

# АНАЛИЗ УСЛОВИЙ И ФАКТОРОВ, ОКАЗЫВАЮЩИХ ВЛИЯНИЕ НА БЕЗОПАСНОСТЬ БИЗНЕС-ПРОЦЕССОВ

**Макеев Сергей Александрович**  
Аспирант, ФГБОУ ВО "Финансовый  
университет при Правительстве  
Российской Федерации"

## ANALYSIS OF THE CONDITIONS AND FACTORS AFFECTING THE SAFETY OF BUSINESS PROCESS

**S. Makeev**

### Annotation

The issues analyzed the business process as the object of protection, identified the key features of the functioning of corporate banking business processes in terms of their safety. Neutralization of negative informational influence breaking the normal state of the business process is needed.

**Keywords:** business model, business process, informational security, threat, vulnerability.

### Аннотация

В статье проведен анализ бизнес-процесса как объекта защиты, определены ключевые особенности функционирования бизнес-процессов кредитных организаций с точки зрения обеспечения их безопасности. Показана необходимость нейтрализации негативных информационных воздействий, нарушающих штатное состояние бизнес-процесса.

*Ключевые слова:*

Бизнес-модель, бизнес-процесс, информационная безопасность, угроза, уязвимость.

## Введение

В настоящее время обеспечение комплексной безопасности бизнеса является весьма актуальной задачей. При этом акцент смещается с защиты непосредственно информационного ресурса, как важнейшего элемента современной организации, на защиту ключевых процессов организации.

Для обеспечения комплексной безопасности бизнеса его владельцам, с одной стороны, следует оптимально выполнить требования триады "безопасность-функциональность-экономичность", а с другой стороны, организовывать мероприятия по нейтрализации (блокированию) угроз в отношении бизнес-процессов.

Широко применяемый риск-ориентированный подход во многом соответствует ценностям бизнеса: для кредитной организации важна её репутация на рынке, ущерб от успешной атаки на бизнес-процесс считается приемлемым в случае, если ущерб не превышает доходы организации.

Для определения текущей обстановки в организации и необходимо проводить периодические выявление и анализ условий и факторов, оказывающих влияние на безопасность бизнес-процессов.

Целью настоящей статьи является определение ключевых особенностей бизнес-процессов как объектов защиты, проведение анализа условий и факторов, оказывающих влияние на безопасность бизнес-процессов.

## Основы бизнес-моделирования

В соответствии с международными стандартами ISO серии 9000 под бизнес-процессом понимается устойчивая целенаправленная совокупность взаимосвязанных видов деятельности, которая по заданной технологии преобразует входы в выходы, представляющие ценность для клиента (потребителя).

Моделирование бизнес-процессов представляется как эффективное средство оптимизации деятельности организаций различных форм собственности, так и средство прогнозирования и минимизации рисков на различных этапах жизненного цикла организации. На рынке имеются специально разработанные инструментариумы моделирования процессов, обладающие своим набором достоинств и недостатков: верхний и средний уровни представления бизнес-процессов – IDEFO, UML; уровень представления процедур и функций ("нижний" уровень) – eEPC, IDEF3, DFD, Cross Functional Flowchart. Практика показывает необходимость применения нескольких но-

таций для повышения качества моделирования реальных бизнес-процессов организаций.

Бизнес-модель наиболее полно описывает кредитную организацию и представляет собой формализованную совокупность элементов стратегического управления организацией, управления её бизнес-процессами, управления персоналом, управления качеством, а также ресурсов, которые используются организацией для решения поставленных задач.

*Процессный подход активно внедряется в кредитные организации, так как это создает для них ряд преимуществ:*

- ◆ формализация деятельности кредитной организации;
- ◆ повышение прозрачности деятельности кредитной организации и её управляемости;
- ◆ внедрение лучших международных практик построения систем менеджмента организаций в соответствии со стандартами серии ISO 9000;
- ◆ создание необходимых условий для объединения всех активов организации в единую систему.

Для дальнейшего анализа воспользуемся типовой бизнес-моделью кредитной организации, предложенной в работе [3]. Наибольший интерес для нас представляют модели управления бизнес-процессами.

*Выделим следующую иерархию бизнес-процессов кредитных организаций:*

1. Основные бизнес-процессы:
  - ◆ обслуживание юридических лиц;
  - ◆ обслуживание физических лиц;
  - ◆ работа на инвестиционных рынках;
  - ◆ обслуживание привилегированных (VIP) клиентов;
  - ◆ др.
2. Обеспечивающие бизнес-процессы:
  - ◆ документооборот;
  - ◆ юридическое обеспечение;
  - ◆ информационное обеспечение;
  - ◆ обеспечение безопасности (в том числе, информационной);
  - ◆ др.
3. Управляющие бизнес-процессы
  - ◆ стратегическое управление;
  - ◆ управление качеством;
  - ◆ управление рисками;
  - ◆ управление персоналом.
  - ◆ др.

Остановимся более подробно на рассмотрении основных бизнес-процессов кредитной организации, так как они формируют собой ключевые направления деятельности организации, и нарушение функционирования которых повлечет за собой серьезные финансовые и / или репутационные потери.

Для описания любого бизнес-процесса весьма важно задать его окружение посредством построения модели окружения бизнес-процесса.

*С помощью модели окружения бизнес-процесса задаются следующие характеристики бизнес-процесса [2]:*

- ◆ границы бизнес-процесса (события завершения и начала, входы-выходы материальные / информационные);
- ◆ цели бизнес-процесса;
- ◆ показатели бизнес-процесса (количественные и качественные);
- ◆ используемые ресурсы (информационные, материальные);
- ◆ функции;
- ◆ регламенты;
- ◆ участники (владелец, исполнители, клиенты).

*Применяя определение топологии информационного объекта, получим альтернативный вариант декомпозиции бизнес-процесса [4]:*

- ◆ структуры: конфигурация информационных систем, др.;
- ◆ программы: регламенты выполнения бизнес-процесса, др.;
- ◆ ресурсы: информационные, материальные, др.;
- ◆ механизмы управления: функции, др.

#### Бизнес-процесс как объект защиты

Отмечая такую особенность бизнес-процессов кредитных организаций, как их высокая изменчивость, целесообразно рассматривать бизнес-процесс как самостоятельный объект защиты.

Бизнес-процесс имеет свойства, нарушение которых приводит к негативным последствиям с точки зрения выполнения целей существования кредитной организации, например, время выполнения бизнес-процесса, качество результата, затраченные ресурсы и др.

Нарушение возможно как из-за неумышленных ошибок исполнителя, некачественного проектирования бизнес-процесса, так и из-за целенаправленного негативного информационного воздействия (реализации угрозы) на бизнес-процесс.

Информационная угроза понимается как намерение или возможность субъекта нанести информационному объекту (бизнес–процессу) вред, заключающийся в:

- ◆ утрате элементов структуры (деструкции);
- ◆ нарушении программ и функций (дисфункции);
- ◆ ухудшению условий функционирования.

В современных условиях анализ рисков является основой обеспечения информационной безопасности организаций. Методы оценки рисков используются для анализа выявленных угроз и уязвимостей, выделения набора актуальных угроз и выбора соответствующих контрмер.

*Анализ возможных рисков бизнес–процессов необходимо проводить на следующих этапах его жизненного цикла:*

- ◆ проектирование;
- ◆ реинжиниринг;
- ◆ штатное функционирование.

В работе [1] предложен подход к построению модели угроз организации информационно–признакового типа. В рамках данного подхода угроза представляется как совокупность неблагоприятных условий и факторов, сложившихся объективно либо создаваемых субъектом (преднамеренные угрозы) или складывающихся без участия субъекта.

*Применение информационно–признаковых моделей угроз организации позволяют:*

- ◆ осуществлять мониторинг внешней и внутренней среды функционирования кредитной организации путем анализа информационного пространства с целью поиска и обнаружения информационных признаков угроз;

- ◆ прогнозировать реализацию угроз организации на краткосрочную перспективу;
- ◆ формировать требования по распределению сил и средств защиты информации.

Среди недостатков вышеуказанного подхода можно отметить тот факт, что при построении информационно–признаковых моделей угроз организации не учитываются организационные и программно–технические уязвимости.

В работе [5] представлен подход к управлению информационной безопасностью на основе формальных моделей бизнес–процессов. Достоинством подхода является рассмотрение обеспечения безопасности как процесса, неразрывного с ключевыми бизнес–процессами: анализ безопасности процесса проводится на основе данных (параметры угроз и уязвимостей, взаимосвязь с другими бизнес–процессами), полученных из рассматриваемого бизнес–процесса.

#### Заключение

В настоящей статье определены ключевые особенности бизнес–процессов как объектов защиты, проведен анализ условий и факторов, оказывающих влияние на безопасность бизнес–процессов, показавший необходимость нейтрализации негативных информационных воздействий, нарушающих штатное функционирование бизнес–процесса.

Целью обеспечения информационной безопасности кредитной организации должно являться поддержание условий эффективного функционирования её ключевых бизнес–процессов.

#### ЛИТЕРАТУРА

1. Галкова Е.А. Информационно–признаковая модель угроз безопасности организации // Интернет–журнал "Науковедение". 2014. № 5 (24). [Электронный ресурс]. М.: Науковедение, 2014. Режим доступа: <http://naukovedenie.ru/PDF/49TVN514.pdf>, свободный. Загл. с экрана. Яз. рус., англ.
2. Ефимов Е.Н., Лапицкая Г.М. Информационная безопасность и бизнес–процессы компании // Известия ЮФУ. Технические науки. 2013. № 12 (149). С. 253–260.
3. Исаев Р.А. Комплексная бизнес–модель коммерческого банка // Финансовая аналитика: проблемы и решения. 2010. № 15. С. 47–59.
4. Макеев С.А. Информационная безопасность бизнес–процессов кредитной организации в условиях проведения информационных операций // Труды международного симпозиума Надежность и качество. 2015. Т. 2. С. 244–246.
5. Пестунова Т.М., Родионова З.В., Горинова С.Д. // Доклады Томского государственного университета систем управления и радиоэлектроники. 2014. № 2 (32). С. 150–156.