Портянко Т.М.

Черкаський державний технологічний університет

Кучеренко В.С.

Черкаська медична академія

РОЛЬ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ ПІД ЧАС ВПРОВАДЖЕННЯ КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ НА ФАРМАЦЕВТИЧНИХ ПІДПРИЄМСТВАХ

Забезпечення безперервності бізнесу є одним із найважливіших стратегічних напрямів розвитку будь-якої компанії. Відповідно до вимог документації, що регламентує впровадження комп'ютеризованих систем (далі – КС) на фармацевтичних підприємствах, забезпечення безперервності бізнесу зумовлено необхідністю зберігати стійкість і стабільність функціонування КС у різних умовах несприятливого впливу зовнішніх і внутрішніх факторів техногенного та/або природного характеру на бізнес-процеси компанії. Безпека пацієнтів, якість продукції та цілісність даних не повинні піддаватися негативному впливу у разі збоїв у роботі або поломки у процесі експлуатації КС. Управління безперервністю бізнесу включає в себе аварійне відновлення, яке охоплює технічне відновлення КС і містить порядок дій персоналу по відновленню критично важливих ІТ-сервісів. Всі дії в аварійних / надзвичайних ситуаціях необхідно ретельно документувати і затверджувати. Для цього необхідно створити документ (план), що описує заходи, які необхідно вжити в разі часткової чи повної відмови КС. У статті розкрито практичні підходи до створення Плану забезпечення безперервності бізнесу та аварійного відновлення (далі – План), враховуючи специфіку та нормативні вимоги фармацевтичного виробництва. Відображені заходи, що можуть варіюватися від запланованого скорочення апаратного обладнання до переходу в систему з паперовими носіями інформації тощо. В статті підкреслено, як План визначає, яким чином бізнес-процеси компанії продовжують функціонувати і обробляти дані після збою в роботі КС. Особливу увагу приділено розділам Плану, де відображені кроки, що необхідні для відновлення бізнес-процесів після порушення і, за необхідності, як проходить керування даними, отриманими під час порушення, ролі і обов'язки персоналу, процес передачі інформації, а також визначення схеми для запуску Плану в дію. Визначається та обґрунтовується його необхідність там, де для продовження роботи бізнес-процесів застосовується інтерактивне внесення інформації, як будь-які електронні записи або дані будуть синхронізуватися відразу після відновлення КС. У статті приділена увага плануванню дій у надзвичайній ситуації, що включають регулярне тестування (випробування), оцінку ефективності Плану для підтвердження його працездатності в умовах, що змінюються, а також його корекцію.

Ключові слова: загрози, аварійні ситуації, бізнес-процеси, безпека пацієнтів, план безперервності бізнесу, комп'ютеризована система.

Постановка проблеми. У сучасному інформаційному суспільстві спостерігається зростаюча залежність успішності бізнесу від ефективної і безперервної роботи інформаційної інфраструктури. Інформатизація та автоматизація всіх сфер людської діяльності тягне за собою підвищення масштабів виробничих аварій і катастроф, які збільшують обсяг збитку для суб'єктів господарювання. Спектр загроз економічній, фізичній та інформаційній безпеці, а також перелік вразливостей технічної інфраструктури вітчизняного бізнесу і, зокрема, корпоративних інформаційних систем, стає дедалі більшим. Форс-мажорні обставини можуть виникнути в будь-який період діяльності організації. Навіть незначні інциденти

можуть мати суттєві наслідки. Забезпечення безперервності бізнесу є одним із найважливіших стратегічних напрямів розвитку компанії. Основними причинами, які призводять до таких втрат, є недооцінка ймовірності ризиків або відсутність у компанії ресурсів на розробку планів дій у разі настання аварійних і форс-мажорних ситуацій.

Особливо це стосується фармацевтичної промисловості, де безпека пацієнтів, якість продукції та цілісність даних не повинні піддаватися негативному впливу у разі збоїв у роботі чи поломки у процесі експлуатації комп'ютеризованих систем (далі – КС) [1, с. 10]. Для цього необхідно планувати безперервність виконання бізнес-процесів, дотримуючись нормативних вимог. Наявність

таких планів зводять до мінімуму наслідки різного роду інцидентів та навіть катастрофи і забезпечує можливість максимально швидко взяти під контроль ситуацію і відновити виконання критично важливих завдань.

Аналіз останніх досліджень і публікацій. У багатьох країнах система безперервності ведення бізнесу в різних формах функціонувала ще з 80-х років XX століття. За звітом, складеним U.S. Department of Homeland Security, Office of Domestic Preparedness разом з Michigan State University, можна констатувати таку статистику в Сполучених Штатах Америки:

- 47% підприємств, у яких відбулася пожежа або крадіжка, виходять з бізнесу;
- 44% компаній, які втратили записи під час катастрофи, ніколи не відновлюються;
- 93% компаній, які втратили значну частину даних, виходять з бізнесу впродовж п'яти років;
- більшість підприємств витрачає менше 3% від їх загального бюджету на планування відновлення бізнесу;
- один випадок втрати даних обходиться бізнесу в середньому у 10 000\$.

У роботах зарубіжних та вітчизняних авторів розглядаються питання актуальності впровадження системи забезпечення безпеки бізнесу в інформаційні системи підприємств та банківську діяльність. Проведені дослідження В. Ситніченко, Г. Кисельової, Є. Стоякіна, О. Дуксенко, А. Корченко та інших переважно націлені на виявлення загроз, таких як хакерські атаки, падіння серверів, технічні збої та інше [2, с. 4]. Але, на жаль, це не єдині загрози діяльності підприємств, особливо фармацевтичного сектора. Низький рівень зацікавленості компаній у виділенні окремого процесу й інвестуванні в його розвиток може бути викликаний складнощами в розумінні технічних процесів та достатньо високою вартістю ІТ-продуктів, які забезпечать впровадження автоматизованого процесу бізнес-безперервності компанії [3, с. 48]. Зважаючи на світову статистику, безпека підприємств фармацевтичної галузі у нашій країні є не тільки актуальною для самих підприємств, а й має соціальне та економічне значення. Держава несе відповідальність за якість лікарських засобів та виробів медичного призначення перед громадянами, а фармацевтичні підприємства, як суб'єкти господарювання, відповідальні перед державою. Тому їх безперервне та безпечне функціонування є важливим для забезпечення населення країни стратегічною продукцією.

Мета статті. З огляду на визначену вище актуальність обумовленого питання метою статті

є розробка методичних підходів і практичних рекомендацій щодо плану із забезпечення безперервності бізнес-процесів, що включає технічне відновлення КС і містить порядок дій персоналу з відновлення критично важливих ІТ-сервісів на підприємствах фармацевтичної промисловості.

Виклад основного матеріалу дослідження. Сьогодні практично всі учасники ринку прагнуть до збільшення автоматизації бізнес-процесів і зменшення людського впливу на їх впровадження. З одного боку, це позитивне прагнення, проте, з іншого боку, беручи до уваги збільшення кількості і складності кібератак, автоматизація стає найбільш вразливим елементом компанії, який може на значний період часу зупинити або паралізувати її діяльність. Коли йдеться про здоров'я та життя людини, ніхто не має права довіряти КС, не будучи впевненим у належному рівні її надійності. Сьогодні комп'ютерні технології використовуються не тільки у виробничих процесах фармацевтичного виробництва, а й у всіх інших системах, що складають фармацевтичну систему якості організації: управління приміщеннями і обладнанням, системами лабораторного контролю, управління матеріалами, процесами, які охоплюють весь цикл маркування продукції, та інше. Інформаційні системи контролюють параметри виробничого процесу, тим самим керуючи ними. За допомогою інформаційних систем персонал створює електронні документи та записи тощо. Прийнятний рівень їх надійності повинен бути збудований шляхом застосування ефективної моделі життєвого циклу КС. Належне планування аварійного відновлення і методи захисту, так само в числі інших процесів, гарантують надійність КС і точність результатів, отриманих у процесі експлуатації. Відповідно до нормативних вимог, щоб забезпечити придатність КС супроводжувати критичні процеси, мають бути вжиті заходи перестороги для гарантування безперервного супроводу таких процесів у разі поломки системи (наприклад, ручна або альтернативна система). Час, необхідний для приведення в дію альтернативних заходів, має враховувати ризик та бути придатним для конкретної системи та супроводжуваного робочого процесу [4, с. 218]. Такі заходи мають бути адекватно задокументовані та випробувані.

Управління безперервністю бізнесу – це комплексний процес, який допомагає визначити потенційні загрози і їх вплив на звичайний порядок ведення бізнесу. Зазначений процес надає компанії можливість завчасно підготуватися і визначити порядок дій для забезпечення максимально

ефективного управління компанією у разі істотних інцидентів або катастроф. Управління безперервністю бізнесу включає в себе кроки, необхідні для відновлення бізнес-процесів після порушення, продовжуючи при цьому виготовляти продукцію або надавати послуги замовнику, та включає заходи, які часто описуються як відновлення в аварійних ситуаціях.

Управління безперервністю бізнесу, як і будь-який процес, починається з аналізу з подальшим визначенням стратегії, сценаріїв і планів дій. Специфіка планів залежить від типу компанії, критичних для бізнесу процесів, необхідного рівня їх стійкості до позаштатних ситуацій. Планування забезпечення безперервності бізнесу може охоплювати кілька рівнів – від відомчого до корпоративного – і гарантує те, що критично важливі бізнес-процеси зможуть тривати, а своєчасне відновлення основних бізнес-функцій буде реалізовано.

Всі дії в аварійних / надзвичайних ситуаціях необхідно ретельно документувати і затверджувати. Для цього необхідно створити документ (план), що описує заходи, які необхідно вжити в разі часткової чи повної відмови КС.

План забезпечення безперервності бізнесу та аварійного відновлення (далі – План) забезпечує альтернативні процедури, які будуть виконуватися персоналом для заміни відсутніх функціональних можливостей КС і забезпечення безпечної роботи бізнес-процесів під час збою, а також включає комплекс технічних і організаційних заходів щодо зниження ризиків переривання бізнесу в разі виникнення надзвичайної ситуації. Заходи можуть варіюватися від запланованого скорочення апаратного обладнання до переходу в систему з паперовими носіями інформації. Документ визначає кроки, необхідні для відновлення бізнес-процесів після порушення і, за необхідності, як проходить керування даними, отриманими під час порушення, ролі і обов'язки персоналу, необхідний процес передачі інформації, а також визначає схеми для запуску Плану в дію [5, с. 187].

Там, де для продовження роботи бізнес-процесів застосовується інтерактивне внесення інформації, необхідно розглянути, як будь-які пов'язані електронні записи або дані будуть синхронізуватися відразу після відновлення КС.

План створюється на основі аналізу бізнес-процесів компанії. Специфіка Плану залежить від критичних для бізнесу процесів і необхідного рівня їх стійкості до аварійних / надзвичайних ситуацій. Основний критерій Плану – час, у рам-

ках якого КС буде відновлена і підготовлена до роботи.

Найбільш важливими факторами, що забезпечують успіх планування, є облік усіх дрібниць і поетапна розробка кожного невеликого елемента Плану.

Етапи створення Плану:

- дослідження;
- розробка;
- впровадження;
- тестування.

Під час підготовки Плану необхідно провести аналіз існуючих для компанії ризиків, визначаючи важливі питання безпеки КС. Ризики, пов'язані з недоступністю даних, призводять до уповільнення бізнес-процесів. Критичні функції КС, що підтримують ці процеси, повинні бути виявлені і також мають бути оцінені ризики для кожного з них [6, с. 229; 7, с. 7; 8, с. 26].

Планування дій у надзвичайній ситуації включає регулярне тестування (випробування), оцінку ефективності Плану забезпечення безперервності бізнесу та аварійного відновлення для підтвердження його працездатності в умовах, що змінюються, і корекцію. На процес формування і тестування впливають часті зміни обладнання, програм і документації. План забезпечення безперервності бізнесу та аварійного відновлення – це документ, що постійно змінюється. План тестується одним із методів, наприклад, за допомогою періодичних оглядів КС, мозкового штурму, покрокових інструкцій (СОПів), тестування розділів Плану, перевстановлення сервера, переходу на резервний вузол і повного тестування.

Безперервність бізнесу неможливо чітко визначити в системі роботи компанії та прив'язати до якоїсь певної функції. Це комплексні заходи, виконання яких залежить від усіх залучених співробітників – служби безпеки інформаційних технологій, інформаційної безпеки, логістики, персоналу та іншого. Важливо пам'ятати, що без прямого залучення власників бізнес-процесів Плани матимуть лише теоретичне значення і у разі кризової ситуації можуть лише завадити, а не виконувати свою основну функцію – забезпечувати та реалізовувати безперервність бізнесу компанії.

Добре підготовлений План забезпечує компанії покрокові інструкції, що відповідають типу і тяжкості ситуації, що виникла. У ньому вказуються функціональні групи фахівців компанії, підготовлені для реалізації Плану. Документ включає в себе максимально докладний опис дій персоналу в разі будь-якої аварійної / надзвичайної

ситуації, яка може статися. Це може бути, наприклад, відмова обладнання, зависання важливих сервісів, вірусні і хакерські атаки, масштабні природні і техногенні аварії тощо. Організація процесів аварійного відновлення функціонування КС повинна бути стратегією всієї компанії, а не тільки власника КС (системного адміністратора). Керівники всіх підрозділів, діяльність яких залежить від послуг, що надаються КС, розробляють процедури дій у надзвичайних обставинах, а також беруть участь у розробці Плану. Кожний функціональний підрозділ «запускає» частину Плану в рамках загальних зусиль з відновлення діяльності КС. Важливим моментом у процесі складання Плану є участь вищого керівництва компанії, відповідального за надання ресурсів і визначення балансу між інвестиціями в інформаційні технології і часом простою втратою даних у разі збою. Обов'язком керівництва підприємства є (в тому числі власників процесів, власника Системи і департаменту Якості) гарантування, що відповідний документ «План забезпечення безперервності бізнесу та аварійного відновлення», розроблений і впроваджений, буде періодично перевірятися і відразу після початку впровадження його вимогам буде слідувати персонал структурних підрозділів і аналізувати відповідність вимог Плану корпоративній стратегії компанії і нормативним вимогам.

У Плані має бути відображено навіть виконання таких забезпечуючих функцій, як утримання будівель і устаткування. Ефективність виконання цих функцій може не впливати безпосередньо на роботу ІТ-інфраструктури, проте від неї буде частково залежати відновлення роботи технічних засобів.

Документ «План забезпечення безперервності бізнесу та аварійного відновлення» є не тільки технічним планом – він передбачає проведення організаційних заходів. Тому в основу Плану покладені відомості про структуру та функції компанії, кошти, необхідні для підтримки її діяльності, величину збитку від неможливості нормального функціонування, персонал, який прийме на себе управління в кризовій ситуації, і процедури, які будуть використовувати.

План включає докладні інструкції з переключення на резервні канали зв'язку, використання резервних потужностей, резервування та відновлення інформації, необхідної для роботи, перелік та методику дій з ліквідації наслідків надзвичайної ситуації, а також план тренувальних і тестувальних заходів для персоналу та керівництва.

Аналіз літературних джерел та практичні підходи дозволили автору сформулювати основні розділи Плану та короткий їх зміст.

Першим розділом має бути вступ, в якому викладено мету, завдання, основні положення документу. Формулювання повинні бути чіткими і конкретними.

Другий розділ – це оцінка надзвичайної / аварійної ситуації. Цей розділ описує чинники ризику і заплановані заходи щодо їх контролю, а саме: опис несприятливих подій і небезпеки (кризові ситуації), які можуть негативно вплинути на функціонування КС. Тут доцільним буде провести класифікацію можливих несприятливих подій і небезпек (наприклад, загрозлива, серйозна, що вимагають уваги ситуації), оцінку ймовірності їх виникнення. Коротко описати перелік критеріїв для визначення несприятливих подій і небезпек, а також їх потенційні джерела. Сценарії кризових ситуацій, визначення можливого збитку (у разі потреби). Необхідно провести й описати оцінку остаточних ризиків.

Третій розділ – діяльність у кризовій ситуації. Розділ описує необхідні ресурси і умови для аварійного відновлення. Під час його формування необхідно описати пріоритетні бізнес-процеси компанії, скласти перелік внутрішніх і зовнішніх ресурсів (наприклад, технічні засоби, програмне забезпечення, засоби зв'язку, документи); внести облікову інформацію про технічне, програмне та інше забезпечення, що необхідне для відновлення бізнесу компанії в разі кризової ситуації, контактну інформацію (наприклад, список осіб, яких необхідно сповістити про кризову ситуацію із зазначенням адрес і телефонів). У разі дії SLA-угоди (угоди про рівень надання послуги постачальником КС) – вказати координати зовнішнього підрядника.

Четвертий розділ – організаційні ресурси. Необхідно визначити необхідні ресурси та умови для аварійного відновлення.

П'ятий розділ – технічне забезпечення. Розділ описує заходи щодо створення і підтримки бази технічних засобів, що забезпечує безперебійну діяльність КС у надзвичайній / кризовій ситуації.

Шостий розділ – тестування Плану. Необхідно описати порядок проведення випробувань плану, при цьому вказати, наприклад:

- що підлягає випробуванням під час перевірки реалізації Плану;
- хто повинен проводити випробування;
- коли повинні здійснюватися випробування;
- результати випробувань.

План тестування може бути загальним або складатися з окремих частин. Деякі розділи цього плану можуть бути розділами інших загальних планів.

В останньому розділі з робочою назвою «Порядок перегляду плану» необхідно вказати терміни перегляду плану (наприклад, плановий, частковий, повний).

План повинен бути створений для кожної впровадженої КС у компанії і повинен охоплювати не тільки процес відновлення системи, але і будь-якої інфраструктури, необхідної для функціонування системи.

На думку автора, створення Плану не підміняє собою систему резервного копіювання, він лише надає їй додатковий функціонал у частині критично важливих інформаційних ресурсів і цілий комплекс процедур, необхідних для того, щоб забезпечити постійний доступ до інформаційних ресурсів компанії.

Висновки. З огляду на викладене забезпечення безперервності бізнесу є важливим фактором ефективного функціонування фармацевтичної компанії. Разом з тим не всі аспекти цієї проблеми знайшли досить повне вивчення. Зокрема, є необхідність пошуку більш ефективних управлінських рішень з забезпечення безперервності бізнесу, що включають: облік нових викликів і ІТ-загроз, підвищення обізнаності персоналу, сертифікації планів безперервності бізнесу та впровадження системи менеджменту безперервності бізнесу, що дасть можливість відповідати корпоративним вимогам і враховувати специфічні ризики фармацевтичної галузі. Дані тенденції приводять до появи нових підходів в управлінні, пов'язаних з забезпеченням безперервності діяльності ІТ-залежного бізнесу.

Список літератури:

1. Фабрис Ж. Валідація комп'ютеризованих систем в контексті GMP. *Аптека*. 2012. № 30 (851). С. 10–11.
2. Зборовська Т.В. Обґрунтування актуальності впровадження стандарту ISO 22301 у фармацевтичному секторі України. *Управління, економіка та забезпечення якості в фармацевтиці*. 2017. № 2 (50). С. 4–10.
3. Борсуковська В.Ю. Борсуковський Ю.В. Безперервність бізнесу: новий тренд або необхідність. *Економіка. Менеджмент. Бізнес*. 2017. № 2 (20). С. 48–53.
4. СТ-Н МОЗУ 42-4.0:2016. Лікарські засоби. Належна виробнича практика. Київ, 2016. 358 с.
5. GAMP 5. Good Automated Manufacturing Practice. International Society for Pharmaceutical Engineering. 2011. 196 p.
6. Портянко Т.М., Кучеренко В.С. Особливості управління ризиками при впровадженні комп'ютеризованих систем на фармацевтичних підприємствах. *Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки*. 2018. № 6. Том 29 (68) Ч. 1. С. 228–333.
7. СТ-Н МОЗУ 42-4.2:2011 (ICH Q9). Лікарські засоби. Управління ризиками для якості. Київ, 2011. 36 с.
8. ISO 31000:2009. Risk management. Principles and guidelines. International Organization for Standardization. 2018. 32 p.

Portianko T.M., Kucherenko V.S. THE ROLE OF THE BUSINESS CONTINUITY PROTECTION PLAN IN THE IMPLEMENTATION OF COMPUTERIZED SYSTEMS AT PHARMACEUTICAL ENTERPRISES

Ensuring business continuity is one of the most important strategic directions for the development of any company. In accordance with the requirements of the documentation regulating the introduction of computerized systems (hereinafter, CP) at pharmaceutical enterprises, ensuring business continuity is due to the need to maintain the stability and stability of CP operation in various conditions of adverse influence of external and internal factors of technogenic and/or natural character on the business processes of the company. Patient safety, product quality and data integrity should not be adversely affected by malfunctions or breakdowns during any CP operation. Business Continuity Management includes disaster recovery, which covers the technical upgrading of the COP and contains the procedures for staff to restore critical IT services. All alarm / emergency operations must be carefully documented and approved. In order to implement the aforementioned, one shall create a document (plan) describing the steps to be taken in the event of a partial or total failure of the CP. The article describes practical approaches to creating a Business Continuity and Disaster Recovery Plan (hereinafter, the Plan), taking into account the specifics and regulatory requirements for pharmaceutical manufacturing. Measures that can range from scheduled hardware reductions to transition to the system with paper information carriers, and the like, are displayed. The article highlights how the Plan defines how companies' business processes continue to function and process data after a malfunction in the CP. Particular attention is given to sections of the Plan, which outline the steps required to restore business processes after a breach and, where appropriate, how the data obtained during a breach, the roles and responsibilities of staff, the process of information transfer, and how to define a scheme for launching the Plan into action. Its necessity is identified and substantiated where, in order to continue the business processes, an interactive input of information is used, as any electronic records or data will be synchronized immediately after the restoration of the CP. The article focuses on contingency planning, including regular testing (trial), evaluating the effectiveness of the Plan to confirm its performance under changing conditions, and its correction.

Key words: threats, emergencies, business processes, patient safety, business continuity plan, computerized system.