УДК 004.056.2

С.В. Медушевський, Черкаси

КЛЮЧОВІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ GXP-КРИТИЧНИХ ДАНИХ АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ФАРМАЦЕВТИЧНИХ ВИРОБНИЦТВ

Abstract. The problem of ensuring the integrity of critical data in automated information systems of pharmaceutical industries, as well as the problem of risk assessment in such systems, are considered and analyzed. It is proposed to justify the use of the method of control of the integrity of confidential information on the basis of the formation and distribution in the information environment of structures of related hash tables, which does not require the storage of controlled information GxP-critical data.

Актуальність

Правила належної виробничої практики встановлюють вимоги до організації виробництва і контролю якості лікарських засобів для медичного застосування та ветеринарного застосування з тим, щоб виробники могли гарантувати високу якість продукції від серії до серії.

У додатку 11 до Правил належної виробничої практики визначаються нормативні вимоги до критичних записів GMP, керованим за допомогою комп'ютеризованих систем: ці вимоги в кінцевому рахунку спрямовані на забезпечення цілісності цих даних, керованих за допомогою автоматизованих інформаційних систем (AIC) [1].

Несанкціоноване втручання в виробничі і технологічні процеси може призводити не тільки до економічних втрат, зниження ефективності управління, а й, в найгіршому випадку, до техногенних катастроф [2].

Управління регульованими даними розвивалося в останнє десятиліття відповідно до довго триваючого розвитку допоміжних технологій (таких, як використання телеметричного збору даних, автоматизація систем і використання дистанційних технологій) і збільшеною складністю ланцюга поставок і способів роботи (наприклад, через постачальників послуг). Системи, що підтримують ці методи роботи, можуть використовувати як ручні процеси з паперовими записами, так і повністю комп'ютеризовані системи.

Процеси збору, перетворення, зберігання і розсилки повідомлень в інформаційно-обчислювальних системах завжди пов'язані з ризиком спотворення і втрати даних [3].

Питання безпеки та цілісності даних висвітлено в багатьох публікаціях закордонних і вітчизняних авторів.

У роботах [4 – 6] доведено, що інтеграція нових технологій збереження, обробки та аналізу великих даних в існуючі реляційні сховища є актуальною поточною задачею і висуває нові вимоги з інформаційної сумісності та

комплексного захисту інтегрованих даних.

Контроль цілісності даних в умовах можливості зловмисних дій (спотворення, видалення, заміни інформації), особливо дій осіб з санкціонованим доступом до баз даних і каналів зв'язку, залишається, на жаль, невирішеним завданням.

Актуальність вирішення даного завдання полягає в необхідності захисту інформації від навмисного впливу з боку легальних користувачів, які можуть приховати сліди раніше реалізованих деструктивних впливів, посилюючи тим самим їх шкідливий ефект або запобігаючи наступ юридичної відповідальності за вчинені помилкові або неправомірні дії [7].

Постановка задачі

Цілісність даних визначається як «ступінь повноти, послідовності і точності даних протягом усього життєвого циклу даних», і має основне значення у фармацевтичній системі якості, яка забезпечує необхідну якість лікарських засобів. Неналежні методи забезпечення цілісності даних і їх уразливість підривають якість записів і в кінцевому рахунку можуть компрометувати якість лікарських засобів [8].

Проаналізувавши ряд робіт в яких розглянута [2, 9, 10, 11, 12] проблема забезпечення цілісності метрологічних даних в інформаційних виробничих системах, а також проблема оцінки ризиків в таких системах, зроблено висновок, що завдання захисту цілісності даних є складною, зважаючи на свою комплексності, так як включає в себе не тільки контроль цілісності даних, але і її забезпечення, що має на увазі відновлення даних, цілісність яких була порушена за різними причинам

Найбільш популярним є рішення комплексного захисту цілісності даних, пов'язаної з одночасним вирішенням завдань контролю і забезпечення цілісності даних, яке досягається за рахунок послідовного застосування спочатку криптографічного перетворення до даних, а потім застосування технології резервного копіювання даних, що, як відомо, призводить до введення високої надмірності [13].

Метою роботи є аналіз та обґрунтування методики забезпечення цілісності даних АІС фармацевтичних виробництв в процесі валідації системи в цілому.

Вирішення задачі

Управління даними – це сукупність організаційних заходів, що забезпечують цілісність даних. Ці організаційні заходи забезпечують повноту, послідовність і точність запису протягом усього життєвого циклу даних, незалежно від процесу, формату або технології, в яких вони генеруються, реєструються, обробляються, зберігаються, витягуються і використовуються.

Ефективний підхід до управління даними заснований на оцінці ризику для цілісності даних, що визначається наступними факторами:

1) критичність даних (вплив на прийняття рішень і якість продукції);

2) схильність порушень (можливість зміни і видалення даних, а також

ймовірність виявлення/видимості змін в процесі рутинної перевірки з боку виробника). Вплив визначається потенційною можливістю видалення, зміни або виключення незареєстрованим особою і можливістю виявлення таких дій і подій.

Життєвий цикл (рис. 1) даних поширюється на те, як дані генеруються, обробляються, повідомляються, перевіряються, використовуються для прийняття рішень, зберігаються і остаточно видаляються в кінці терміну зберігання. Дані, що відносяться до продукту або процесу, можуть перетинати різні границі протягом життєвого циклу.

Найбільш поширеним методом забезпечення цілісності даних є використання засобів електронно-цифрового підпису.

Під життєвим циклом даних розуміються всі фази даних з моменту їх первісного створення і реєстрації, їх подальшої обробки (включаючи перетворення або міграцію), використання, перевірки і зберігання даних, архівування/вилучення і виведення даних з використання.

Життєвий цикл складається з активної (звернення з даними / записами) і неактивній (архівація/знищення даних) фаз.

Рис. 1. Життєвий цикл даних

Комп'ютеризовані системи, які можуть впливати на якість продукції або послуг і цілісність даних, підпадають під дію правил GMP і потребують валідації. Цілісність даних (Data integrity) – це якісне і цілісне зберігання даних, яке визначається неможливістю змін даних в процесі їх створення або неврахованих змін.

Система менеджменту якості повинна створювати умови для дотримання цілісності даних (Data integrity) через використання стандартних процедур і правил та підтримуватися під час життєвого циклу підприємства валідації і перевіркою помилок. Актуальність Data Integrity останнім часом обумовлена наступними факторами:

- запис даних не в момент виконання операції;

- запис даних заднім числом.
- використання старих даних як нових даних;
- використання тестів на минулі серії в нових серіях;
- повторне виконання тестів для отримання кращих результатів без аналізу первинних результатів;
- підробка даних і «вкидання» невдалих даних;
- підміна негативних результатів, неякісна обробка помилок.

Системи управління даними є невід'ємною частиною фармацевтичної системи якості (PQS) для кожного етапу життєвого циклу продукції: PQS повинна володіти даними протягом усього життєвого циклу і враховувати проектування, використання та моніторинг процесів/систем з метою дотримання принципів цілісності даних, включаючи контроль навмисних і ненавмисних змін і видалення інформації.

Процес управління цілісністю GxP-критичними даними можна представити у вигляді схеми на рис. 2.

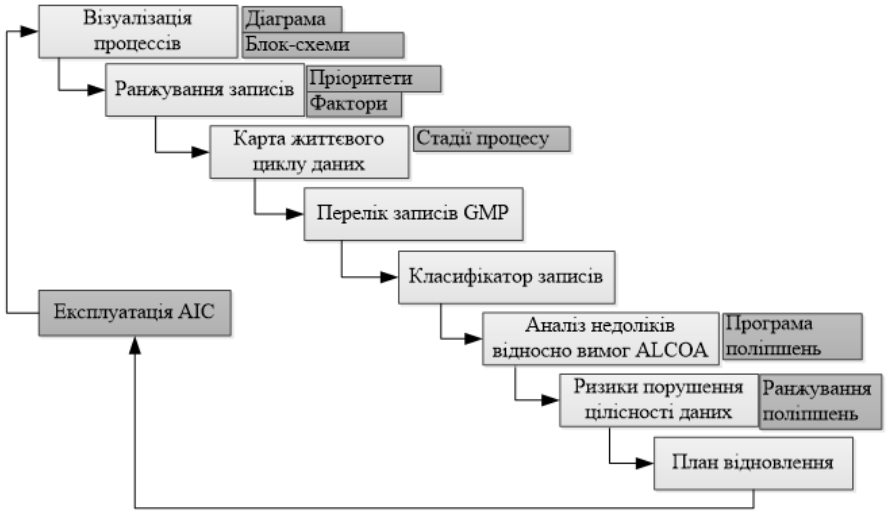

Рис. 2. Процес управління цілісністю GxP-критичними даними AIC

Найбільш поширеними методами вирішення завдання забезпечення цілісності даних в AIC є:

- застосування різних видів резервування (RAID-масиви, методи дублювання, методи надлишкового кодування);
- застосування криптографічних методів: ключове і безключового хешування, засоби електронного підпису (ЕП).

Використання систем забезпечення цілісності даних на основі використання ключових хеш-функцій має ряд переваг [9]:

- зменшення кількості криптографічних перетворень;
- можливість регулювати довжину хеш-коду.

Заходи контролю для забезпечення цілісності даних вбудовуються в фармацевтичну систему якості, яка гарантує, що лікарські засоби мають необхідну якість. Цілісність даних може бути застосована до всіх елементів фармацевтичної системи якості, і принципи, викладені в цьому документі, в рівній мірі застосовні до даних, створюваним і електронними і паперовими системами. Для забезпечення точності, повноти, послідовності та надійності записів і даних протягом усього періоду їх затребуваності (на протязі всього життєвого циклу даних) організації повинні слідувати належної виробничої практики документування (GDocP).

Ключові принципи як паперового, так і електронного документообігу об'єднані в акронім ALCOA. Простежуваність (Attributable), Читабельність (Legible), Своєчасність (Contemporaneous), Оригінальність (Original) і Точність (Accurate)), який був розширений додаванням інших атрибутів: (Повнота (Complete), Послідовність (Consistent), Стійкість (Enduring) і Доступність (Available), які тепер називаються ALCOA+.

Таблиця 1

Характеристика атрибутів ALCOA+ стосовно GxP-критичних даних AIC

Атрибут	Характеристика
Простежуваність	унікальна реєстрація користувачів
	унікальні електронні підписи
	журнал реєстрації подій
Читабельність	забезпечення збереження запису
	відсутність перезапису
	відсутність видалення записів
	збір інформації про всі зміни
	резервне копіювання та архівування
Своєчасність	синхронізація всіх відміток за датою/часом
Оригінальність	порівняння копії з оригінальною записом
	підтвердження правильності та повноти копії
	документальне оформлення перевірки
Точність	забезпечення дійсності (валідності) даних
Повнота	в наявності всі дані, включаючи записи журналу реєстрації подій
Послідовність	всі елементи повинні відповідати послідовності епізодів, а також мати позначки за часом і датою, розміщені відповідно до очікуваної послідовністю подій
Стійкість	необхідна наявність апаратного резервування і ефективних процедур щодо створення резервної копії/відновлення, які гарантують надійне збереження даних
Доступність	необхідна наявність доступу до даних для їх огляду, перевірки або інспектування протягом усього життєвого циклу запису

Виконання очікувань ALCOA+, опис яких наведено вище (табл. 1), гарантує, що події належним чином задокументовані і дані можуть використовуватися для прийняття обґрунтованих рішень.

Відновлення цілісності даних, в силу непередбачуваності характеру спотворення в результаті впливу випадкових подій, ґрунтується на статистичному спостереженні. Виявити порушення інформаційної цілісності вдається послідовними обчисленнями контрольних сум значень полів запису про об'єкт і порівняннями зі значеннями, обчисленими в момент попереднього включення процедури. Ці ж контрольні суми використовуються для вирівнювання вмісту копій, що зберігаються на взаємодіючих серверах (в тому числі, віртуальних). При кожній санкціонованій зміні запису, контрольні суми перераховуються заново, і неузгодженість даних виявляється тільки у випадках, якщо зміни викликані порушеннями інформаційно-обчислювального процесу, а не технологічними операціями.

Тестування і перевірка обмежень цілісності при проектуванні і супроводі бази даних є запорукою збереження даних [14].

Типовий алгоритм контролю цілісності даних заснований на:

- періодичній перевірці ідентичності розосереджених описів керованих об'єктів і елементів системи шляхом зіставлення їх ключових параметрів;
- перевірці фактичного виконання розсилки санкціонованих змін записів у взаємодіючі бортові і наземні фрагменти (копії) розподіленої бази даних щодо подій оновлень інформації на основі обміну;
- заміщення спотвореного запису, виявленого в будь-якому фрагменті бази даних, її еталонною копією, супроводжувано. підсистемою поточного аналізу якості роботи АІС.

Метод пов’язаних хеш-таблиць (Associated Hashes), створює можливості контролю цілісності GxP-критичних даних без звернення до реєстратора даних і дозволяє практично виключити безслідну зміну даних. Даний метод засновано:

- на реєстрації інформації шляхом її хешування, створенні структури пов'язаних хеш-таблиць і виділення з неї контрольної суми;
- на поширенні копій контрольної суми, її фрагментів і спеціально розроблених реперів в інформаційному просторі;
- на створенні алгоритмів повного або часткового відновлення контрольних сум шляхом порівняння його копій або копій його фрагментів.

У методі пов’язаних хеш-таблиць записи, що відносяться до різних даних, пов'язують один з одним за допомогою системи пов'язаних хеш-таблиць, схожою з використовуваної в протоколі штампу часу (TSP), з якого потім виділяють частину інформації про контрольну суму в інформаційному просторі.

Порядок формування контрольних сум за методом пов’язаних хеш-записів включає:

- формування початкового рядка;
- обчислення локального хеш-запису h_m початкового рядка;
- обчислення пов'язаного хеш-запису H_m, як хеш-запису від конкатенації рядків локального хеш-запису h_m і пов'язаного хеш-запису H_m_i попереднього запису (H_i – по заданому H_0, названому кореневим хеш-записом контрольної суми).

Реєстрація шляхом вбудовування в контрольне ядро не самого початкового рядка, а його хеш-запису, дозволяє не розкривати її змісту, що забезпечує конфіденційність при відкритому доступі до контрольної суми.

При проведенні тестування інтеграційних рішень величезну роль грає регресійне тестування, при цьому серйозною проблемою є порівняння результатів тестування, отриманих на одних і тих же тестових прикладах. Складність полягає в необхідності локалізації розбіжності у вихідних даних за умови їх великого обсягу.

Застосування системи автоматизованого тестування використовує метод пов’язаних хеш-записів, що дозволяє вирішити проблему обробки великих обсягів вихідних даних:

1) при первинному тестуванні вихідні дані реєструються шляхом формування контрольної ідентифікаційної записи, де кожен локальний хеш – це хеш одного вихідного набору даних.
2) при кожному наступному тестуванні відпадає необхідність в повному порівнянні даних і досить порівняння значень пов'язаних хеш, починаючи, наприклад, з останніх і закінчуючи першим яке співпало з відповідним хешем вихідного контрольного ядра – збіг інших випливає з властивостей контрольних сум.

Висновки

В ході проведених досліджень встановлено, що база даних АІС, побудована відповідно до розроблених структур і алгоритмів з використанням методу пов’язаних хеш-таблиць, буде володіти високими показниками ефективності в частині забезпечення цілісності GxP-критичних даних, які обробляються і зберігаються протягом життєвого циклу лікарського засобу.

Ефективна система управління даними демонструє розуміння і прихильність керівництва компанії надійним практикам управління даними, включаючи необхідність поєднання відповідної організаційної культури і поведінки і розуміння ризику, пов'язаного з даними на протязі їх життєвого циклу.

Доведено об'єктивність і доцільність використання методу контролю цілісності конфіденційної інформації (метод пов’язаних хеш-таблиць) на основі формування і поширення в інформаційному середовищі структур пов'язаних хеш-таблиць (контрольних сум), що не вимагає зберігання контрольованої інформації GxP-критичних записів АІС.

1. СТ-Н МОЗУ 42-4.0:2016. Настанова. Лікарські засоби. Належна виробнича практика. Київ: МОЗ України, 2016. – 357 с.
2. *Фазлиахметов Т.И.* Модель анализа рисков несанкционированной модификации метрологических данных в производственных системах / Фазлиахметов Т.И., Фрид А.И. // Вестник Уфимского государственного авиационного технического университета. – 2012. – №16 (3 (48)). – С.187-193.
3. *Рудельсон Л.Е.* Стратегия контроля целостности данных в концепции управления общесистемной информацией / Рудельсон Л.Е. Смородский С.Н., Степаненко А.С. // Научный вестник Московского государственного технического университета гражданской авиации. – 2017. – № 20 (4). – С.114-126.
4. *Спасітєлєва С.О.* Комплексний захист гетерогенних корпоративних сховищ даних / Спасітєлєва С.О., Бурячок В.Л. // Сучасний захист інформації. – 2017. – №1. – С.58-65.
5. *Лучинин З.С.* Математическая модель документо-ориентированной базы данных с отражением ограничений целостности. / Лучинин З.С., Сидоркина И.Г. // Вестник Чувашского университета. – 2015. – №1. – С.174-180.
6. *Королева Ю.А*. Разработка концепции миграции данных между реляционными и нереляционными системами БД / Ю.А. Королева В.О. Маслова В.К. Козлов // Программные продукты и систем. – 2019. – №32 (1). – С.63-67.
7. *Савин С.В.* Обеспечение целостности данных подсистемы регистрации и учета автоматизированных систем на основе метода «Однократной записи» / Савин С.В., Финько О.А // Известия Южного федерального университета. Технические науки. – 2015. – №5 (166). С.64-77.
8. *Душкин А.В.* Аналитическая модель оценки эффективности обеспечения защиты данных от угроз нарушения целостности в информационных системах / Душкин А.В., Демченков А.В. // Вестник Воронежского института МВД России. – 2015. – №1. – С.87-95.
9. *Савин С.В.* Обеспечение целостности данных в автоматизированных системах на основе линейных систем хэш-кодов / Савин С.В., Финько О.А. // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2015. – №114. – С.796-811.
10. *Алексеев Д.М.* Обеспечение ссылочной целостности данных / Алексеев Д.М., Кутняк Н.А. // Инновационная наука. – 2016. – № 16. – С.19-21.
11. *Клименко С.В.* Метод контроля целостности данных с использованием CRC кода / Клименко С.В., Яковлев В.В., Ададуров С.Е // Известия Петербургского университета путей сообщения. – 2017. – №14 (4). – С.738-746.
12. *Колісник Т.П.* Підтримка цілісності у базах даних з неоднорідною структурою / Колісник Т.П. // Збірник наукових праць Харківського університету Повітряних Сил. – 2011. – № 1(27). С.184-187.
13. *Диченко С.А.* Контроль и обеспечение целостности информации в системах хранения данных / Диченко С.А. // Наукоемкие технологии в космических исследованиях Земли. – 2019. – № 11 (1). – С.49-57.
14. *Хомоненко А.Д.* Программа для автоматизированной верификации ограничений целостности баз данных. / Хомоненко А.Д., Глухарев, М.Л., & Косаренко А.П. // Программные продукты и системы. – 2011. – № 1. – С.91-95.

http://doi.org/10.5281/zenodo.3612230

Поступила 19.08.2019р.