РОССИЙСКАЯ АКАДЕМИЯ НАУК

ЦЕНТР ИССЛЕДОВАНИЯ ПРОБЛЕМ БЕЗОПАСНОСТИ
ИНСТИТУТ СОЦИАЛЬНО-ПОЛИТИЧЕСКИХ ИССЛЕДОВАНИЙ

НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ

научный журнал

nota bene

№1 (18), 2012

www.nbpublish.com

РОСИЙСКАЯ АКАДЕМИЯ НАУК
ЦЕНТР ИССЛЕДОВАНИЯ ПРОБЛЕМ БЕЗОПАСНОСТИ,
ИНСТИТУТ СОЦИАЛЬНО-ПОЛИТИЧЕСКИХ ИССЛЕДОВАНИЙ

НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ, 1'2012 | NATIONAL SECURITY, 1'2012

Статьи принимаются через сайт издательства www.nbpublish.com
После регистрации на сайте следует прикрепить файл с аннотацией на русском языке в пять-шесть предложений, десять ключевых слов, раскрывающих смысл статьи, саму статью со сносками и список литературы по теме (библиографию) в десять-пятнадцать наименований.

Уважаемые читатели, в первом полугодии 2010 года будут выходить сдвоенные номера журнала.

Журнал зарегистрирован в Министерстве по делам печати, телерадиовещания и средств массовых коммуникаций.
Свидетельство о регистрации СМИ № 016421 от 25 июля 1997 г. Изд. лиц. № 065828 от 20.04.98 г.
Тел./факс: (495) 424-26-02 **E-mail**: w.danilenko@gmail.com;

Внимание: отправка статей в редакцию возможна только через сайт издательства http://www.nbpublish.com

Почтовый адрес редакции: 123242, Россия, Москва, Д-242, а/я 38.
ISSN 1811-9018

Объем 13,5 усл.-печ.л., формат 60x84 1/8. Тираж 1115 экз. Печать офсетная. Бумага офсетная.
Сдано в набор 16.01.2012. Подписано в печать 31.01.2012.
Отпечатано с готовых диапозитивов в типографии Липецкого издательства
398055, г. Липецк, ул. Московская, 83. Тел.: (0742) 25-40-48, 25-99-21.

Подписка на журнал возможна с любого месяца.
Смотрите в Объединенном каталоге "ПРЕССА РОССИИ"
Наш индекс — 81935 (полугодовая и ежемесячная подписка).
Любой журнал или статью можно заказать в магазине Книга-почтой на сайте издательства www.nbpublish.com

А. В. Царегородцев, А. К. Качко

ОДИН ИЗ ПОДХОДОВ К УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРИ РАЗРАБОТКЕ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОРГАНИЗАЦИИ

Аннотация: моделирование угроз и уязвимостей информационной безопасности довольно широко применяется, как в зарубежных практиках, так и в рекомендациях отечественных стандартов. ключевой недостаток используемых методов состоит в отсутствии формализованного описания концептуальных решений при проектировании информационных систем. в связи с этим в статье предлагается рассматривать особый вариант описания концептуального решения в виде формализованных моделей. это важный этап при установлении связей между требованиями бизнеса и возможностями информационных технологий. в статье предлагается улучшить существующие решения архитектурой, состоящей из трёх ключевых компонентов: компонента моделирования, архитектурного компонента и модуля анализа рисков.
Ключевые слова: военное дело, информация, угроза, безопасность, риски, управление, бизнес-активы, бизнес-модель, инфраструктура, контрмеры.

Введение

В современном мире аспекты безопасности информационных систем играют жизненно важную роль и становятся центральным вопросом эффективного использования информационных ресурсов организации. Сегодня руководители компаний понимают, что построение системы информационной безопасности в организации является большой статьёй расходов в бюджете департамента информационных технологий. И речь в данном случае идёт как о стоимости применяемых технологий, так и об эффективном выборе методов управления информационной безопасностью. Многие финансовые организации (например, банки) первыми освоили инфраструктуру сертификации открытых ключей, стали рассматривать её, как наиболее безопасную платформу для обеспечения аутентификации, конфиденциальности, целостности, а также для обеспечения невозможности отказа партнёров по связи от факта передачи или приёма сообщения. Но через некоторое время из-за возрастающей стоимости владения сложными системами безопасности многие из организаций отказались от них в пользу простых и менее надёжных решений. Это связано с тем, что сопутствующие расходы напрямую связаны с проблемами управления и совместимости процессов безопасности в организации, а также косвенно связаны с трудностями их использования и поддержки со стороны конечных клиентов. Таким образом, многие решения для обеспечения информационной безопасности могут быть успешно внедрены в организации, но главная проблема заключается в прямых и косвенных расходах, возникающих по мере функционирования данных систем. На практике, эти расходы на внедрение и сопровождение могут быть сопоставимы с потерями организации, в случае если она в принципе не будет уделять внимание угрозам информационной безопасности.

Окупаемость инвестиций в области информационной безопасности напрямую связана отношением расходов на внедрение к предоставляемым преимуществам. Выбор наиболее подходящего решения становится жизненно важным вопросом для многих организаций.

В международном праве существует ряд законов и отраслевых стандартов для финансовых организаций, компаний телекоммуникационной отрасли, учреждений здравоохранения и обязательных и рекомендательных документов, затрагивающих защиту информации от внутренних угроз и управление операционными рисками:

- **Стандарт Банка России** СТО БР ИББС-1.0-2010. Настоящий стандарт распространяется на организации банковской системы Российской Федерации (далее — организации БС РФ) и устанавливает положения по обеспечению информационной безопасности в организациях БС РФ [1].

- **Кодекс корпоративного поведения ФСФР**. Свод правил и рекомендации ФСФР России для компаний-участников рынков ценных бумаг России. В Кодексе раскрываются основные принципы наилучшей практики корпоративного поведения, в соответствии с которыми российские общества могут строить свою систему корпоративного поведения, а также содержатся рекомендации по практической реализации данных принципов и раскрытию соответствующей информации.
- **PCI DSS**. Обязательный стандарт для операторов данных платежных карт систем VISA, MasterCard, American Express, JCB, Discover. В стандарте регламентируется необходимость шифрования носителей информации, содержащих данные платежных карт, и надежной защиты ключей шифрования, определена необходимость генерации стойкого ключа и разделение криптографического ключа между несколькими лицами и необходимость использования двухфакторной аутентификации для доступа к данным.
- **Basel II**. Нормативный акт, регламентирующий банковскую деятельность в Евросоюзе, Северной Америке и Японии. В стандарте описана необходимость ведения архива конфиденциальной информации и создания системы управления операционными рисками.
- **SOX**. Sarbanes-Oxley Act of 2002 является обязательным для всех публичных компаний, акции которых котируются на фондовых биржах США. Секция 404 закона регламентирует необходимость внедрения системы внутреннего контроля для предотвращения и защиты информационных активов компании от утечек и несанкционированного использования.
- **SEC Rule 17a-4 и NASD 3010/3110**. Своды правил для компаний, акции которых котируются на биржах США. В правилах регламентируется создание архива электронной корреспонденции и переписки через службы мгновенных сообщений: требуется архивировать не только корреспонденцию участников системы, но и все транзакции брокеров, трейдеров и лиц, действующих от их имени.
- **Combined code on corporate governance**. Кодекс корпоративного управления Великобритании регламентирует создание и поддержку системы внутреннего контроля и необходимость как минимум один раз в год проводить независимый аудит такой системы. В Кодексе говорится о необходимости постоянного мониторинга самой системы внутреннего контроля, а в случае возникновения какого-либо инцидента ИБ, высшее руководство компании должно быть немедленно информировано.
- **HIPAA**. Американский закон HIPAA регламентирует необходимость создания системы внутреннего контроля, написания правил использования рабочих компьютеров и внешних устройств и организации системы контроля доступа к информации.
- **GBLA & FACTA**. Защита непубличной информации клиентов финансовых корпораций регламентируется законами Gramm-Leach-Bliley Act of 1999 и Fair and Accurate Credit Transactions Act of 2003. Стандарт «Interagency Guidelines Establishing Information Security Standards» вносит дополнительные уточнения в приведенные законы и требует от финансовых институтов США защищать непубличные данные граждан в процессе хранения, использования, пересылки и утилизации от всех прогнозируемых рисков информационной безопасности, а также обеспечить надежный контроль доступа к этой информации.

Для решения задачи оценки информационных рисков необходимо последовательно описать процессы от идентификации бизнес активов до процессов, обеспечивающих поддержку и эксплуатацию комплексных систем управления информационной безопасностью.

В статье особое внимание будет уделено методам управления информационной безопасностью и аспектам построения архитектуры системы управления информационными рисками. Также будут описаны недостатки популярных решений в области управления рисками и представлены преимущества дополнения этих решений формальной структурой (концептуальным решением).

В концептуальном решении подчеркивается важность построения цепи процессов, как на бизнес уровне (проблема ''что защищать''), так и на технической программной архитектуре (''как защищать''). Принимая во внимание тот факт, что такие модели не всегда могут быть применимы в решении конкретных ИТ/бизнес вопросов, будет приведено преимущество выработки требований к проектируемой системе в контексте процессов

управления ИТ рисками. На программно-архитектурном уровне будет отражено, как достижение цели совершенствует процесс управления рисков и покрывает требования информационной безопасности. Особое внимание будет уделено компонентам архитектуры системы управления информационными рисками и будет показано, как требования безопасности становятся начальными точками для анализа информационных рисков.

1. Предпосылки к построению архитектуры системы управления информационными рисками

В настоящее время сотрудникам службы информационной безопасности доступно большое количество методов анализа рисков, которые отвечают требованиям непрерывности ведения бизнеса. На рисунке 1 приведена модель управления рисками, показывающая взаимосвязь между ключевыми активами организации.

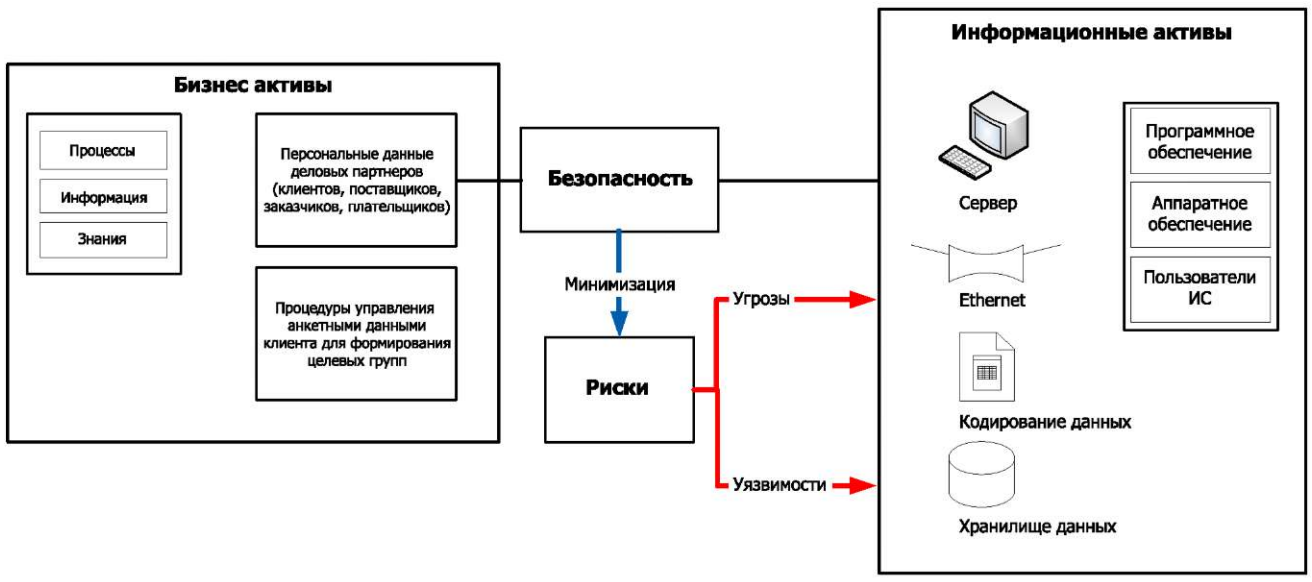

Рис. 1. Модель взаимодействия ключевых активов организации

В модели можно выделить следующие ключевые активы.

- *Бизнес активы* – это всё, что имеет экономическую ценность в организации и является основой для реализации бизнес целей. Защита бизнес активов жизненно необходима организации.
- Бизнес активы организации управляются с помощью корпоративных информационных систем. *Активы информационной системы* (информационные активы) – это любые компоненты, которые являются частью операционной среды управления данными. Во многих случаях информационные активы являются отражением бизнес активов (хранилище данных организации отражает информацию о бизнес активах, таких как: покупатели, контракты с поставщиками и т. д.).
- *Безопасность* является центральным компонентом корпоративной информационной системы. Помимо прямых функций безопасности (например, конфиденциальность данных), выполняет также критически важные для организации процессы, позволяющие обеспечить надежность, производительность и устойчивость бизнес активов.
- *Управление рисками* является центральным процессом измерения различных показателей информационной безопасности. Для каждого информационного актива, нужно определить уровень его уязвимости, наличие потенциальных угроз, способных использовать эти уязвимости, а также оценить влияние инцидентов безопасности на бизнес процессы организации в рамках повседневной работы. Чтобы успеш-

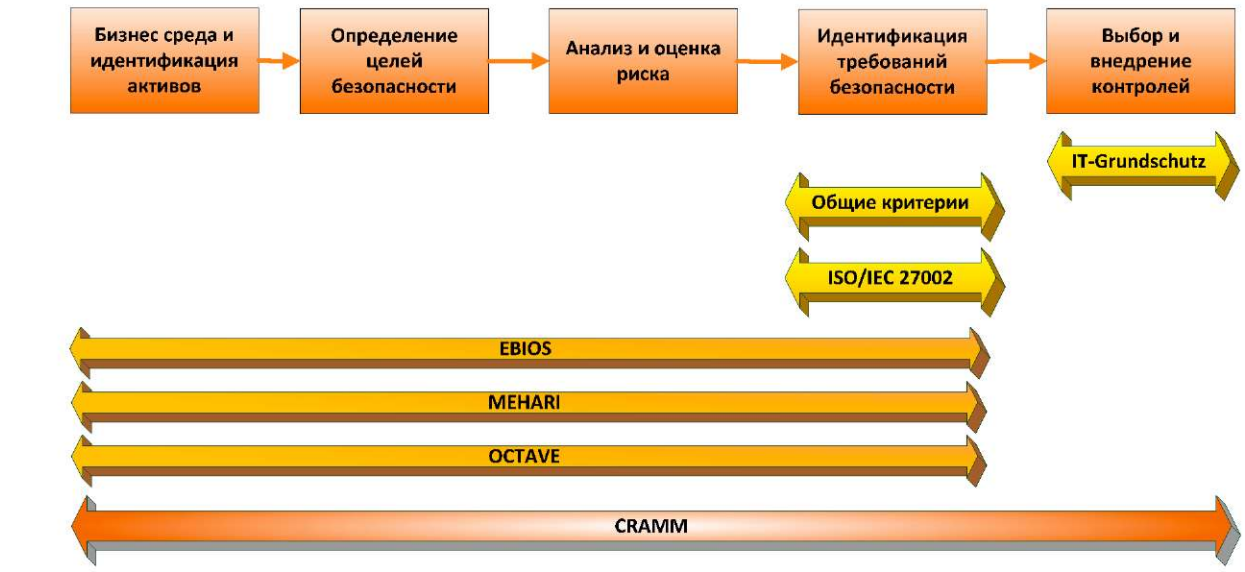

Рис. 2. Классификация существующих методов управления рисками

но реализовать все действия процесса анализа риска необходимо внедрить в организации процессы контроля и применения контрмер.

Основные этапы процесса управления рисками и их реализация в современных инструментальных средствах показаны на рисунке 2.

Процесс начинается с предпроектного исследования организации и идентификации бизнес активов. На этом этапе анализируется бизнес среда организации и приводится описание информационных систем, обеспечивающих ключевые процессы. Например, для крупного ритейлера основными информационными системами могут являться:

- система управления предприятием (ERP), состоящая из модулей по управлению логистикой, финансами, бухгалтерией;
- система взаимоотношением с клиентами (CRM), которая является центральной точкой взаимодействия (контакт центр, интернет магазин);
- хранилище данных, позволяющее проводить анализ клиентской базы, сегментировать клиентов по различным показателям, прогнозировать отток клиентов, проводить RFM, ABC анализ и т.д.

Затем, в зависимости от требуемого уровня защиты для активов, необходимо определить *цели информационной безопасности*. Цели безопасности часто определяются, как достижение конфиденциальности, целостности и доступности активов. Возвращаясь к примеру с ритейлером, не позднее 1 июля 2011 года необходимо обеспечить выполнение требований ФЗ № 152, без соответствия которому невозможно построить функционирующую систему управления информационной безопасности [1].

Согласно закону, а также ряду подзаконных актов и руководящих документов регулирующих органов (ФСТЭК России, ФСБ России, Роскомнадзор), операторы персональных данных должны выполнить ряд требований по защите персональных данных физических лиц (своих сотрудников, клиентов, посетителей и т. д.) обрабатываемых в информационных системах организации и предпринять ряд действий:

- направить уведомление об обработке персональных данных (Закон № 152-ФЗ Ст. 22 п. 3);
- получать письменное согласие субъекта персональных данных на обработку своих персональных данных (Закон № 152-ФЗ ст. 9 п. 4);
- уведомлять субъекта персональных данных о прекращении обработки и об уничтожении персональных данных (Закон № 152-ФЗ ст. 21 п. 4).

Главным шагом процесса управления рисками является его анализ, на основании которого определяется его значение. Определенный риск в зависимости от ситуации может либо нанести вред бизнес процессу или привести к угрозе срыва комплексных целей информационной безопасности. Этот шаг состоит из идентификации риска и оценки

его уровня качественным или количественным способом. Понятие «оценки риска» возникает только после того, как уровень проанализированных рисков сопоставлен с требованиями информационной безопасности организации, которые определены во время второго шага процесса.

Например, веб сервисы, поддерживающие взаимодействие между сайтом и центральной системой обработки данных могут стать целью заинтересованного лица, желающего перехватить конфиденциальную информацию используя слабые стороны протокола TCP/IP. Риск перехвата можно оценить, как достаточно высокий (используя терминологию качественной оценки). После осуществления анализа риска, должны быть приняты решения (*обработка риска*) по противодействию угрозе, используя выработанные контрмеры или привлечь сторонних экспертов в области защиты информации для решения поставленной задачи. Требования безопасности к информационным активам могут диктовать решения для смягчения информационных рисков. Для нашего примера уменьшение риска может быть достигнуто путём выбора технических средств, таких как: включение фильтрации трафика и обнаружение вторжений в корпоративной сети. Требования, в конечном счете, трансформируются в контроли безопасности (т.е. в наборы контрмер), которые реализуются в рамках организации.

В настоящее время доступно большое количество коммерческих программных комплексов для оценки информационных рисков. Одни из самых известных приведены в следующем списке:

- метод «OCTAVE» (авторы Альбертс и Дорофе, 2001),
- IT-Grundschutz (BSI, 2004),
- метод CRAMM (Insight Consulting, 2003),
- стандарт ISO/IEC 27002 (ISO, 2005a),
- общие критерии (Общие критерии, 2006),
- метод MEHARI (Club de la Se´curite´ de l'Information Francais, 2004),
- метод EBIOS (Генеральный секретариат министерства национальной обороны Франции, 2004).

Как показано на рис. 2 методы отличаются по набору составляющих шагов в процессе анализа риска. Некоторые из методов включают в себя только один блок действий (ISO, 2005a; Общие Критерии, 2006).

2. Недостатки существующих методов управления рисками

Существующие методы поддерживают операции управления рисками, но у них есть много недостатков, которые происходят, главным образом, от нехватки четких понятий, подробного анализа, отсутствия концептуальных решений при проектировании.

Можно выделить следующие направления совершенствования существующих методов.

1. Требуется формализованное описание процессов, изображенных на рис. 2. В течение долгого времени концептуальное моделирование информационных систем было сопряжено с проблемами, связанными с документами, написанным в произвольной форме. В связи с этим предлагается рассматривать ''модели'', как лучший способ достижения высокого качества и формального описания. Модель представляет собой совокупность процессов предприятия, которая может быть полезна для идентификации и описания бизнес активов предприятия, а также для описания логической или аппаратной архитектуры информационных систем для представления используемых информационных технологий и программных компонентов.
2. Необходимо систематическое описание методов для четкого понимания бизнес целей и возможностей технической реализации в контексте информационной безопасности. Это важное требование для установления связей между бизнесом и информационными ресурсами. Большинство существующих подходов поддерживает только верхнеуровневое описание этих связей, тогда как более детальный и подробный анализ может привести к оптимальному решению проблем информационной безопасности. Результаты, полученные из формализованного описания процессов управления информационными рисками в рамках концептуального моделирования, могут быть очень полезными для определения общей схемы связей между требованиями безопасности и компонентами информационной системы.
3. Необходимо обеспечить улучшенную интеграцию процессов анализа рисков на всех этапах жизненного цикла разработки информационной системы. В большинстве из подходов анализ

информационных рисков планируется в конце этапа разработки и иногда даже на фазе внедрения информационной системы. Однако большинство процедур анализа рисков может быть выполнено на различных стадиях разработки. Это принесёт ощутимые преимущества и выгоду, так как позволит отследить связи между решениями по управлению рисками и информацией накопленной за время этих этапов.

3. Моделирование процессов анализа информационных рисков

Для улучшения существующих методов необходимо дополнить их архитектурой, состоящей из трёх ключевых компонентов. Особое внимание уделяется на более ранние и продуктивные стадии разработки информационной системы.

1. Моделирование компонентов информационной системы для обеспечения качественной поддержки, формализации информации и знаний, полученных во время мероприятий по управлению рисками. Это может быть достигнуто путем построения моделей, включающих в себя бизнес активы и архитектуру решения по реализации (компонент моделирования).
2. Разработка концептуального решения, который обеспечивает систематизированный подход и приведение конфигурации информационной системы для достижения бизнес целей (архитектурный компонент). Для решения проблемы идентификации требований безопасности в организации особое внимание необходимо уделить двум аспектам, а именно:
   - совершенствование метода определения требований безопасности для текущих активов (целенаправленный метод),
   - соответствие архитектуры информационной системы требованиям безопасности (регулярный анализ информационных рисков).
3. Модуль анализа рисков, который поддерживает действия по выработке требований безопасности будет описан в виде процесса принятия решений, который основывается на анализе затрат и преимуществ (в частности на основе ROI анализа).

Предлагаемая архитектура отображена на рис. 3, которая является дополнением рис. 1 и детализирует ключевые компоненты усовершенствования в модели взаимодействия основных активов организации.

Модуль моделирования

При моделировании работы системы управления информационными рисками критически важные преимущества достигаются за счёт точного понимания бизнеса организации («что защищать») и архитектуры («как защищать»).

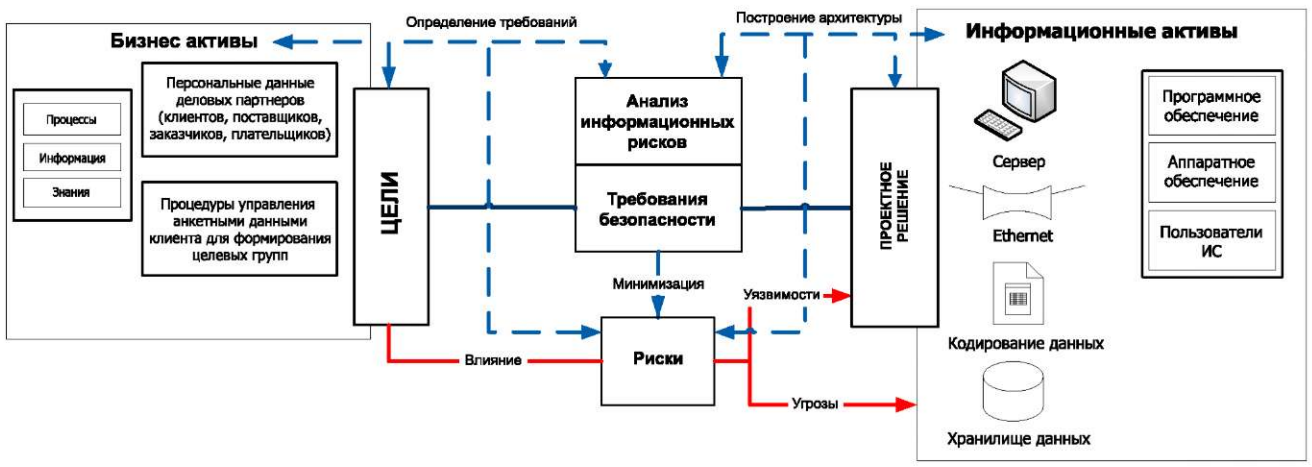

Рис. 3. Предлагаемая модель управления информационными рисками

Но наиболее важной задачей при анализе рисков становится описание процессов управления информационными активами, а также определение их взаимосвязи с бизнес активами. Даже принимая во внимание, что эти активы могут быть представлены в виде диаграмм «что» и «как», необходимо дополнительно рассматривать решение (диаграмму «зачем») для поддержки связей между различными активами и таким образом получить необходимые знания для проведения анализа информационных рисков.

Модуль выработки требований информационной безопасности

Соответствие требований бизнеса с возможностями информационных систем гарантируется за счет использования методов выработки требований, которые определяются:

- высокоуровневыми целями, связанными с бизнес-активами;
- низкоуровневыми целями, которые относятся к ожидаемым результатам ИТ решения.

Из-за значительного воздействия *нефункциональных аспектов* по всем видам деятельности в рамках построения архитектуры решения, выявление этих аспектов (в первую очередь аспектов безопасности) должно быть осуществлено на самых ранних этапах процесса внедрения, в частности, на этапе выработки требований. Решение данной задачи заключается в построении управляемой событиями цепи процессов (EPC диаграммы).

Анализ технического задания приведет к проектному решению, а анализ проектного решения покажет необходимость дальнейших шагов для оптимизации. Управление этими двумя взаимосвязанными аспектами является частью компонента анализа информационных рисков.

Модуль анализа информационных рисков

В проекте внедрения информационных систем разрабатывается большое количество решений, в которых на абстрактном уровне описываются стратегические цели бизнеса в виде процессов и описанием подробной архитектуры и возможных путей реализации. Во все решения закладываются соответствующие риски, большинство из них имеют серьезное воздействие на уровень безопасности, поддержка которого, в конечном счете, является главной целью информационной системы. Например, эти воздействия могут быть связаны с неправильной идентификацией:

- бизнес активов компании;
- целей информационной безопасности;
- требований к информационным активам.

В результате неправильного определения всех или некоторых из этих элементов может появиться некорректная оценка риска и/или неправильный выбор мер обеспечения информационной безопасности.

Для решения обозначенных проблем необходимо описать и внедрить процесс управления информационными рисками организации, при этом:

1) гарантировать качество проектного решения путём нахождения компромисса между затратами на внедрение и получаемыми преимуществами. В частности, описание нефункциональных аспектов в виде требований и предложений по архитектуре зависит от полноты проведенного анализа, который является одним из наиболее важных аспектов качества проектной деятельности наряду с точностью и достаточностью;

2) обеспечить динамическое приведение процесса принятия решения в рамках двухуровневой абстракции:

- высокоуровневая бизнес модель,
- подробная архитектура ИТ решения;

3) обеспечить своевременное определение внедренных проектных решений (концепций) для выбора путей развития. Это самая важная особенность, учитывая, что модели, имеют тенденцию разрастаться до больших размеров и с практической точки зрения необходимо установить отношения между различными концепциями безопасности и абстрактными уровнями архитектуры решения по безопасности.

4. Основные положения метода управления информационными рисками

Предлагаемый метод основывается на качественной оценке риска и фокусируется на итерационных шагах разработки решения по безопасности, а именно на критичных составляющих бизнеса и информационной системы.

Критерии оценки основываются на определении риска и затрат на его уменьшение. Точность качественной оценки риска в первую очередь зависит от экспертных знаний и очень часто от субъективных точек зрения всех заинтересованных лиц.

На данном этапе мы не будем вдаваться в подробности получения объективной оценки в процессе качественного анализ и поиска компромисса между

различными точками зрения. А отметим, что точность качественной оценки повышается при моделировании процессов. Например, в зависимости от специфики внедряемого решения, можно выделить следующие аспекты на различных этапах жизненного цикла.

1. На начальном этапе необходимо провести грубую оценку стоимости бизнес активов независимо от вероятности возникновения информационных рисков.
2. Необходимо провести поэтапную идентификацию информационных активов, которые являются отражением бизнес активов, и определить цели информационной безопасности.
3. Рассчитать вероятность возникновения критичных воздействий на информационные активы (атаки) на основании идентифицированных угроз и уязвимостей.
4. Принять во внимание (включить в бюджет информационной безопасности) стоимость выбранных контрмер.
5. Детально оценить затраты на обеспечение информационной безопасности.

Рассматривая все процессы информационной безопасности, необходимо выделить только наиболее важные и качественные аспекты, которые позволят оптимизировать ресурсы (бюджет), не затрагивая при этом полноту анализа информационных рисков. Кроме того, пользуясь отслеживанием ссылок (трассировкой) между ключевыми активами, детализация каждой итерации процесса информационной безопасности будет определяться на должном уровне абстракции. В результате будет происходить добавление смысловых деталей к уровню детализации каждой конкретной итерации по безопасности.

Весь процесс во многом зависит от архитектуры информационной системы, её описание и моделирование процессов становятся критичным при управлении рисками организации. Действительно, подход «средства – цель» при решении задачи отношений между активами может быть использован для определения требуемой детализации анализа рисков организации.

Предлагаемый метод является результатом обобщения ряда концепций в области информационной безопасности.

5. Управление информационными рисками на примере бизнес модели консалтинговой фирмы

Бизнес модель

Рассмотрим модель управления рисками в организации малого или среднего бизнеса, например консалтинговой фирмы. Все операции, которые совершает фирма можно отразить в виде диаграммы информационных процессов (рисунок 4), в которой будет отражены следующие ключевые моменты.

- Организационная структура компания включает в себя несколько ключевых подразделений (отдел развития, административный отдел, отдел продаж). Важно отметить, что последние два отдела непосредственно работают с внешними клиентами.
- Необходимо определить зависимости и отношения между ключевыми ответственными сотрудниками. Первый тип зависимости – это зависимость от цели. На диаграмме 4 отражены следующие ключевые цели:

1. Управление финансовой деятельностью.
2. Управление юридическими вопросами и техническими службами.
3. Управление проектами.

- Необходимо определить зависимость от задач. В нашем случае, например, отдел развития должен подготовить калькуляцию для отдела продаж
- Необходимо определить зависимость от ресурсов. Например, отдел развития должен подготовить техническое задание и модели для отдела продаж, а отдел продаж в свою очередь должен включить результат в виде наценки на услуги для внешних клиентов.

Происхождение целей информационной безопасности

После идентификации бизнес активов методы управления информационными рисками предлагают выделить цели информационной безопасности относительно этих бизнес активов. Существует общепринятая категоризация целей, которая включает в себя обеспечение конфиденциальности, целостности и доступности [3].

- Конфиденциальность: защиты чувствительной информации от несанкционированного раскрытия или доступного перехвата;

Рис. 4. Бизнес модель консалтинговой фирмы

- Целостность: сохранение точности и полноты информации и программного обеспечения;
- Доступность: обеспечение того, что информация и жизненно важные услуги доступны для пользователей при необходимости.

Цели информационной безопасности можно отразить в проектном решении в виде целей выработки требований для достижения формализованного описания и поддержки. Рисунок 5 показывает дерево целей, которое разработано в рамках нашего примера. Его разработка представляет процесс, состоящий из двух итерационных шагов.

1. Применение категорий компонентов информационной безопасности по отношению к конкретным бизнес активам (например, конфиденциальность ценовой политики)
2. Структурирование идентифицированных целей в виде иерархии, которая отражает различные цели и их вклад в высокоуровневые цели, которые могут быть частью стратегии компании (например, доверие клиентов или принудительное выполнение правовых обязательств).

На диаграмме 5 показано, что цель «Конфиденциальность ценовой политики» непос-

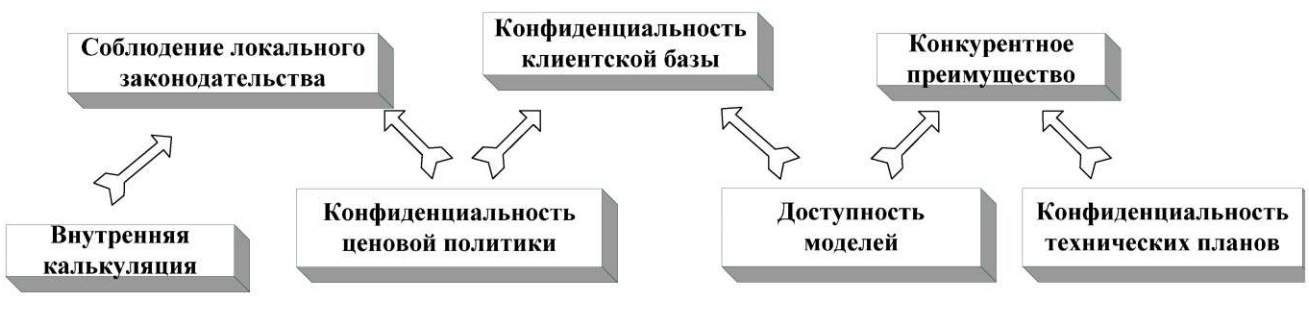

Рис. 5. Цели информационной безопасности

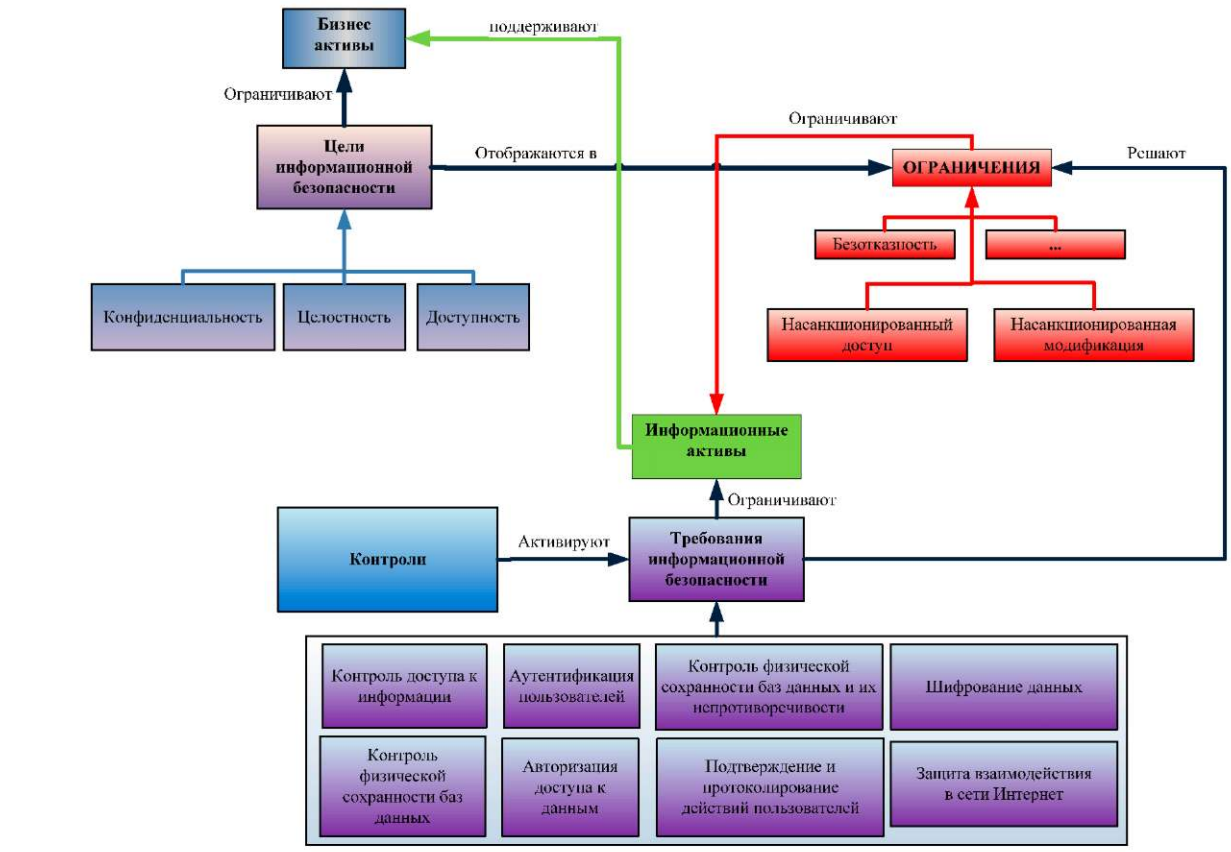

Рис. 6. Позиционирование требований безопасности в модели управления информационными рисками

редственно влияет на цель «Конфиденциальность клиентской базы», достижение которой не позволит со стороны конкурентов её раскрытие. Важно отметить, что в дерево целей можно включить дополнительную количественную или качественную оценку значений [15].

Идентификация высокоуровневых требований и ограничений

В предыдущем разделе было показано, как цели информационной безопасности в классической интерпретации методов оценки рисков могут быть получены исходя из бизнес целей организации. В этом разделе будет показано, как эти цели могут быть усовершенствованы с точки зрения требований к системе управления информационными рисками.

На рисунке 6 показана общая архитектура взаимодействия активов, целей и требований безопасности.

Как указано в работах Лин и Моффета необходимо отразить цели бизнеса в терминологии служб информационной. Например, цель "Конфиденциальность" может быть отражена на диаграмме в виде ограничения «Неавторизованный доступ к клиентской базе». На данном этапе важно понять, что информационная безопасность является «черным ящиком», поддерживающим ряд сервисов (например, «Управление счетами») без детализации реализации, а именно: в каком виде это можно спроектировать с точки зрения инфраструктуры информационной безопасности. Как показано в литературе [14] промежуточный уровень требований имеет критичное значение для определения свойств системы (скрытых потенциалов), её поведения на запросы пользователей.

Если рассматривать существующие методы управления информационными рисками, то использование в них *ограничений* представляет существенные преимущества при концептуальном дизайне информационной безопасности, а также преимуществом пересмотра архитектуры при развитии системы.

Выдвигая ограничение "Несанкционированный доступ" на данном этапе не рассматривается его

реализация. Она может быть осуществлена на более позднем этапе путём использования веб портала и/или путём найма сотрудников из охранного предприятия. На диаграмме 6 показана категоризация ограничений.

Большинство методов управления рисками вводят требования и поддерживают для них базу знаний. Тем не менее, у понятия "требования" могут быть различные значения в различных методах.

В некоторых случаях эти требования безопасности являются техническими, связанными со свойствами различных компонентов инфраструктуры: уровень базы данных, уровень приложений, уровень сетевых коммуникаций и т.д.

В другой нотации требования безопасности соответствуют родовым нефункциональным требованиям [10], входящими в руководство, которое может помочь системному архитектору во время проектирования решения.

В «Общих Критериях» [5] отражено два типа требований. Одни из них общие и звучат как "необходимость в применении некоторых механизмов управления доступом" (без детализации как их осуществить), другие – технические требования, например "длина ключа в механизме шифрования". С методологической точки зрения между ними необходимо сделать различие. В частности на данном этапе исследования отражены только нетехнические требования.

Также необходимо отметить связь между требованиями безопасности и ограничениями. Ограничение описывает проблему информационной безопасности, которая будет решена, в то время как требования безопасности представляют собой элементы решения вопросов информационной безопасности.

6. Анализ информационных рисков при построении системной архитектуры

При построении системы управления информационными рисками ключевую роль играет фаза построения архитектуры. На данном этапе происходит определение ключевых компонентов и средств управления (контрмер), которые могут использоваться для выполнения требований безопасности. Идентификация приемлемых контрмер является ключевой задачей в процессе обработки угрозы безопасности.

На рисунке 7 контроль «Протоколирование действий пользователя» происходит из следующих задач:

- Необходимо обеспечить аудиторскую проверку информационной системы отдела развития;
- Необходимо определить правила, на основании которых будет происходить анализ события, связанным с потенциальным нарушением информационной безопасности;
- Необходимо поддерживать трассировку изменений ключевых данных.

Осуществление контролей информационной безопасности требует существенных затрат со стороны организации для разработки, внедрения, продуктивной работы и поддержки выбранного решения. Поэтому определение контроля является результатом экономического анализа затрат и результатов дополненного анализом информационных рисков, основанным на доступной информации и статистических данных, связанных с уязвимостями, угрозами и возможными воздействиями. В нашем примере этот анализ может привести к идентификации угрозы, происходящей от внутреннего сотрудника, который мог изменить подвергнутые аудиту события. Эта угроза также связана с потенциальной уязвимостью, идентифицированной как следствие плохого определения права доступа (другой пример уязвимости мог быть связан с проблемами в физическом доступе к серверу). Эта информация представлена на рисунке 7 в виде концептуальной модели для анализа риска и контролей.

Заключительное решение для определения необходимости в протоколировании действий пользователя будет следовать из баланса, установленного между стоимостью решения, степенью воздействия риска на бизнес и потенциальной возможностью возникновения риска.

Заключение

Большинство существующих подходов по управлению информационными рисками поддерживает только верхнеуровневое описание этих связей и предполагает анализ информационных рисков в конце этапа разработки информационной системы, а в некоторых случаях на фазе внедрения.

В статье предлагается улучшить существующие решения архитектурой, состоящей из трёх ключевых компонентов: компонента моделирования, архитектурного компонента и модуля анализа рисков. При построении архитектуры необходимо выделять только наиболее важные и качественные аспекты, которые позволят оптимизировать ресурсы (бюджет), не затрагивая при этом полноту анализа

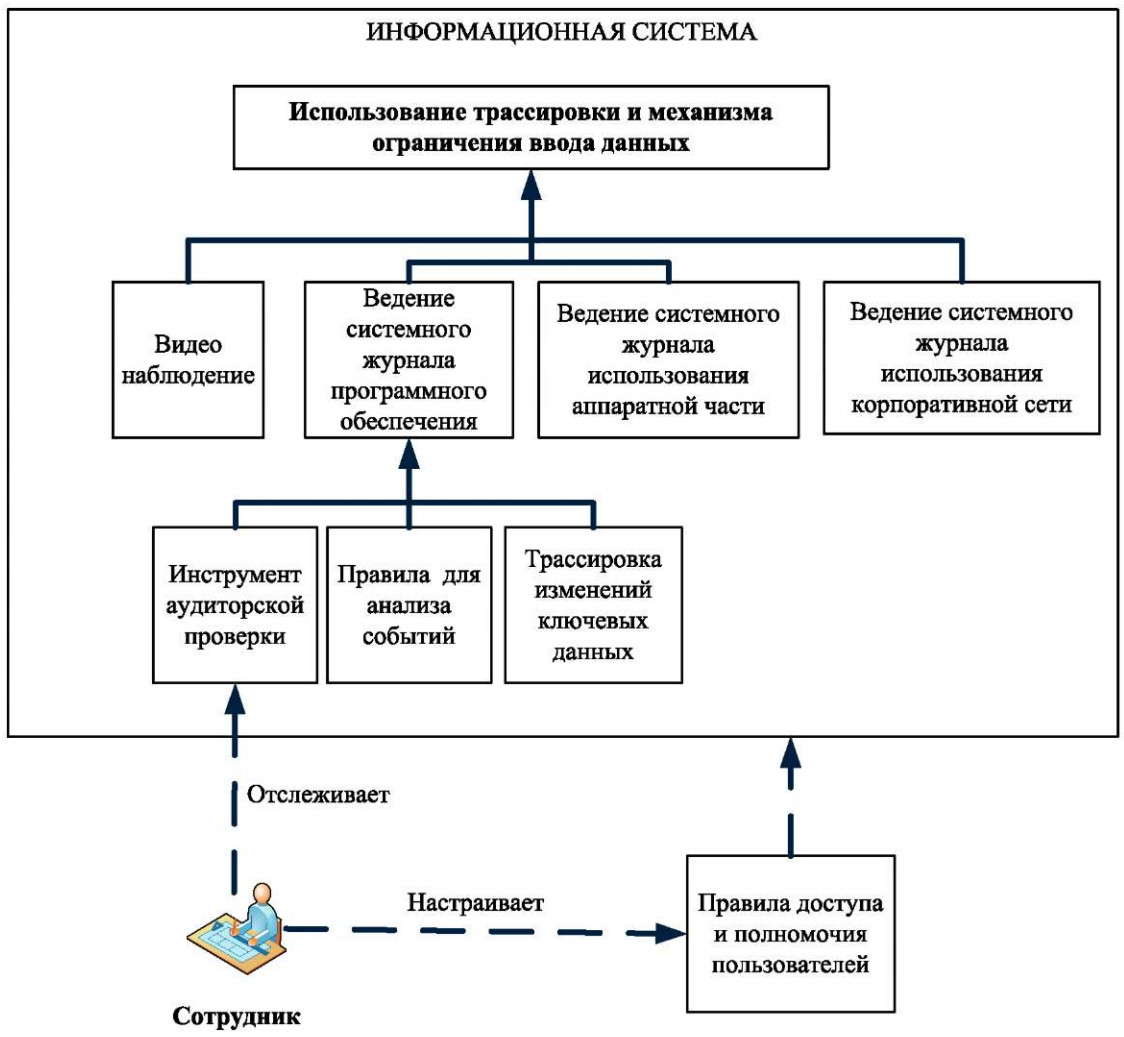

Рис. 7. Анализ рисков и внедрение контрмер

информационных рисков. Предложенный подход «средства – цель» при решении задачи поиска отношений между активами организации является результатом обобщения ряда концепций в области информационной безопасности и может быть использован для определения требуемой детализации анализа информационных рисков.

Рассматривая модель управления рисками в организации малого или среднего бизнеса, в статье показано каким образом формируется дерево целей информационной безопасности и как эти цели трансформируются в требования к системе управления информационными рисками предприятия.

Библиография:

1. Стандарт Банка России СТО БР ИББС-1.0-2010. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ. Дата введения: 2010-06-21, Москва 2010.
2. Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных». Гарант.
3. BS 7799-1:2005 — Британский стандарт BS 7799 первая часть. BS 7799 Part 1 — Code of Practice for Information Security Management (Практические правила управления информационной безопасностью).
4. BS 7799-2:2005 — Британский стандарт BS 7799 вторая часть стандарта. BS 7799 Part 2 — Information Security management — specification for information security management systems (Спецификация системы управления информационной безопасностью)
5. ГОСТ Р ИСО/МЭК 15408 — «Общие критерии оценки безопасности информационных технологий»
6. BS 7799-3:2006 — Британский стандарт BS 7799 третья часть стандарта.
7. Федеральный закон 363 «О внесении изменений в статьи 19 и 25 и Федерального закона «О персональных данных»». Гарант.
8. Геррити Т. П. Проблема управления. - М.: Наука, 1971.
9. ГОСТ Р 50922-96 Защита информации. Основные термины и определения. – М.: ИПК Издательства стандартов, 2004, - 6с.
10. Л. Чунг, Б. А. Никсон, Дж. Милополус. Нефункциональные требования в проектировании программного обеспечения // Kluwer Academic Publishers, Boston, 2000.
11. Домарев В.В. Оценка эффективности систем защиты информации // Издательство «ДиаСофт». 2007.
12. Зырянова, Т.Ю. Проблема анализа информационных рисков // Сборник докладов // Материалы международной научно-технической конференции «Наука, инновации, образование, актуальные проблемы развития транспортного комплекса России».
13. Об информации, информационных технологиях и о защите информации: ФЗ РФ от 27.07.2006 № 149-ФЗ // Консультант Плюс. Законодательство. Версия-Проф.
14. Дж. Гордийн, В. Карцева, Дж. Шильдвотч, Р. Виринга, Дж. Аккерманс. Разработка методов выработки специфических требований к информационным доменам организации // 12th IEEE International Requirements Engineering Conference, M. Aoyama, Motoshi Saeki, Neil Maiden (eds), IEEE CS, Kyoto, Japan, 2004.
15. М. Саеки. Применение метрик в методах проектирования информационных систем // Proceedings of CAiSE'03 Conf., Springer Verlag, 2003, стр. 374-389.

References (transliteration):

1. Standart Banka Rossii STO BR IBBS-1.0-2010. OBESPEChENIE INFORMACIONNOJ BEZOPASNOSTI ORGANIZACIJ BANKOVSKOJ SISTEMY ROSSIJSKOJ FEDERACII. Data vvedenija: 2010-06-21, Moskva 2010.
2. Federal'nyj zakon RF ot 27 ijulja 2006 goda № 152-FZ «O personal'nyh dannyh». Garant.
3. BS 7799-1:2005 — Britanskij standart BS 7799 pervaja chast'. BS 7799 Part 1 — Code of Practice for Information Security Management (Prakticheskie pravila upravlenija informacionnoj bezopasnost'ju).
4. BS 7799-2:2005 — Britanskij standart BS 7799 vtoraja chast' standarta. BS 7799 Part 2 — Information Security management — specification for information security management systems (Specifikacija sistemy upravlenija informacionnoj bezopasnost'ju)
5. GOST R ISO/MJeK 15408 — «Obwie kriterii ocenki bezopasnosti informacionnyh tehnologij»
6. BS 7799-3:2006 — Britanskij standart BS 7799 tret'ja chast' standarta.
7. Federal'nyj zakon 363 «O vnesenii izmenenij v stat'i 19 i 25 i Federal'nogo zakona «O personal'nyh dannyh»». Garant.
8. Gerriti T. P. Problema upravlenija. - M.: Nauka, 1971.
9. GOST R 50922-96 Zawita informacii. Osnovnye terminy i opredelenija. – M.: IPK Izdatel'stva standartov, 2004, - 6s.
10. L. Chung, B. A. Nikson, Dzh. Milopolus. Nefunkcional'nye trebovanija v proektirovanii programmnogo obespechenija // Kluwer Academic Publishers, Boston, 2000.
11. Domarev V.V. Ocenka jeffektivnosti sistem zawity informacii // Izdatel'stvo «DiaSoft». 2007.
12. Zyrjanova, T.Ju. Problema analiza informacionnyh riskov // Sbornik dokladov // Materialy mezhdunarodnoj nauchno-tehnicheskoj konferencii «Nauka, innovacii, obrazovanie, aktual'nye problemy razvitija transportnogo kompleksa Rossii».
13. Ob informacii, informacionnyh tehnologijah i o zawite informacii: FZ RF ot 27.07.2006 № 149-FZ // Konsul'tant Pljus. Zakonodatel'stvo. Versija-Prof.
14. Dzh. Gordijn, V. Karceva, Dzh. Shil'dvotch, R. Viringa, Dzh. Akkermans. Razrabotka metodov vyrabotki specificheskih trebovanij k informacionnym domenam organizacii // 12th IEEE International Requirements Engineering Conference, M. Aoyama, Motoshi Saeki, Neil Maiden (eds), IEEE CS, Kyoto, Japan, 2004.
15. M. Saeki. Primenenie metrik v metodah proektirovanija informacionnyh sistem // Proceedings of CAiSE'03 Conf., Springer Verlag, 2003, str. 374-389.