Наталья И. Касперская[1], Василий В. Кузьменко[2], Дмитрий А. Мананников[3],
Рустем Н. Хайретдинов[4], Андрей Ю. Щербаков[5]
[1, 2, 4] Группа компаний InfoWatch,
Верейская ул., 29, стр. 134, г. Москва, 121357, Россия
[1]Московский институт электроники и математики им. А.Н.Тихонова НИУ ВШЭ
Таллинская ул., 34, г. Москва, 123458, Россия
[2]ООО КБ «Нэклис-Банк»
Никитская Б. ул., 17, стр. 2, г. Москва, 125009, Россия
[3]Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации
Проспект Вернадского, 84, г. Москва, 119571, Россия
[5]Центр развития криптовалют и цифровых финансовых активов ВИНИТИ
Усиевича ул., 20, г. Москва, А-190, 125190, Россия
[1]e-mail: natalya.kaspersky@infowatch.com, https://orcid.org/0000-0002-5205-679X
[2]e-mail: vasily.kuzmenko@infowatch.com, https://orcid.org/0000-0002-5042-2012
[3]e-mail: dmitriy@manannikov.ru, https://orcid.org/0000-0003-1116-7028
[4]e-mail: rustem.khairetdinov@infowatch.com, https://orcid.org/0000-0002-3391-7646
[5]e-mail: a.shcherbakov@c3da.org, https://orcid.org/0000-0002-1593-6704

К ПРОБЛЕМЕ ОЦЕНКИ И ОБЕСПЕЧЕНИЯ КОРРЕКТНОСТИ БИЗНЕС-ПРОЦЕССОВ

DOI: http://dx.doi.org/10.26583/bit.2019.3.01

Аннотация. В современных условиях можно констатировать, что классические методы обеспечения информационной и технологической безопасности, связанные с формулированием политики безопасности для разрабатываемой и внедряемой информационной системы, утрачивают ценность и эффективность, поскольку отстают от развития собственно информационных технологий, не вписываются в скорости обновления программного обеспечения и изменение потребностей пользователей. Для решения этих проблем рассмотрено понятие бизнес-процесса как целевой функции, реализованной информационной (компьютерной) системой, введено понятие корректности («здоровья») бизнес-процесса. На основе субъектно-объектной модели компьютерной системы предложена математическая модель здорового бизнес-процесса как траектории или семейства желательных траекторий в состоянии информационной системы. На основе данной модели предложены непротиворечивые практические реализации платформы обеспечения здоровья бизнес-процесса как совокупность интерфейса, отображающего показатели здоровья бизнес-процесса, отчеты, оповещения, предикты (предсказатели или экстраполяторы в виде формальных выражений), коррелятора – ядра платформы, контролирующего логику и содержащее в себе информационные модели, паттерны (образцы траекторий), правила реагирования на события, базы хранения данных бизнес-процесса и коннектора, осуществляющего нормализацию данных бизнес-процесса. С точки зрения системно-аналитического подхода эта платформа представляет собой информационно-аналитическую систему, формирующую новое свойство – здоровье бизнес-процесса, направленное на снижение ресурсных потерь посредством выявления и предотвращения нарушений (в частности, киберпреступлений и мошенничества) на уровне процесса, а также формирования контрольной среды бизнес-процесса. Приведен практический пример обеспечения здоровья бизнес-процесса для логистической системы. Предложен новый универсальный методологический подхода к оценке и обеспечению корректности функционирования бизнес-процессов на основе новой парадигмы доверия (корректности) субъектно-объектной модели бизнес-процесса и понятия здоровья бизнес-процесса, предложена концепция платформы обеспечения здоровья бизнес-процесса. Результаты работы могут широко использоваться для проектирования и оценки систем технологического и финансового профиля.

Ключевые слова: бизнес-процесс, доверие, модель бизнес-процесса, здоровье бизнес-процесса, контрольная точка, зрелость, платформа, метрика здоровья бизнес-процесса, субъектно-объектная модель, логистика, информационные артефакты.
Для цитирования: КАСПЕРСКАЯ, Наталья И. et al. К ПРОБЛЕМЕ ОЦЕНКИ И ОБЕСПЕЧЕНИЯ КОРРЕКТНОСТИ БИЗНЕС-ПРОЦЕССОВ. Безопасность информационных технологий, [S.l.], v. 26, n. 3, p. 8-21, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1213>. Дата доступа: 11 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.01.

Natalya I. Kasperskaya[1], Vasily V. Kuzmenko[2], Dmitry A. Manannikov[3],
Rustem N. Khairetdinov[4], Andrey Yu. Shcherbakov[5]
[1, 2, 4]Group of companies InfoWatch,
Vereyskaya str., 29, building 134, Moscow, 121357, Russia
[1]Moscow Institute of electronics and mathematics. A. N. Tikhonov HSE
Tallinn str., 34, Moscow, 123458, Russia
[2]Bank "Neklis-Bank"
Nikita Big str., building 17, Moscow, 125009, Russia
[3]RANEPA - National School of Public and Business Administration
Prospect Vernadskogo, 84, Moscow, 11957, Russia
[5] Center for development of cryptocurrency and digital of financial assets VINITI
Usievich str., 20, Moscow, A-190, 125190, Russia
[1]e-mail: natalya.kaspersky@infowatch.com, https://orcid.org/0000-0002-5205-679X
[2]e-mail: vasily.kuzmenko@infowatch.com, https://orcid.org/0000-0002-5042-2012
[3]e-mail: dmitriy@manannikov.ru, https://orcid.org/0000-0003-1116-7028
[4]e-mail: rustem.khairetdinov@infowatch.com, https://orcid.org/0000-0002-3391-7646
[5]e-mail: a.shcherbakov@c3da.org, https://orcid.org/0000-0002-1593-6704

To the problem of assessing and ensuring the correctness of business processes

DOI: http://dx.doi.org/10.26583/bit.2019.3.01

Abstract. In modern conditions, it can be stated that the classical methods of information and technological security related to the formulation of security policy for the developed and implemented information system lose value and efficiency, because they lag behind the development of information technology itself, do not fit into the speed of software updates and changing user needs. To solve these problems, the concept of the business process as a target function implemented by the information (computer) system is considered, the concept of correctness ("health") of the business process is introduced. Based on the subject-object model of a computer system, a mathematical model of a healthy business process as a trajectory or a family of desirable trajectories in the state of an information system is proposed. Based on this model, we propose consistent practical implementation of the platform to ensure the health of the business process as a set of interface that displays indicators of the health of the business process, reports, alerts, predicates (predictors or extrapolators in the form of formal expressions), the correlator – the core of the platform that controls the logic and contains information models, patterns (sample trajectories), the rules of response to events, the database storage of the business process and the connector that normalizes the data of the business process. From the point of view of the system-analytical approach, this platform is an information-analytical system that forms a new property – the health of the business process, aimed at reducing resource losses by identifying and preventing violations (in particular, cybercrime and fraud) at the process level, as well as the formation of the control environment of the business process. There is also a practical example of ensuring the health of the business process for the logistics system. Thus, a new universal methodological approach to assessing and ensuring the correct functioning of business processes on the basis of a new paradigm of trust (correctness) of the subject-object model of the business process and the concept of health of the business process is proposed, the concept of a platform for ensuring the health of the business process is proposed.

The results of the work can be widely used for the design and evaluation of systems of technological and financial profile.
Keywords: the business process, the trust model of the business process, the health of the business process, a reference point, the maturity of the platform, the metric of the health of the business process, subject-object model, logistics, information artifacts.
For citation: KASPERSKAYA, Natalya I. et al. To the problem of assessing and ensuring the correctness of business processes. IT Security (Russia), [S.l.], v. 26, n. 3, p. 8-21, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1213>. Date accessed: 11 sep. 2019. doi:http://dx.doi.org/10.26583/bit.2019.3.01.

Введение

Современная организация бизнеса построена на использовании информационных технологий, систем и сервисов. От их эффективного использования в бизнес-процессе зависят в первую очередь его ключевые показатели. Сегодня очевидна тенденция – эффективность бизнес-процессов зависит не только от нормального функционирования информационно-телекоммуникационной инфраструктуры, на которой они реализованы, но и от того, насколько правильно процесс выстроен с точки зрения безопасности, ведь несовершенство состояния безопасности, равно как и отклонения от стандартного выполнения операционной деятельности, может привести к ущербу для организации.

Современные подходы к организации безопасных и доверенных бизнес-процессов (термины «безопасность» и «доверенность» будут раскрыты и формализованы ниже) испытывают определенный кризис [1]. Это в первую очередь связано с тем, что классические подходы к реализации свойств безопасности и доверенности основаны либо на методиках аудита (когда изучается алгоритмика бизнес-процесса и сравнивается с некоторым внешним эталоном), либо на методиках соответствия регламентам или политиках безопасности (в этом случае бизнес-процесс проверяется на соответствие некой априорно заданной политике безопасности).

Причины кризиса данных подходов объясняются следующими факторами:

- высокой изменчивостью и динамичностью развития, как самих бизнес-процессов, так и платформ, на которых они реализованы;
- отставанием формальных моделей обеспечения доверенности и безопасности от реальности;
- недостаточным осознанием управляющим персоналом и пользователями проблемы безопасности бизнес-процесса как системно-аналитической сущности.

Таким образом, можно сделать вывод, что подходы «статического» плана, когда заранее формулируется безопасная модель или регламент бизнес-процесса, вступают в диалектическое противоречие с реальностью, не успевают ни за изменчивостью бизнес-процесса, ни за изменением его целей.

Следовательно, необходимо переходить к динамической модели обеспечения безопасности и доверенности бизнес-процесса, когда оцениваются понятия и показатели его изменчивости в некоторые моменты времени и отклонения от некоторых нормальных или «здоровых» состояний. Данный подход апеллирует к опыту построения безопасных технических систем, например, газотурбинных установок, когда мерами безопасности бизнес-процесса в его технологическом понимании является сохранение набора параметров, гармоничных для технической системы и тесно связанных с понятиями технологического смысла и эффективности (температура, давление, вибрации).

Используя понятия ведомственного стандарта Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации [2], перечислим базовые определения, касающиеся безопасности бизнес-процессов.

Риск – мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.

Актив – все, что имеет ценность для организации и находится в ее распоряжении.

К активам организации могут относиться:

- работники (персонал), финансовые (денежные) средства, средства вычислительной техники, телекоммуникационные средства и пр.;
- различные виды информации – платежная, финансово-аналитическая, служебная, управляющая, персональные данные и др.;
- бизнес-процессы и технологические процессы;
- продукты и услуги, предоставляемые клиентам.

Информационный актив – информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для организации либо находящаяся в распоряжении организации и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

Объект среды информационного актива – материальный объект среды использования и (или) эксплуатации информационного актива (объект хранения, передачи, обработки, уничтожения и т.д.).

Ресурс – актив организации, который используется или потребляется в процессе выполнения некоторой деятельности.

Точка (область) риска – область с высокой вероятностью совершения инцидента безопасности и нарушения операционной деятельности предприятия.

В качестве методической основы для повышения эффективности бизнес-процессов, обеспечения их доверенности и безопасности используются методические материалы по реагированию на инциденты информационной безопасности (ИБ) [2].

1. Понятие бизнес-процесса

Приведем два определения бизнес-процесса (далее – БП или бизнес-процесс).

1. Бизнес-процесс – несколько связанных работ или процедур, в совокупности реализующих конкретную цель текущей деятельности в рамках существующей организационной структуры [3].

2. Бизнес-процесс в информационной системе – совокупность информационных потоков и данных, реализующая заданный и описанный внешними регламентациями бизнес-процесс.

Существуют три основных вида бизнес-процессов – управляющие, операционные и поддерживающие.

Управляющие – БП, которые управляют функционированием системы. Примером управляющего процесса может служить корпоративное управление и стратегический менеджмент.

Операционные – БП, которые составляют основной бизнес компании и создают основной поток доходов. Примеры операционных бизнес-процессов: снабжение, производство, маркетинг, продажи.

Поддерживающие – БП, которые обслуживают основной бизнес. Например, бухгалтерский учет, подбор персонала, техническая поддержка, административно-хозяйственный учет, аналитика.

Бизнес-процесс начинается с фиксации спроса потребителя в материальной форме и заканчивается его удовлетворением.

С точки зрения системного анализа можно изобразить схему бизнес-процесса в виде «черного ящика» с тремя входами и одним выходом (рис.1).

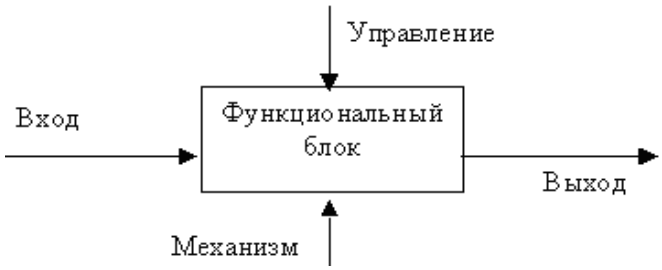

Рис. 1. Схема бизнес-процесса
(Fig. 1. Business process diagram)

БП может быть декомпозирован на несколько подпроцессов, процедур и функций, имеющих собственные атрибуты, но при этом направленных на достижение цели основного БП. Такой анализ бизнес-процессов обычно включает в себя составление карты БП и его подпроцессов, разнесенных между определенными уровнями активности.

Бизнес-процессы должны быть построены таким образом, чтобы создавать стоимость и ценность для потребителей (владельцев, создателей) данных бизнес-процессов, а также исключать любые необязательные или лишние активности [4-7]. На выходе «правильно» построенных бизнес-процессов увеличивается ценность товаров и услуг для потребителя и рентабельность (за счет уменьшения себестоимости производства товара или услуги).

БП могут подвергаться различному анализу в зависимости от целей моделирования. Например, при бизнес-моделировании, функционально-стоимостном анализе, формировании организационной структуры, реинжиниринге бизнес-процессов, автоматизации технологических процессов.

Один из методов анализа текущей деятельности – составление модели бизнес-процесса «как есть» (*as is*), т.е. описание последовательности действий по определенному выбранному направлению деятельности. Полученная модель БП подвергается критическому изучению или обрабатывается специальным программным обеспечением. По результатам анализа формируется модель бизнес-процесса «как будет» (*to be*) и план мероприятий по внедрению необходимых изменений.

Существует несколько нотаций, применяемых для описания и моделирования бизнес-процессов, например:

BPMN (*Business Process Model and Notation* – нотация и модель бизнес-процессов) – служит для отображения функциональной последовательности работ в виде диаграмм бизнес-процессов, понятных бизнес-аналитикам, техническим специалистам и другим бизнес-пользователям;

EPC (*Event-driven process chain* – событийная цепочка процессов) – блок-схема, представляющая упорядоченную логически взаимосвязанную событийную последовательность действий для получения желаемого результата;

IDEF0 (*Integration Definition for Process Modelling* – функциональное моделирование бизнес-процессов) – графическая нотация, описывающая функции системы и логические связи между ними и внешней средой.

Описание бизнес-процесса – это фиксация последовательности действий при его выполнении с целью их анализа и оптимизации, а также улучшения свойств БП (в частности, безопасности и доверенности) и повышения его качества [8, 9].

2. Математическая модель компьютерной системы и бизнес-процесса. Понятие здоровья бизнес-процесса

В современной информатике **модель компьютерной системы** (КС) чаще всего рассматривается в виде **совокупности элементов**, которые можно разделить на два подмножества: множество **объектов** и множество **субъектов** [9-12].

В любой системе с точки зрения системного анализа выделяются существенные для ее качественной определенности части, подсистемы или компоненты. В случае компьютерной системы компонентами будут субъекты и объекты. Разделение компонент на субъекты и объекты в компьютерной системе основывается на свойстве компонента «быть активным» или «получить управление», т.е. субъектами в компьютерной системе являются программы, а объектами – данные.

Передача или поток информации от одного объекта к другому происходит по инициативе субъекта, поэтому в соответствии с [9] введем формальное определение. **Потоком информации** между объектом O_m и объектом O_j называется произвольная операция над объектом O_j, реализуемая в субъекте S_i и зависящая от O_m.

Обозначения: $\boldsymbol{Stream}(S_i, O_m) \rightarrow O_j$ – поток информации от объекта O_m к объекту O_j.

Изменение и порождение новых объектов компьютерной системы (т.е. появление в компьютерной системе новых программ) производится субъектом как активной компонентой, управляемой пользователем через органы управления.

Соответственно вводится понятие порождения субъекта [9] $\boldsymbol{Create}(S_j,O_i) \rightarrow S_k$ – из объекта O_i порожден субъект S_k при активизирующем воздействии субъекта S_j. ***Create*** назовем операцией порождения субъектов.

Тогда с точки зрения субъекто-объектной модели **бизнес-процесс** представляет собой последовательность матриц состояний декартова произведения множества субъектов на множество объектов $<S,O>t$, где t – моменты времени или контрольные точки бизнес-процесса, т.е. такие моменты времени, в которых матрица состояний подвергается сравнению с заданными эталонными значениями либо проверяется на выполнение некоторых свойств. В данном случае полагаем, что бизнес-процесс реализован в рамках компьютерной системы.

Введем также следующее определение. Бизнес-процесс является доверенным (корректным) или здоровым, когда последовательность матриц состояний не выходит за пределы априорно установленных значений для всех моментов времени или в контрольных точках, а потоки в моменты t обусловлены логикой бизнес-процесса. Например, процесс увеличения кредитного лимита в банке выполняется каждым субъектом на своем шаге – приемщиком заявки, кредитным оператором, администратором смены; появление потока от субъекта не своего шага является недоверенным (нездоровым).

Этим определением задается также методология установления здоровья бизнес-процесса:

- бизнес-процесс есть совокупность изменения объектов субъектами в некоторые моменты времени;
- его текущий ход (траектория БП) описывается матрицей состояний $<S,O>t$;
- матрица состояний может быть проверена на соответствие некоторым внешним и/или внутренним правилам, и эта проверка позволяет сделать вывод о здоровье или нездоровье бизнес-процесса (можно сформулировать эквивалентное положение о том, что матрица состояний должна соответствовать желательной траектории).

Итак, мы перешли от статичной модели к динамической, которая ниже будет проиллюстрирована конкретным примером. В первую очередь бизнес-процесс должен

быть обследован на предмет формирования матрицы его состояний в удобном для восприятия и последующей реализации виде. Задача обследования направлена на выявление угроз безопасности индивидуально для каждого БП, на определение оценки эффективности обеспечения его здоровья и безопасности, выявление «точек риска» (областей с высокой вероятностью совершения инцидента безопасности и нарушения операционной деятельности).

Работы по обследованию включают в себя анализ информационных активов бизнес-процессов на предмет выявления чувствительной информации и определения критериев ее легитимной обработки, изучение основного функционала и ролей доступа в используемых информационных системах и сервисах, построение информационных моделей бизнес-процессов с выделением проблемных областей – «точек риска», моделирование в них угроз безопасности и нарушения операционной деятельности, подготовку мероприятий по их устранению за счет формирования непрерывной контрольной среды.

Второй важный момент наряду с обследованием бизнес-процесса – формулирование технического механизма контроля, предусматривающего в первую очередь накопление данных, а затем их анализ исходя из результатов обследования.

Для обеспечения непрерывного контроля безопасности функционирования бизнес-процессов предлагается создание системы, осуществляющей агрегацию, корреляцию и анализ собранных на этапе обследования данных для определения отклонения бизнес-процесса от описанной информационной модели (возникновение нестандартных событий, которые могут указывать на потенциальное киберпреступление, внутреннее мошенничество или другие бизнес-риски). Делается это с целью обозначения отклонения траектории бизнес-процесса от желаемой. Разработка такой системы направлена на автоматизированное непрерывное обеспечение контрольной среды, выявление и мониторинг девиантных состояний, потенциально свидетельствующих о возможных нарушениях внутри контролируемого бизнес-процесса.

3. Цели обеспечения здоровья бизнес-процессов

Основная цель обеспечения здоровья бизнес-процесса заключается в снижении потерь (т.е. в предотвращении снижения коэффициента эффективности или полезного действия бизнес-процесса) в его рамках, как прямых – в случае реализации инцидентов информационной безопасности и внутреннего мошенничества, так и косвенных – в случаях отхождения бизнес-процесса от описанной модели (снижение доверенности, качества, эффективности) за счет обеспечения прозрачности информационных потоков бизнес-процессов, выявления, сквозного контроля или устранения всех «точек риска» в каждом из функционирующих в организации бизнес-процессов.

Согласно [13], **доверие** – свойство системы, объективно, обоснованно и документально выраженное основание того, что элемент системы (в терминах стандартов – изделие информационных технологий, информационный продукт, информационно-телекоммуникационная система, ее компоненты, бизнес-процесс в целом) отвечает априорно заданной (регламентациями высшего уровня) целевой функции на всем протяжении своего жизненного цикла и во всех режимах функционирования. Исходя из этого определения, понятие доверия включают в понятие здоровья.

По уровню защищенности разделим бизнес-процессы на: базово-защищенные – безопасность поддерживается на необходимом базовом уровне за счет применения штатных средств обеспечения информационной безопасности; уверенно-защищенные – безопасность поддерживается на необходимом уверенном уровне за счет применения

отечественных средств обеспечения информационной безопасности; высокозащищенные – безопасность поддерживается на необходимом высоком уровне за счет применения отечественных сертифицированных (рекомендованных, аттестованных) средств. По уровню доверенности бизнес-процессы можно разделить на базово-доверенные, среднедоверенные и высокодоверенные.

Высокая защищенность и доверенность подразумевают использование средств обеспечения информационной безопасности отечественной разработки, собственное управление ими (отсутствие аутсорсинга), проведение аудита и аттестации.

4. Платформа обеспечения здоровья бизнес-процесса

Для решения задачи обеспечения здоровья бизнес-процесса рассмотрим понятие платформы обеспечения здоровья БП.

С точки зрения системно-аналитического подхода платформа обеспечения здоровья БП представляет информационно-аналитическую систему, формирующую новое рассмотренное выше свойство – «здоровье БП», направленное на снижение ресурсных потерь посредством выявления и предотвращения нарушений (в частности, киберпреступлений и мошенничества) на уровне бизнес-процесса, а также формирования его контрольной среды.

Архитектура такой платформы включает компоненты:

- интерфейс – визуальный компонент платформы, отображающий показатели здоровья БП, отчеты, оповещения, предикты (предсказатели или экстраполяторы в виде формальных выражений);
- коррелятор – ядро платформы, контролирующее логику БП и содержащее в себе информационные модели, паттерны (образцы траекторий), правила реагирования;
- БД – базу хранения данных бизнес-процесса;
- коннектор – пассивный компонент, осуществляющий нормализацию и парсинг данных бизнес-процесса. Может принудительно запрашивать данные БП, не вмешиваясь в его логику и/или его данные.

Платформа через коннекторы к компьютерной системе и сервисам собирает весь объем информационных артефактов, используемых в рамках БП. Информационные артефакты приводятся к единому формату, сохраняются в базе данных и индексируются для обеспечения возможности онлайн-поиска и запросов. Коррелятор (в соответствии с загруженными в него информационными моделями БП) выполняет наложение паттернов процессов на базу информационных артефактов и фиксирует все возможные отклонения. Интерфейс системы формирует отчеты и оповещения об отклонениях, а также поддерживает процедуры обеспечения безопасности.

Измеряемыми результатами внедрения платформы являются: существующие индикаторы эффективности бизнес-процесса и его «здоровья», БП – индикатор, определяющий устойчивость к нарушениям в рамках этого БП.

Методология обеспечения безопасности бизнес-процесса базируется на обоснованных утверждениях:

- нарушением в БП является любое отклонение от заданной логики (желательной траектории БП);
- БП существует на уровне событий информационных систем независимо от степени формализации заданной логики;
- правила, устанавливаемые заданной логикой БП, однозначно идентифицируются набором взаимосвязанных событий и данных в информационных системах.

Приведенные утверждения лежат в основе построения информационной модели бизнес-процесса – фундаментальной задачи в рамках обеспечения его безопасности, решаемой платформой обеспечения здоровья БП.

Информационная модель является частью платформы и представляет совокупность трех уровней информационной модели БП. Первый уровень информационной модели БП – логический. Служит для фиксации заданной логики БП: взаимосвязи этапов, процедур, логических событий и т.д. Исходно логика БП может быть задана как формализовано – в рамках утвержденного документа в формате одной из существующих международных схем, так и не формализовано – в виде каких-либо инструкций и общепринятых правил.

Второй уровень – информационный. Определяет совокупность событий и данных в информационных системах (с учетом временных интервалов создания этих событий), отвечающих заданной логике БП – паттерн информационных артефактов, соответствующий траектории в виде событий информационной системы (выше говорили о совокупности потоков и порождений субъектов). Поскольку одним из основных и неотъемлемых ресурсов бизнес-процессов является человек – пользователь соответствующих информационных систем, среди паттернов информационных артефактов выделяются паттерн БП и паттерн пользователя. Паттерн БП не зависит от конкретного пользователя и является общим для процесса. Паттерн пользователя соответствует конкретному пользователю, выполняющему процесс (процесс соответствует субъекту). Информационный уровень напрямую связан с логическим и формируется на основе анализа логов информационных систем, которые генерируются каждым отдельным логическим событием БП (зафиксированным на первом уровне).

Третий уровень – корреляционный. Определяет перечень и состав контрольных точек БП.

Контрольная точка – взаимосвязь логических блоков БП, правил их выполнения и требований к результатам, а также соответствующий им набор событий и данных в информационных системах, являющихся частью паттерна информационных артефактов. Совокупность контрольных точек БП и взаимосвязанных с ними логических блоков и правил, событий и данных в информационных системах формируют модель корреляции – один из основных элементов, входящих в состав информационной модели БП.

Метод обеспечения безопасности бизнес-процессов на основе построенной информационной модели базируется на возможности выявлять нарушения в процессах по их следам в информационной инфраструктуре. Опишем его суть.

- Нарушения выявляются сравнением фактической логики выполнения БП (т.е. отдельной итерации) с заданной логикой.
- Так как заданная логика однозначно определяется паттерном информационных артефактов, то наложение паттерна на их текущую базу покажет отклонения фактической логики выполнения бизнес-процесса (отдельной итерации) от заданной. В зависимости от необходимой степени детализации в качестве паттерна информационных артефактов можно использовать либо паттерн БП, либо паттерн пользователя БП. В последнем случае следует более точно задать границы логики, соответствующие выполнению бизнес-процесса определенным пользователем с учетом особенностей его работы в конкретных информационных системах, и тем самым выявлять нарушения, связанные с подменой пользователя.
- Использование модели корреляции при наложении паттерна БП/пользователя БП на текущую базу информационных артефактов позволяет на уровне логов информационных систем сформировать предикты (выражения, описывающие экстраполяцию состояний) по возможным отклонениям и, соответственно, предотвратить

нарушения в бизнес-процессе – реализовать контрольную среду. Информационная модель БП позволяет автоматизировать выявление и предотвращение нарушений на основе платформы обеспечения здоровья БП: информационный и корреляционный уровни формируют логику работы платформы, логический уровень — является интерфейсом между внутренней логикой работы платформы и оператором/пользователем платформы.

Алгоритм обеспечения безопасности БП представляет непрерывный цикл, включающий указанные выше три шага. Непрерывность этого цикла обеспечивается, с одной стороны, функционирующей платформой обеспечения здоровья БП, с другой – процессом обеспечения безопасности БП, реализуемым в компании.

Численным показателем здоровья бизнес-процесса служит метрика, отражающая отсутствие отклонений от заданной логики и определяемая отношением количества итераций БП, выполненных без нарушений, к общему числу итераций БП за определенный интервал времени.

Другим эквивалентным показателем здоровья бизнес-процесса будет отношение количества его итераций (шагов) без нарушений за заданный период к общему количеству итераций БП за тот же период.

Предложенная метрика здоровья БП может быть уточнена. Возможна, например, такая ситуация, что будет иметь место одно отклонение из ста, но очень серьезное, которое приведет к существенному нарушению на выходе (простой пример – вброс в финансовую систему платежного документа задним числом. При этом очевидное, лежащее на поверхности, решение – добавить в метрику коэффициент серьезности отклонения, который формируется заказчиком по анкете – «несерьезное», «среднее», «серьезное» [14-15].

Архитектура платформы является универсальной для любого бизнес-процесса и не зависит от перечня и количества поддерживаемых им информационных систем. С точки зрения архитектуры на базе одной платформы можно реализовать (масштабировать) контрольную среду и устойчивое к мошенничеству состояние для неограниченного количества БП.

5. Пример применения платформы обеспечения здоровья бизнес-процесса

Представим бизнес-процесс на двух уровнях – уровне логики и уровне информации [16-17].

Уровень логики

1. Клиент отгружает логистической компании товар для последующей доставки конечным покупателям. При этом груз приходит одной машиной, например, в 10 000 товарных мест. С грузом идет одна товарно-транспортная накладная (ТТН), в которой описан весь груз.
2. Склад принимает груз, деконсолидирует его для отправки в сортировочные центры, где его деконсолидируют до уровня единицы груза.
3. Склад сортирует единицы груза и создает на каждую единицу груза – единицу накладной. Вносит в нее дополнительную стоимость, например, сумму страховки.
4. Склад выдает единицу груза курьеру для доставки.
5. Курьер осуществляет доставку, принимает денежные средства, выписывает (пробивает) кассовый чек, сдает деньги в бухгалтерию.
6. Бухгалтерия консолидирует суммы, полученные от курьеров, и отправляет их на счет клиента.

7. Клиент осуществляет сверку стоимости отгруженного товара (ТТН из п. 1) и полученной суммы (п. 6), в случае расхождения сумм клиент выставляет претензию, а логистическая компания ее оплачивает.

Уровень информации (представление процесса на уровне событий в информационной сети логистической компании)

1. По электронной почте клиент отправляет логистическому оператору сообщение, содержащее количество единиц товара и сумму. После утверждения этих данных в переписке клиент отправляет на интерфейс логистического оператора файл-реестр с содержанием количества единиц груза, стоимостью каждой единицы и адресом доставки
2. Логистический оператор принимает файл-реестр и конвертирует его в формат, понятный системе обработки документов логистического оператора, которая разбивает общий реестр на логические единицы, соответствующие единицам груза, и по признакам адреса определяет правила их пересылки и обработки на складах.
3. Система обработки документов создает электронную накладную для каждой единицы груза, присваивая дополнительные поля по совокупности признаков (например, наложенный платеж, сумма страховки или надбавка за срочную доставку по просьбе клиента).
4. Электронная накладная загружается в коммуникатор курьера. Формируется маршрутный лист.
5. Курьер ставит признак «доставлено», коммуникатор передает информацию на мобильную кассу, печатающую чек, в котором общая сумма платежа разбита по различным секциям учета.
6. Бухгалтерская система консолидирует платежную информацию. По всем счетам проводит зачисления и формирует платежные поручения для банка в пользу клиента.
7. Происходит обмен реестрами по электронной почте.

Может показаться, что бизнес-процесс довольно прост. Однако на практике в нем постоянно происходят инциденты. Базовые нарушения при конвертации реестров на интерфейсе логистического оператора, такие как некорректные символы, дополнительные поля и т.д., приводят к тому, что значения в системе обработки документов отличаются от значений в файле-реестре. В результате значение суммы не соответствует фактическому и делятся на два типа – недостаточная сумма/недостаточные условия доставки и избыточная сумма/избыточные условия доставки. Первый тип ошибок выясняется на этапе сверки с клиентом. Инциденты второго типа вызывают конфликт с конечным получателем, который не готов платить больше. Эти инциденты выясняются сразу по мере возникновения. Для их обработки существует процесс коррекции сумм в накладных, однако он не автоматизирован, а количество накладных с потенциальной ошибкой может исчисляться в тысячах единиц. При этом создаются ошибки второго уровня – ошибки ввода оператором новых значений. Помимо репутационных потерь логистический оператор теряет на подобных коллизиях до 2% от всей выручки (суммы, которые он получает в счет оплаты груза от конечного получателя).

Уровень корреляции в данном случае работает по принципу вычисления сверки общей суммы и последующего вычисления суммы всех значений логических единиц, которые появляются после обработки реестра в режиме реального времени на всех этапах процесса, включающего работу операторов по корректировке. В том случае, если сумма перестает совпадать с эталоном, система блокирует дальнейшие действия с накладными до успешной корректировки.

На рис. 2 показана схема, иллюстрирующая описанный процесс внутреннего контроля в логистике и обеспечение здорового логистического бизнес-процесса.

Рис. 2. Внутренний контроль накладных в логистике
(обеспечение здорового логистического бизнес-процесса)
(Fig. 2. Internal control of invoices in logistics (ensuring a healthy logistics business process))

Заключение

Статические методы корректировки бизнес-процессов перестают работать в условиях быстро развивающейся среды. Нужны динамические методы анализа и корректировки бизнес-процессов (БП). Для решения этой задачи был предложен подход формирования модели здоровья БП, на основании которого можно строить платформу обеспечения здоровья БП.

С точки зрения системно-аналитического подхода эта платформа представляет собой информационно-аналитическую систему [20], формирующую новое свойство – здоровье бизнес-процесса, направленное на снижение ресурсных потерь посредством выявления и предотвращения нарушений (в частности, киберпреступлений и мошенничества) на уровне процесса, а также формирования контрольной среды БП.

Целью внедрения платформы обеспечения здоровья БП является снижение потенциальных потерь (как прямых, так и косвенных), связанных с нарушениями в БП, посредством формирования контрольной среды – предиктивности (предсказательности) к нарушениям и обеспечения качества и стабильности БП (отсутствия нарушений).

Ключевые преимущества платформы: повышение качества результата бизнес-процесса и формирование устойчивости к его отклонениям.

СПИСОК ЛИТЕРАТУРЫ:

1. Колин К.К. Эволюция информатики //Информационные технологии. – 2005. №1. С. 2–16.
2. Стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения". – СТО БР ИББС-1.0-2014" (введен в действие Распоряжением Банка России от 17.05.2014 №Р-399). URL: https://www.cbr.ru/Content/Document/File/46921/st-10-14.pdf (дата обращения: 12.08.2019).
3. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств". – СТО БР ИББС-1.3-2016". URL: https://www.cbr.ru/content/document/file/46920/st-13-16.pdf (дата обращения: 12.08.2019).
4. Биктимиров М.Р., Щербаков А.Ю. Избранные главы компьютерной безопасности. – Казань: Изд-во Казанского матем. общества, 2004. – 372 с.
5. Абдеев Р.Ф. Философия информатизационной цивилизации. – М.: ВЛАДОС, 1994. – 336 с.
6. Gloning T., Fritz G. (Hrsg.): Digitale Wissenschaftskommunikation – Formate und ihre Nutzung. 2011. Gießen: Gießener elektronische Bibliothek. Abgerufen am 27. Mai 2014.
7. Voshmgir Sh. Blockchains, smart contracts und das dezentrale Web. 2016. Technologie Stiftung Berlin.
8. Михайлов А.И., Черный А.И., Гиляревский Р.С. Основы информатики. – М.: Наука, 1968. – 756 с.
9. Михайлов А.И., Черный А.И., Гиляревский Р.С. Научные коммуникации и информатика. – М.: Наука, 1976. – 435 с.
10. Колин К.К. Природа информации и философские основы информатики. Открытое образование. 2005. №2. С. 43–51.
11. Эпштейн В.Л. Антропоцентрическое информационное взаимодействие (вопросы терминологии)// Проблемы управления. 2003. № 1. С. 28–33.
12. Шемакин Ю.И. Семантика самоорганизующихся систем. – М.: Академический проект, 2003. – 176 с.
13. Правиков Д.И., Щербаков А.Ю. Новая парадигма информационной безопасности: взгляд основоположников //Актуальные вопросы науки и техники. Вып. 5. Сборник научных трудов по итогам международной научно-практической конференции (11 апреля 2018 г.), Самара, 2018.
14. Mainelli M., von Gunten C. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. 2014. A Long Finance report prepared by Z/Yen Group.
15. McKinsey & Company. Beyond the Hype: Blockchains in Capital Markets.
16. Hagenhoff S., Seidenfaden L., Ortelbach B., Schumann M. Neue Formen der Wissenschaftskommunikation. Eine Fallstudienuntersuchung. Göttingen, 2007, S. 5f.
17. Dernbach B., Kleinert C., Münder H. (Hrsg.): Handbuch Wissenschaftskommunikation. Wiesbaden, 2012.
18. Codd E.F. A Relational Model of Data for Large Shared Data Banks. Communications of the ACM, v. 13, n. 6, June, 1970.
19. Schlatt V., Schweizer A., Urbach N., Fridgen G. 2016. Blockchain: Grundlagen, Anwendungen und Potenziale. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT.
20. Рязанова А.А. Технология блокчейн в научно-информационной деятельности // Научно-техническая информация. Сер.1. – 2018. № 4. С. 8–12.

REFERENCES:

[1] Kolin K.K. the Evolution of computer science. Information technology. - 2005. №1. P. 2–16 (in Russian).
[2] Standard of The Bank of Russia "Information security of organizations of the banking system of Russian Federation. Generalities" - STO BR IBBS-1.0-2014" (introduced by the order of the Bank of Russia from 17.05.2014 №P-399). URL: https://www.cbr.ru/Content/Document/File/46921/st-10-14.pdf (accessed: 12.08.2019) (in Russian).
[3] Standard of The Bank of Russia “Collection and analysis of technical data in response to information security incidents in the implementation of money transfers”. - STO BR IBBS-1.3-2016. URL: https://www.cbr.ru/content/document/file/46920/st-13-16.pdf (accessed: 12.08.2019) (in Russian).
[4] Biktimirov M.R., Shcherbakov A.Yu. Elected heads of computer security. – Kazan: publishing House of Kazan Matem. societies, 2004. – 372 p. (in Russian).
[5] Abdeev R.F. Philosophy of civilization.– M.: VLADOS, 1994. – 336 p. (in Russian).
[6] Gloning T., Fritz G. (Hrsg.): Digitale Wissenschaftskommunikation – Formate und ihre Nutzung. 2011. Gießen: Gießener elektronische Bibliothek. Abgerufen am 27. Mai 2014.
[7] Voshmgir Sh. Blockchains, smart contracts und das dezentrale Web. 2016. Technologie Stiftung Berlin.
[8] Mikhailov A.I., Chernyi A.I., Gilyarevskyi R.S. Foundations of computer science. – M.: Publishing house "Science". 1968. – 756 p. (in Russian).
[9] Mikhailov A.I., Chernyi A.I., Gilyarevskyi R.S. Scientific communications and Informatics. – M.: Publishing house "Science". 1976. – 435 p. (in Russian).

[10] Colin K.K. Nature of information and philosophical foundations of Informatics. Open education. 2005. №2. P. 43–51 (in Russian).
[11] Epstein V.L. Anthropocentric information interaction (questions of terminology). Problems of management. 2003. № 1. P. 28–33 (in Russian).
[12] Shemakin Yu.I. Semantics of self-organizing systems. – M.: Academic project, 2003. – 176 p. (in Russian).
[13] Pravikov D.I., Shcherbakov, A.Yu. A new paradigm to information security: a view of the founders of the Topical issues of science and technology. Issue. 5. Collection of scientific papers on the results of the international scientific-practical conference (April 11, 2018), Samara, 2018 (in Russian).
[14] Mainelli M., von Gunten C. Chain Of A Lifetime: How Blockchain Technology Might Transform Personal Insurance. 2014. A Long Finance report prepared by Z/Yen Group.
[15] McKinsey & Company. Beyond the Hype: Blockchains in Capital Markets.
[16] Hagenhoff S., Seidenfaden L., Ortelbach B., Schumann M. Neue Formen der Wissenschaftskommunikation. Eine Fallstudienuntersuchung. Göttingen, 2007. S. 5f.
[17] Dernbach B., Kleinert C., Münder H. (Hrsg.): Handbuch Wissenschaftskommunikation. Wiesbaden, 2012.
[18] Codd E.F. A Relational Model of Data for Large Shared Data Banks. Communications of the ACM, v. 13, n. 6, June, 1970.
[19] Schlatt V., Schweizer A., Urbach N., Fridgen G. 2016. Blockchain: Grundlagen, Anwendungen und Potenziale. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT.
[20] Ryazanova A. A. Blockchain Technology in scientific and information activities. Scientific and technical information. Ser.1. – 2018. № 4. P. 8–12 (in Russian).

Поступила в редакцию – 06 июня 2019 г. Окончательный вариант – 15 августа 2019 г.
Received – Juny 06, 2019. The final version – August 15, 2019.