприємство повинно розробити Політику інформаційної безпеки, в якій будуть викладені правила та рекомендації щодо використання КС, ПЗ та доступу до них. Для гарантії відсутності втручання, Політика інформаційної безпеки також повинна враховувати використання КС що кваліфіковані, валідовані та контролюють критичні процеси. У Політику інформаційної безпеки імпортера слід враховувати:

- - Фізичну безпеку та безпеку доступу до КС та ПЗ, включаючи надання та скасування доступу (наприклад, видача ідентифікаторів користувача та керування паролями);
- - Доступ третіх сторін;
- - Систему електронних повідомлень та сповіщень;
- - Спільні мережеві ресурси, доступ до інтернету та локальної мережі;
- - Використання мобільних обчислювальних ресурсів (наприклад, портативні комп'ютери, кишенькові персональні комп’ютери, мобільні телефони);
- - Підключення до зовнішніх КС;
- - Антивірусні політики та виявлення несанкціонованих вторгнень.

Доцільно для побудови системи управління інформаційною безпекою у імпортера ЛЗ

необхідно враховувати вимоги і рекомендації міжнародних стандартів ISO:

- - Вимоги до системи управління інформаційною безпекою (ISO/IEC 27001);
- - Зведення правил системи управління інформаційною безпекою (ISO/IEC 27002);
- - Розробка системи управління інформаційною безпекою (ISO/IEC 27003);
- - Управління ризиками інформаційної безпеки (ISO/IEC 27005).

Розроблення ІТ-інфраструктури та впровадження правил та політики інформаційної безпеки у імпортера ЛЗ – це у пержу чергу завдання кваліфікованого персоналу. Окрему увагу необхідно приділити охороні, захисту та зберігання даних КС та ПЗ, з якими працює інший персонал, що авторизується у самій системі та/або має доступ до апаратної частини. З ростом кількості вразливостей, які зачіпають традиційні рішення для авторизації, необхідно посилювати можливості аутентифікації за допомогою «строгої аутентифікації»:

- - Фактор знання. Загальний секрет між користувачем і суб'єктом перевірки автентичності користувача (наприклад, паролі, відповіді на секретні питання і т.д.);
- - Фактор володіння. Пристрій, яким володіє тільки користувач (наприклад, мобільний пристрій, криптографічний ключ і т.д.);
- - Фактор невід'ємності. Фізичні та біометричні характеристики користувача (наприклад, відбиток пальця, малюнок райдужної оболонки ока, голос, поведінка і т.д.)

Таким чином доцільно враховувати зазначені способи аутентифікації до формування політики щодо захисту та зберігання критичних даних КС та доступу тільки уповноваженого персоналу до такої інформації.

Двоетапна аутентифікація користувачів до критичного ПЗ та КС, серверів, баз даних, програмних архівів значно знизить ризик або попередить втручання сторонніх осіб та/або часткову чи повну втрату даних. Для поєднання методів строгої аутентифікації пропонуємо розглянути логічний метод доступу (фактор володіння) та біометричний метод доступу (фактор невід’ємності).

До системи логічного доступу можна віднести систему управління ключами з урахуванням вимог стандартів, процедур і безпечних методів для:

- - генерації ключів для різних криптосистем і додатків;
- - виготовлення та отримання сертифікатів відкритих ключів;
- - розсилки ключів відповідним користувачам, включаючи навчання активації ключів після отримання;
- - зберігання ключів, включаючи навчання авторизованих користувачів та отримання доступу до ключів;
- - заміни або поновлення ключів, включаючи правила і терміни заміни ключів;
- - анулювання ключів, включаючи порядок вилучення і деактивації;
- - відновлення ключів, які були загублені або зіпсовані;
- - резервного копіювання або архівування ключів;
- - знищення ключів;
- - реєстрації та аудиту дій, пов'язаних з управлінням ключами.

Таблиця 1. Деякі методи логічної аутентифікації.

Аутентифікація	*Короткий опис*
Апаратна	Спеціальний пристрій, що генерує одноразові паролі
Програмна	Програма, яка генерує одноразові паролі, та відправляє коди на персональний мобільний телефон, чи пошту

Аутентифікація	*Короткий опис*
Смарт-карти	Карта, яка містить криптографічний чіп і захищену пам'ять з ключами, що використовується для аутентифікації інфраструктуру відкритих ключів
Ключі безпеки - токени	Пристрій з інтерфейсом USB, який містить криптографічний чіп і захищену пам'ять з ключами, що використовується для аутентифікації інфраструктуру відкритих ключів

Ідентифікація та аутентифікація по **біометричним характеристикам** найбільш поширена та оптимальна тим, що персоналу не треба запам'ятовувати інформацію ідентифікації та аутентифікації. У вітчизняних дослідженнях автора Ніжніченко О. К., приділяється увага коефіцієнту помилкового пропуску та відмови для різних систем біометричного доступу, де використовувались параметри FAR (False Acceptance Rate) – коефіцієнт помилкового пропуску, тобто відсоток виникнення ситуацій, коли система дозволяє доступ користувачу, незареєстрованому в системі та FRR (False Rejection Rate) – коефіцієнт помилкової відмови, тобто відмова в доступі справжньому користувачеві системи.

Таблиця 2. Коефіцієнти помилкового пропуску та відмови для різних систем біометричного доступу.

Біометрична система керування доступу використовує:	FAR*	FRR*
Відбиток пальця	0,001%	0,6%
Розпізнавання 2D	0,1%	2,5%
Розпізнавання обличчя 3D	0,0005%	0,1%
Райдужна оболонка ока	0,00001%	0,016%
Сітківка ока	0,0001%	0,4%
Малюнок вен	0,0008%	0,01%

* - Чим нижче ці показники, тим вище точність розпізнання об'єктів.

Висновок. Під час складання специфікації вимог користувача та вибір комерційної КС та ПЗ необхідно приділити особливу увагу охороні, захисту та зберіганню даних, з якими працює персонал. У зв’язку із необхідністю довготривалого зберігання даних, мають бути прикладені зусилля до захисту, пропорційні вірогідності ризику, пов’язаному з втратою доступності, читабельності, неушкодженості, відтворюваності та відновлення. Робочий доступ персоналу імпортера ЛЗ до критичних КС та ПЗ – невід’ємна частина у функціонуванні таких систем. Усі співробітники імпортера ЛЗ повинні проходити відповідне навчання і бути в курсі актуальних політик і процедур, які можна застосувати до їх функцій. Відповідальний за інформаційну безпеку ІТ – персонал, відповідно до політики інформаційної безпеки, повинен впровадити строгу аутентифікацію для персоналу імпортера ЛЗ, що працює з КС та ПЗ.

Виходячи з викладеного матеріалу та з урахуванням вимог GMP, GDP, GAMP 5, для захисту даних та їх архівів можна використовувати двоетапну аутентифікацію за допомогою біометричних характеристик та логічного доступу. Відносно недорогим та достатньо надійним методом пропонується застосовувати відбиток пальця для попереднього доступу до критичних КС та ПЗ з додатковим застосування пристрою «токен», який містить криптографічний чіп і захищену пам'ять з ключами. Така комбінація для користувача достатньо зручна, для ІТ-персоналу добре контрольована і придатна для тестування, валідації та верифікації.