ОЦЕНКА ЦЕЛОСТНОСТИ ДАННЫХ – ПОЧЕМУ ОНА ДОЛЖНА ПРЕДШЕСТВОВАТЬ ВАЛИДАЦИИ

АЛЕКСАНДР БЕЛИНСКИЙ,
технический директор
POE CIS

Зачастую при выполнении проектов по валидации компьютеризированных систем для различных компаний посещает мысль, что, несмотря на запрос от Заказчика, не факт, что он обратился за помощью по самому важному аспекту среди всех имеющихся у него «на борту». Ведь каковы основные побудительные мотивы такого запроса? Заведомо отсутствуют внутренние ресурсы, получено замечание внутреннего или внешнего аудита и т.п.

Так или иначе, речь чаще всего идет о каком-то точечном запросе, даже если это валидация какой-то крупной системы или ряда систем. Ведь при этом неминуемо остаются за кадром все остальные системы и их аспекты. И даже если ключевые риски определены верно – например, у Заказчика провалидирована система класса ERP[1], но не провалидирована система LIMS[2], то при разрозненном подходе может оказаться так, что валидационные стратегии сильно разнятся, в то время как бизнес-процессы между таковыми системами часто могут пересекаться. Скажем, отбор проб на складе формируется в системе ERP (сегмент WMS[3]) – именно там возникает предъявительское извещение, формируемое сотрудником склада, но вот уже сама проба «продолжает жить» в системе LIMS – т.е. имеется интерфейс. Учтен ли он? Не «потерялась» ли какая-то информация в таком интерфейсе? Вопрос открытый. Как, впрочем, и ряд других вопросов, часто менее очевидных, но в своей совокупности – не менее значимых.

Далее по тексту на рис. 1 представлен схематично порядок действий, иллюстрирующий интегрированный подход к оценке целостности данных, нацеленный на выявление пробелов и, при выявлении таковых, на выработку мероприятий по их устранению. Для того, чтобы подобная деятельность не была хаотичной, существует целая методология (впрочем, даже не одна – при желании каждая компания может добавить свою специфику). Но мы опишем магистральный маршрут.

Разумеется, первым шагом является создание реестра всех компьютеризированных систем предприятия. Тут сразу стоит оговориться, что, отталкиваясь от реестра компьютеризированных систем, мы сужаем оценку пробелов целостности данных до данных в электронном виде, максимум – для части гибридных (в электронном и бумажном виде). Вместе с тем целостность данных должна быть обеспечена и для бумажных записей. Для решения этой задачи может быть использована интегральная методология, описанная в другой статье автора – там выполнен охват сквоз-

[1] ERP = enterprise resource planning, планирование ресурсов предприятия.
[2] LIMS = laboratory information management system, система управления лабораторной информацией.
[3] WMS = warehouse management system, система управления складом.

ных бизнес-процессов [1]. В этой же статье рассмотрены только компьютеризированные системы, поскольку несмотря на то, что в отношении бумажных записей также может использоваться созвучная методология, все же мероприятия по устранению выявленных пробелов для бумажных документов будут иными. Поэтому и в этой части различия в детальных шагах уже будут существенными. Хотя верхнеуровнево останутся все те же базовые этапы.

Итак, получив реестр компьютеризированных систем, мы сразу же автоматически закрываем пробел по п. 4.4 приложения 11 [2][3], но самое важное – теперь у нас появляется полная картина того, чем мы располагаем. В терминологии ИТ-безопасников мы также начинаем с реестра информационных активов, что, по сути, можно соотнести с перечнем компьютеризированных систем. Я не напрасно упомянул направление ИТ-безопасности, поскольку на предприятиях может быть развитая ISMS[4] или ITSM[5]. Зачастую в рамках ISMS/ITSM уже могут быть выполнены эти шаги, т.е. создан реестр информационных активов и даже может быть проведена оценка рисков / приоритизация в их отношении, чаще всего в шкале «конфиденциальность» – «целостность» – «доступность». Это очень похоже на FME(C)A, только названия шкал отличаются. Можно оттолкнуться от результатов работы ИТ-безопасников, если таковая работа выполнена. Говорю очевидные, казалось бы, вещи, но лично сталкивался с ситуацией, что ИТ-службы предприятия работают в своем «колодце», а отдел обеспечения качества – в своем. В результате созвучная деятельность может выполняться дважды или заметно пересекаться, иногда в части аспектов – противоречить друг другу. Разумеется, все эти расходы ложатся на собственника. Конечно, это не нарушает какие-то

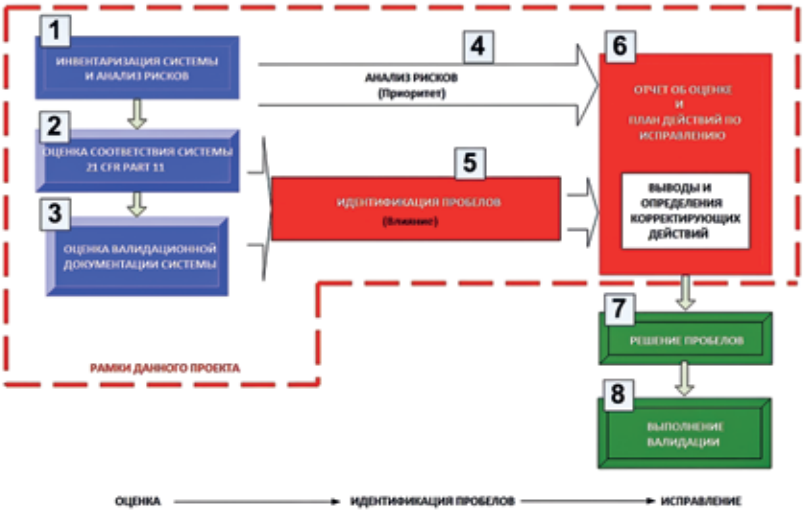

Рис. 1. Схематический порядок действий при оценке пробелов целостности данных

конкретные требования ни GxP, ни ISMS, но это явно не является рациональным.

Второй шаг уже обладает GxP-спецификой (хотя, если вдуматься, тоже может быть решен с фланга ISMS/ITSM или с большим его вовлечением). Оценив для каждой системы ее приоритет в шкале GxP-критичности и сложности, далее можно оценить ее соответствие применимым требованиям 21 CFR Part 11. И, попутно, соответствие приложению 11 GMP EU/EAЭС, хотя стоит признать, что собственно в рассматриваемых аспектах в отношении электронных записей, электронных подписей и их свойств приложение 11 GMP EU/EAЭС в значительной степени уступит в части конкретных указаний 21 CFR Part 11, несмотря на то, что последний документ создан гораздо раньше и не пересматривался более 25 лет. В частности, только 21 CFR Part 11 содержит конкретные требования к паролям в части необходимости их периодической смены (§11.300 (b)) или попыток их неавторизованного использования (§11.300 (d)). Такой степени детализации и близко нет в приложении 11 GMP EU/EAЭС – по этой причине часто возникает вопрос: мол, а где конкретно написано то или иное требование? Вопрос справедливый. До недавнего времени завуалированный в п. 4.1 главы 4 «Документация» основного текста GMP EU/EAЭС: ***«Должны быть соответствующие меры контроля для обеспечения целостности записей в течение срока хранения».*** Какие это конкретные меры – прямо не уточняется. В сентябре 2023-го вступила в силу «Рекомендация ЕЭК № 25» [4], где уже таковой конкретики найти можно больше – но ее первоисточник – 21 CFR Part 11, дополненный лучшими практиками ISMS (в частности, описанными в серии стандартов ISO 27k), и ITSM (аналогично, в частности, изложенными в серии стандартов ISO 20k). Чем удобны последние практики, которые, казалось бы, не имеют прямого отношения к фарме? Факторов «удобства» два:

1. Специалистов по ISMS, ITSM гораздо больше на рынке, чем специалистов по ISMS, ITSM именно в фарме. Или, напротив, фармацевтов с ИТ-бэкграундом требуемого уровня.

[3] ISMS = information security management system, система управления информационной безопасностью (СУИБ).
[4] ITSM = information technology service management, управление ИТ-услугой.

Безопасность (Security)	Целостность (Integrity)	Прослеживаемость (Traceability)	Подотчетность (Accountability)
- S1: Наличие уникальных персональных учетных записей для ПО? - S2: В наличии как минимум три группы пользователей (администратор, супервайзер, пользователь)? - S3: Настройки безопасности сконфигурированы в соответствии с СОП (сложность пароля, срок его действий, количество неудачных попыток входа, блокировка при бездействии? - S4: В наличии перечень авторизованных пользователей, и он периодически пересматривается?	- I1: В наличии автоматическое резервное копирование? -I2: Данные защищены от модификации/удаления в рамках ПО? -I3: Базы данных / папка с данными защищены от модификации/удаления в рамках ОС? -I4: В наличии функция автосохранения (для выходных (отчетных) записей)?	- T1: Контрольный след характеризуется следующими свойствами: - включен на уровнях пользователя, безопасности и системы? - является полным (кто, где, что и по какой причине изменил)? - защищен от модификации? -T2: Временная привязка (дата, время, временная зона) защищены от изменений? -T3: Контрольный след периодически проверяется согласно утвержденному СОП? - T4: Исходные данные или истинные копии поддерживаются контролируемым способом в течении требуемого времени хранения?	- ES1: Уникальность идентификационных компонентов и неудачных попыток неавторизованного использования мониторится в рутине - ES2: Связь межу электронной подписью (ЭП) и электронной записью (ЭЗ) - ES3: Публикация ЭП - ES4: Использование ЭП имеет ту же силу, что и использование рукописной подписи

2. Выполнив требования и рекомендации в сферах ISMS, ITSM, практически автоматически будут реализованы и применимые требования GMP. Возможно, за некоторым исключением, как, например, специфика по выпуску серии (в той же банковской безопасности подобный аспект отсутствует) или описания конкретных действий Уполномоченного лица.

Здесь могут быть предложены следующие шаги по категориям (см. табл. 1).

Разумеется, слепое использование практик ISMS/ISTM требует создания матрицы соответствия требованиям GxP, однако это вполне решаемая задача, позволяющая оптимизировать деятельность не только по поиску, но и по устранению пробелов в части целостности данных.

А в качества вывода следует указать, что собственно валидация компьютеризированных систем – это уже финальный шаг, который сам по себе ничего не улучшает и не устраняет. Перед тем как приступить собственно к валидационным шагам (п. 8 на рис. 1), гораздо более важными представляются разработанный план мероприятий по устранению (п. 6 на рис. 1) и реализация этих мероприятий (п. 7 на рис. 1). Например, при отсутствии разграничения прав доступа сначала следует эти права разграничить, согласовав бизнес-функции с владельцами системы и владельцами процесса, а только потом подтверждать в ходе валидации, что такие права разграничены надлежащим способом. Иначе сходу будет замечание даже по «неконкретному» приложению 11 GMP EU / ЕЭАС. Ведь п. 12.1 в нем гласит: ***«Должны иметься в наличии физические и (или) логические элементы контроля для обеспечения доступа к компьютеризированной системе только уполномоченным на то лицам»***, а при попытке парировать, мол, и тут неконкретно описано (какие лица и где именно собственно говорится о том, что у этих лиц должно быть разграничение прав доступа) – есть п. 12.3: ***«Создание, изменение и аннулирование прав доступа должно быть зарегистрировано»***. В этом примере мы логично приходим к тому, что все упирается в разработку процедуры «Управление учетными записями» – а это неотъемлемый элемент ISMS/ISTM.

Поэтому оценка целостности данных позволяет выстроить все процессы в этом отношении в их логической взаимосвязи, при которой валидация – всего лишь «зеркало», отражающее правильно выстроенную систему и хорошо проделанную работу для того, чтобы заниматься фармацевтическим производством, а не «подставлять табуретки под сервисы». ◆

ИСТОЧНИКИ

[1] Евразийское отделение ISPE. Оптимизация бизнес-процессов – как неотъемлемый шаг перед цифровизацией, Белинский А., NPJ.
[2] Решение Совета Евразийской экономической комиссии от 3 ноября 2016 г. № 77 «Об утверждении Правил надлежащей производственной практики Евразийского экономического союза», приложение 11.
[3] GMP EU, Annex 11.
[4] Рекомендация Коллегии Евразийской экономической комиссии от 19 сентября 2023 г. № 25 «О Руководстве по обеспечению целостности данных и валидации компьютеризированных систем».

PQE GROUP
GLOBAL QUALITY SOLUTIONS

25TH Anniversary

Выбирайте PQE для обеспечения качества и соответствия регуляторным требованиям:

GXP

- **GLP** Good **Laboratory** Practice
- **GCP** Good **Clinical** Practice
- **GVP** Good **Pharmacovigilance** Practice
- **GMP** Good **Manufacturing** Practice
- **GDP** Good **Distribution** Practice

- Подготовка к инспекции регуляторных органов
- Квалификация проектной документации, помещений, оборудования
- Аудиты GMP/GLP/GDP
- Внедрение современных подходов к организации валидационных работ
- Аудит поставщиков
- Поддержка при внедрении GXP критичных компьютеризированных систем
- Сопровождение при внедрении научного подхода к построению и оптимизации системы качества
- Проведение практик ориентированных тренингов на основе кейсов заказчиков

pqegroup.com
ru.info@pqegroup.com