УДК 004.7

Т.М. Пестунова, З.В. Родионова, С.Д. Горинова

Анализ аспектов информационной безопасности на основе формальных моделей бизнес-процессов

Представлен подход к анализу аспектов информационной безопасности на основе формальных моделей процессов организации, разработанных в стандартных нотациях бизнес-моделирования. Процесс рассматривается как объект защиты информации. Проведён частичный анализ некоторых распространённых методик оценки рисков информационной безопасности в контексте объектов, содержащихся в EPC-модели.

Ключевые слова: информационная безопасность (ИБ), модели бизнес-процессов, права доступа, риски.

Согласно стандартам объектами защиты являются «информация или носитель информации или информационный процесс, которые надо защищать в соответствии с целью защиты» [1]. Анализ литературы и практика показывают, что при создании систем защиты информации в качестве объектов защиты, как правило, рассматриваются информация и её носители. В условиях, когда процессный подход к организации деятельности предприятия является основным принципом и при управлении, и при автоматизации, ограничиваться этим недостаточно. Цель защиты определяется целями деятельности организации, достижение которых обеспечивается, в частности, корректной реализацией основных и вспомогательных бизнес-процессов. Постановка задач ИБ в контексте бизнес-процессов позволяет соотнести аспекты безопасности с результатами бизнес-процессов, а значит, и с целями деятельности организации. Следует отметить, что бизнес-процессы организаций и предприятий не являются статичными. Их высокая изменчивость обусловлена многими причинами, в частности, слиянием фирм, оптимизацией организационной структуры, внедрением автоматизированных технологий и т.п., что требует постоянного отражения происходящих изменений в системе обеспечения ИБ. При этом изменения могут касаться всех элементов системы ИБ: от концептуальных документов, инструкций и регламентов до конфигурации программно-технических решений.

Анализ моделей бизнес-процессов даёт возможность отследить влияние происходящих изменений на многие аспекты ИБ. В частности, в [5, 6] и ряде последующих работ авторами был предложен автоматизированный подход к управлению правами доступа на основе анализа EPC-модели, основные этапы которого представлены на рис. 1. Говоря о целесообразности обращения к формальным моделям бизнес-процессов при решении задач ИБ, следует отметить, что эти модели обычно разрабатываются в ходе бизнес-планирования и реинжиниринга процессов предприятия, в частности, при автоматизации. Результаты таких работ приводят к необходимости внесения изменений в политики и (или) технологии ИБ, и если при моделировании бизнес-процессов предусмотреть анализ параметров, влияющих на ИБ, то можно снизить трудоёмкость работ по выявлению и обоснованию изменений в системе ИБ.

В данной работе исследуются модели бизнес-процессов в контексте решения задач анализа угроз и уязвимостей для последующей оценки рисков информационной безопасности. В современных условиях анализ рисков является основой обеспечения ИБ и проектирования систем защиты информации, что находит отражение не только в научно-методической литературе, но и закреплено в нормативно-правовых актах и стандартах [2, 3]. Важным документом при этом является модель угроз, в которой отражаются и актуализируются данные об источниках угроз, уязвимостях системы, объектах воздействия и ряде других параметров. Методы оценки рисков используются для анализа критичности выявленных угроз, обоснования множества актуальных угроз и выбора соответствующих контрмер.

Некоторые авторы [4] отмечают необходимость рассмотрения бизнес-процессов как основных активов организации, представляющих собой комбинацию из разнородных активов: информации, технических и программных средств, кадровых ресурсов и т. д. Но, несмотря на это, решение задач ИБ напрямую с моделями бизнес-процессов не связывается. Целесообразным считается получение

информации об основных бизнес-процессах от владельцев и участников этих процессов при помощи опросных листов. При этом цель сбора этих данных – выявление критичных информационных активов и технологических аспектов их обработки, на основе которых можно сделать выводы об угрозах и уязвимостях. Дальнейшая оценка не предполагает обращения к бизнес-процессам.

Рис. 1. Этапы процесса формализации и актуализации прав доступа на основе бизнес-процессов

Не подвергая сомнению данный метод, который используется и при описании бизнес-процессов, следует учесть три существенных обстоятельства. Во-первых, значительная часть информации, которая выявляется из ответов опросных листов, уже содержится в объектах формальных моделей бизнес-процессов. В качестве примера в табл. 1 приведено сопоставление элементов разработанной авторами модели формализации и актуализации прав доступа к графически отображаемым объектам бизнес-процессов для двух распространённых сред бизнес-моделирования, поддерживающих нотацию EPC. Указанные объекты также важны и с точки зрения задачи анализа угроз и уязвимостей. Схематично этот процесс изображён на рис. 2.

Во-вторых, получение актуальных данных о состоянии организации – это непрерывный процесс. После проведения аудита, который является периодическим процессом, в организации могут произойти разного рода изменения. Даже если используются автоматизированные системы управления рисками, при изменении бизнес-процессов информация об этих изменениях должна вручную отслеживаться и вноситься в соответствующую систему. Автоматизированное извлечение данных из модели бизнес-процесса позволяет упростить данную процедуру и повысить оперативность решения задач переоценки рисков не только по результатам аудита, но и на основе данных текущего мониторинга безопасности и в случаях реинжиниринга бизнес-процессов.

Анализ ряда распространённых моделей анализа рисков, краткие обобщённые результаты которого представлены в табл. 2, позволяет сделать вывод об их основных параметрах, многие из которых являются общими для разных методик. Выделяется методика ГРИФ, использующая понятие

«бизнес-процесс»: под ним подразумеваются производственные процессы, в которых обрабатывается ценная информация [8]. Они не оцениваются, и не детализируется обработка информации внутри этих процессов. Но при использовании бизнес-процесса для оценки рисков можно отследить путь информационного объекта внутри процесса, что даёт возможность выявить угрозы и уязвимости. В методике определения актуальных угроз в информационных системах персональных данных [7] существенным образом учитывается специфика обрабатываемой информации при оценке исходной защищённости системы (например, операции с обезличенными данными) и при экспертном определении опасности угроз (оцениваются последствия для субъекта персональных данных).

Таблица 1

Описание и графическое представление элементов модели бизнес-процессов для разных сред бизнес-моделирования в модели формализации и актуализации прав доступа

Элементы модели формализации и актуализации прав доступа	Графическое представление объектов модели бизнес-процесса в средах	
	Business Studio	ARIS
FF – множество функций, выполняемых участниками бизнес-процесса (исполнителями)	Функция	Функция
IS – множество информационных систем	Информационная система	Прикладная система
IO – множество информационных объектов	Информация	Кластер информации
PP – множество исполнителей		Должность
FI – ФИО исполнителя	Нет графического представления	ФИО
AT – множество типов доступа	——→	- - - - - - - - - - - - - - →

В-третьих, бизнес-процесс, представленный в виде модели, может быть рассмотрен как самостоятельный объект защиты информации. Он имеет определённые свойства, нарушение которых приводит к негативным последствиям с точки зрения достижимости целей (подцелей) организации, что лежит в основе оценки критичности процесса. Примерами таких свойств являются: своевременность результата (выхода процесса), соответствие результата установленным требованиям, соответствие затраченных на выполнение процесса ресурсов плановым значениям и др. Их нарушение возможно из-за ошибок исполнителя, ненадлежащего состояния ресурсов, нарушения своевременности входа процесса, излишних затрат времени исполнителей на реализацию предусмотренных процессом работ, несогласованности действий исполнителей и т.п. Причины многих факторов риска лежат в области организации и исполнения информационных процессов, следовательно, должны быть объектом внимания при выполнении работ по ИБ. Это позволяет соотнести информационные объекты и функции по их обработке с конкретными результатами бизнес-процесса, установив влияние нарушения одних процессов (подпроцессов) на другие, а в итоге – на цели деятельности. Отследить такие взаимосвязи можно, опираясь на формальную модель бизнес-процесса. Подобный подход рассматривается, в частности, в [11]. Основные объекты этой модели представлены в табл. 3.

Для организации процесса оценки рисков на основе модели бизнес-процесса необходимы:

1) правила построения модели бизнес-процессов, обеспечивающие наличие и однозначную интерпретацию содержащихся в ней данных для а) идентификации угроз и уязвимостей; б) оценки значимости информационного ресурса как с точки зрения последствий для результата процесса, так и с точки зрения влияния изменённого результата процесса на цели деятельности;

2) алгоритмы извлечения из бизнес-процесса данных, используемых в модели анализа рисков;

3) алгоритмы реагирования на изменения, отображающие изменения параметров модели бизнес-процесса в значения параметров модели оценки рисков.

Практическая реализация данного подхода осуществляется посредством создания информационной системы анализа безопасности процесса (далее – ИС АБП), место которой в системе ИБ показано на рис. 3: ИС АБП получает данные из бизнес-процесса, а далее может передавать их на ана-

лиз в системы управления информационными рисками (СУИР), которые могут быть основаны на разных методиках. Результаты работы СУИР используются традиционным образом для реализации мер защиты информации как в автоматизированных информационных системах (АИС), так и при неавтоматизированной обработке (ИС).

Рис. 2. Диаграмма процесса «Анализ угроз и уязвимостей»

Таблица 2

Сопоставление параметров оценки рисков для некоторых типовых методик

Наименование методики	CRAMM [4, 9]	Модель NIST [10]	ГРИФ [8, 9]
Схожие объекты (с учётом возможных различий в детализации)	*Модель ИС*: границы системы и функциональная спецификация; *ресурс* (физический, программный, информационный): ценность ресурса; *угроза*: уровень угрозы, ожидаемые финансовые потери; *уязвимость*: уровень уязвимости; *контрмера*	*Модель ИС*: границы и функции системы, важность системы и данных; *ресурс* (физический, программный, информационный); *угроза*: возможность реализации, величина ущерба для ИС; *уязвимость*: вероятность использования; *контрмера*;	*Модель ИС*: архитектура сети; *ресурс* (физический, программный, информационный): ценность; *угроза*: вероятность реализации, ущерб от реализации угрозы; *уязвимость*; *контрмера*
Отличительные объекты		*источник угрозы*: мотивация	*группа пользователей*: класс, доступ к информации; *аспекты ИБ ресурса*: конфиденциальность, целостность, доступность; *бизнес-процесс*

Таблица 3

Перечень данных модели оценки рисков Таубенбергера–Юрьенса [11]

Объекты модели	Примечание о содержании
Модель бизнес-процесса	Представляется в формальной нотации
Критичность бизнес-процесса	Высокая, средняя и низкая критичность для бизнеса оценивается на основе внешних правил
Информационный ресурс	Информационный объект, обрабатываемый бизнес-процессом
Аспект ИБ для ресурса	Конфиденциальность, доступность и/или целостность
Точка входа	Момент начала обработки информации бизнес-процессом
Точка завершения обработки	Момент передачи данных между пользователями, их изменения или сохранения
Канал связи	Канал передачи данных от одной точки обработки к другой
Цель безопасности	Задается по отношению к бизнес-процессу на основе внешнего правила (например, экспертным путем)

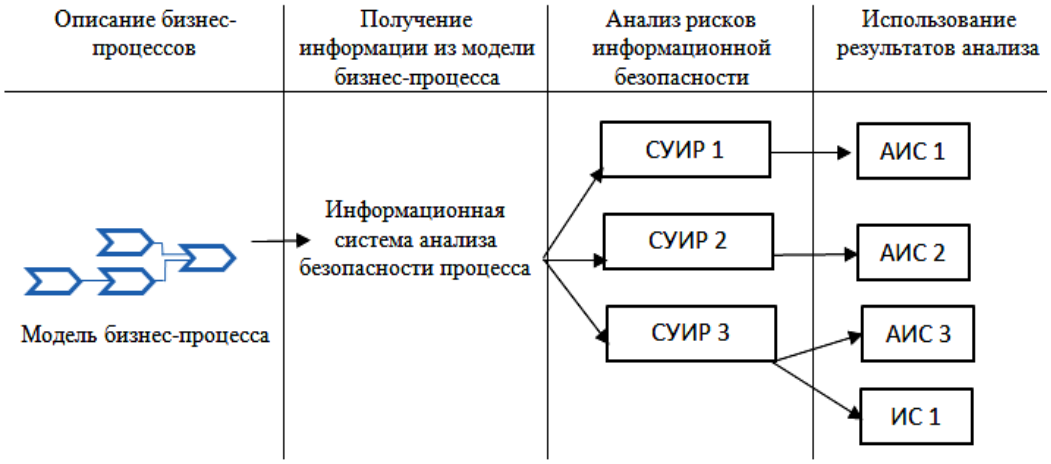

Рис. 3. Место ИС АБП в СУИБ

Сопоставление сведений, представленных в табл. 1 и 2, с данными в нотации EPC, показывает, что из модели бизнес-процесса можно извлечь данные для определения границ и особенностей ИС: содержание и носители обрабатываемой информации, пользователи, способы передачи данных внутри и вне ИС, используемые технологии. Эта информация является основой для идентификации защищаемых активов. Для автоматизированной идентификации возможных угроз в ИС АБП предусмотрена структура данных, содержащая используемые в методиках оценки рисков параметры угроз и уязвимостей во взаимосвязи с объектами бизнес-процесса, формируемая по следующим принципам:

1) каждой уязвимости должен быть поставлен в соответствие объект, определяющий, какому способу обработки, передачи и/или хранения присуща данная уязвимость;

2) каждой угрозе должны быть поставлены в соответствие аспекты ИБ, к нарушению которых может привести угроза: конфиденциальность, доступность и/или целостность;

3) каждой угрозе должен быть присвоен источник – источником может являться исполнитель бизнес-процесса, лицо, не принимающее участия в исполнении бизнес-процесса, стихия и проч.

Полная модель бизнес-процессов организации, представленная в формальной нотации, является иерархией моделей процессов и подпроцессов, которая отражает взаимосвязи процессов разного уровня детализации. При задании причинно-следственных связей между аспектами безопасности для информационных объектов, с одной стороны, и факторами и последствиями рисков для соответствующих подпроцессов, с другой стороны, можно, опираясь на взаимосвязи бизнес-процессов, отражаемые в формальной нотации, автоматизированным путём получить данные о степени влияния аспектов безопасности информационных объектов подпроцесса на результаты процессов более высокого уровня и в конечном итоге – на достижимость целей организации.

Заключение. В статье представлен подход к управлению аспектами ИБ на основе формальных моделей бизнес-процессов. В частности, на основе данных модели, представленной в терминах нотации EPC, разработана ИС формализации и актуализации прав доступа. Сформулирована концепция ИС АБП для автоматизированного анализа угроз и уязвимостей в ходе реинжиниринга бизнес-процессов, позволяющая оценивать планируемые изменения в организации бизнес-процессов с точки зрения возможных последствий ИБ и обоснованно принимать соответствующие решения.

Литература

1. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. – М.: Стандартинформ, 2006. – 18 с.

2. ГОСТ Р ИСО/МЭК 27005–2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – М.: Стандартинформ, 2011. – 51 с.

3. ГОСТ Р ИСО/МЭК 27005–2010. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. – М.: Стандартинформ, 2013. – 210 с.

4. Астахов А.М. Искусство управления информационными рисками. – М.: ДМК-Пресс, 2010. – 312 с.

5. Пестунова Т.М. Информационная система управления правами доступа на основе анализа бизнес-процессов / Т.М. Пестунова, З.В. Родионова // Доклады ТУСУРа. – 2010. – № 2 (22), ч. 2. – С. 253–256.

6. Родионова З.В. Управление процессом предоставления прав доступа на основе анализа бизнес-процессов / З.В. Родионова, Т. М. Пестунова // Прикладная дискретная математика. – 2008. – № 2. – С. 91–95.

7. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [методический документ ФСТЭК России: утв. ФСТЭК России 14.02.2008]. – М., 2008. – 10 с.

8. Методика оценки риска ГРИФ 2006 из состава Digital Security Office [Электронный ресурс]. – Режим доступа: http://dsec.ru/ipm-research-center/article/risk_assessment_method_vulture_2006_from_the_composition_of_the_digital_security_office/, свободный (дата обращения: 28.04.2014).

9. Лопарев С.А. Анализ инструментальных средств оценки рисков утечки информации в компьютерной сети предприятия / С.А. Лопарев, А.А. Шелупанов // Вопросы защиты информации. – 2003. – № 4. – С. 2–5.

10. Петренко С.А., Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. – М.: ДМК Пресс, 2004. – 384 с.

11. IT Security Risk Analysis based on Business Process Models enhanced with Security Requirements [Электронный ресурс]. – Режим доступа: http://ceur-ws.org/Vol-413/paper16.pdf, свободный (дата обращения: 20.04.2014).

Пестунова Тамара Михайловна
Канд. техн. наук, доцент, зав. каф. информационной безопасности
Новосибирского государственного университета экономики и управления (НГУЭУ)
Тел.: 8-913-922-53-05
Эл. почта: t.m.pestunova@nsuem.ru

Родионова Зинаида Валерьевна
Канд. техн. наук, доцент каф. информационной безопасности НГУЭУ
Тел.: 8-962-839-43-94
Эл. почта: z.v.rodionova@nsuem.ru

Горинова София Дмитриевна
Студентка НГУЭУ
Тел.: 8-953-792-63-27
Эл. почта: gsd0201@gmail.com

Pestunova T.M., Rodionova Z.V., Gorinova S.D.
Analysis of information security aspects based on the formal models of business processes

We outline an approach to analysis of information security aspects basing on formal models of company's business processes that are described in terms of standard business-modeling notations. Process is considered as a protected object. We partially analyzed some widespread risk evaluation methods in context of the objects used in EPC-model.
Keywords: information security, risks, models of business processes, access rights.
