

СЕРТИФИКАТ БЕЗОПАСНОСТИ

Борис ДЪЯКОНОВ,
председатель совета директоров
«Банк24.ру» (ОАО), QMS Auditor,
СРМ «В» IPMA, канд. пед. наук,
доцент

Валентин НИКОНОВ,
исполнительный директор
консалтинговой компании
«Траектория роста», РМР IPMA,
QMS Auditor, канд. экон. наук

Этой весной «Банк24.ру» (ОАО) – первый российский банк, работающий в формате «24/7» – прошел сертификацию системы управления информационной безопасностью на соответствие требованиям международного стандарта ISO 27001:2005. **В данной статье мы расскажем о том, как внедрялась эта система.**

Для финансовых компаний риски информационной безопасности являются, пожалуй, наиболее критичными из всего многообразия операционных рисков. От того, насколько эффективно банки, страховые и инвестиционные компании и другие организации финансового сектора управляют этими рисками, зависит их конкурентоспособность и капитализация. Существует множество подходов к обеспечению информационной безопасности. Часть из них отражена в различных международных, национальных и отраслевых стандартах, в частности, в стандарте ISO 27001:2005, на основе которого была построена система управления рисками информационной безопасности в «Банке24.ру». Методология внедрения системы была разработана сотрудниками банка совместно со специалистами консалтинговой компании «Траектория роста».

В ее основе лежат четыре основных принципа:

1. Для эффективного обеспечения информационной безопасности требуются системные решения;
 2. Система менеджмента информационной безопасности должна быть основана на подходах современного риск-менеджмента;
 3. Система менеджмента информационной безопасности должна быть интегрирована в общую систему управления операционным риском организации;
 4. Для обеспечения информационной безопасности необходимо формирование соответствующей корпоративной культуры.
- Стандарт ISO 27001:2005 «Требования к системе менеджмента информационной безопасности» был опубликован Международной организацией по стандартизации в ноябре 2005 года и сейчас активно внедряется в организациях по всему миру.¹ В апреле 2008 года Банк24.ру стал первым российским банком, успешно прошедшим сертификацию на соответствие требованиям этого стандарта. Зачастую информационная безопасность ассоциируется в первую очередь с защитой от вирусов и хакеров, однако деятельность по ее обеспечению значительно шире. Она подразумевает систематическую защиту всех информационных активов компании. Под

По результатам исследования IT Governance Institute, объявление об инциденте информационной безопасности негативно влияет на рыночную стоимость компании. Организации, в которых произошел инцидент информационной безопасности, в среднем потеряли 2,1% рыночной стоимости в течение двух дней после объявления – около \$1,65 млрд на один инцидент.

¹ Полный перечень организаций, сертифицированных по стандарту, опубликован на сайте www.iso27001certificates.com

определение информационного актива, согласно ISO 27001:2005, подпадает все, что так или иначе связано с информацией и имеет ценность для организации – документы, серверы, компьютеры, программное обеспечение, базы данных, сотрудники и т.д. Естественно, найти в банке бизнес-процесс, который так или иначе не был бы связан с информационными активами, сложно.

Любой информационный актив обладает как минимум тремя нуждающимися в защите свойствами, сохранение соответствия которых заданным значениям и определяет уровень информационной безопасности. Это конфиденциальность, целостность и доступность (рис.1). Информационная безопасность – это сохранение всех свойств актива.

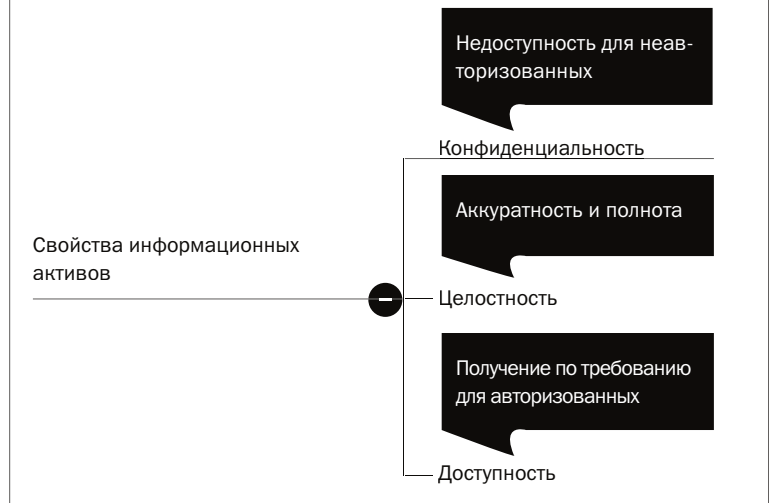
Сохранение свойства конфиденциальности подразумевает, что, например, к информации о банковских счетах клиентов будут иметь доступ только сотрудники, получившие соответствующую авторизацию, и эта информация не будет разглашена.

Если же вдруг из-за сбоя в работе базы данных у клиента на счете вместо тысячи рублей окажется миллион (или наоборот), это будет ярким примером нарушения свойства целостности информационного актива.

Если же информация из базы никуда не ушла, сохранена целостность данных, однако сведения недоступны, – это нарушение третьего свойства, которое определяет нашу возможность воспользоваться информационным активом, когда это необходимо.

Рис. 1

Свойства информационных активов



• у проектов по обеспечению безопасности очень сложно посчитать ROI или NPV. К примеру, ни один аэропорт в мире с точки зрения эффективности бизнеса не заинтересован во внедрении мер обеспечения безопасности: досмотр пассажиров уменьшает пропускную способность, а специальное оборудование стоит дорого. Но при этом очевидно, что безопасность, во-первых, необходима, во-вторых, должна быть не больше и не меньше, чем это на самом деле требуется.



Борис ДЬЯКОНОВ

Любой информационный актив обладает как минимум тремя нуждающимися в защите свойствами. Это конфиденциальность, целостность и доступность

Эффективный менеджмент информационной безопасности не может быть «точечным». Подобное несистемное управление информационной безопасностью чаще всего приводит к тому, что проблемы возникают совсем не там, где их ожидали.

Риск-ориентированный подход к обеспечению информационной безопасности

Не зная рисков информационной безопасности и не управляя ими, очень сложно оценить адекватность мер защиты. А это очень важно, поскольку:

- безопасность, безусловно, необходима, однако ее меры зачастую тормозят бизнес;

Единственный способ определить адекватность мер информационной безопасности – принимать решения об их внедрении на основе анализа рисков. Необходимо идентифицировать риски, реализация которых может повлечь наиболее тяжелые последствия, и рассматривать меры обеспечения информационной безопасности как стратегию управления этими рисками.

Почему был выбран стандарт ISO 27001:2005

Риски информационной безопасности – это операционные риски. Поэтому совершенно естественно, что система управления информационной безопасностью, а это, по сути, система управления рисками информационной безопас-

ности, должна быть интегрирована в общую систему управления операционным риском. В «Банке24.ру» система управления операционным риском основана на подходах, определенных в международном стандарте ISO 9001:2000 (в 2003 году «Банк24.ру» стал первым российским банком, успешно прошедшим сертификацию на соответствие ISO 9001:2000). Возможность интеграции системы управления информационной безопасностью в общую систему управления операционным риском была одним из немаловажных факторов, повлиявших на то, что в качестве основы для построения системы был выбран стандарт ISO 27001:2005. Решение ISO 27001:2005 было выбрано «Банком24.ру», поскольку оно позволяет реализовать четыре основных принципа, пере-

численных в начале статьи. Помимо того, что ISO 27001:2005 – это система, которая интегрируется в общую систему управления операционным риском (первый и третий принципы), она основана на подходах современного риск-менеджмента, а также позволяет сформировать корпоративную культуру, необходимую для обеспечения информационной безопасности (второй и четвертый принципы). Еще одно немаловажное достоинство ISO 27001:2005 – это возможность использовать инструменты аккредитованной сертификации на соответствие международным стандартам, благодаря чему компания может получить дополнительную экспертизу и независимую оценку системы, подтверждаемую международным сертификатом от признанного сертифицирующего органа.

Как на практике работает система менеджмента информационной безопасности ISO 27001:2005
 Для того чтобы понять, как работает на практике система менеджмента информационной безопасности, необходимо, в первую очередь, представить себе более общую систему – систему управления операционным риском. Система управления операционным риском «Банка24.ру» основана на ISO 9001:2000. Это задает общий формат управления бизнес-процессами банка и помимо прочего определяет общую процедуру управления операционным риском. В банке разработана процедура, в которой определены методы:

- идентификации операционного риска;
- проведения оценки риска;
- формирования рабочей группы;
- определения уязвимостей и причин риска;
- определения стратегий управления риском (на языке ISO 9001 – это «корректирующие и предупреждающие действия»);
- внедрения стратегий управления риском;
- оценки результативности внедренных стратегий управления риском.

Как известно, названия функций процесса управления риском (идентификация – оценка – определение и внедрение стратегии управления – оценка действий) мало зависят от типа рисков. Специфика заключается в том, как реализовать эти функции применительно к тому или иному виду рисков. Идентификация операционных рисков может проходить по-разному. В «Банке24.ру» информация об операционных рисках (их идентификация) поступает из трех основных источников:

- наблюдения сотрудников – каждый сотрудник может зарегистрировать несоответствие (реализовавшийся риск) или наблюдение (риск) во внутрикорпоративной сети (рис. 2);
- результаты обратной связи с клиентами – жалоба клиента – это реализовавшийся риск, анализ обратной связи позволяет выявить риски (рис.3);

Рис. 2
Форма регистрации несоответствия

Рис. 3
Форма регистрации рекламации клиента

- результаты внутренних аудитов.

Процесс управления операционным риском реализуется в интранете (внутренней компьютерной сети банка) с помощью специальных форм, поля которых отображают типовой процесс управления риском.

Процесс управления риском информационной безопасности незначительно отличается от общего процесса управления риском. Разница

Управление информационными активами

Этот процесс дает ответ на вопрос «Что мы защищаем?». Для определения информационных рисков в первую очередь необходим всегда актуальный перечень информационных активов, проранжированных по важности. Для этого в банке разработан процесс «Управление информационными активами» – это одна из ключевых, основополагающих процедур, обе-



Валентин
НИКОНОВ

Внедрение и сертификация системы менеджмента информационной безопасности вовсе не гарантирует избавления компании от рисков

заключается в технологии идентификации рисков и в определении стратегий управления ими. ISO 27001:2005 как раз содержит рекомендации о том, каким образом идентифицировать риски информационной безопасности (для этого необходимо внедрить соответствующие процессы, речь о которых пойдет далее) и каким образом их смягчать (для этого необходимо внедрить множество процедур).

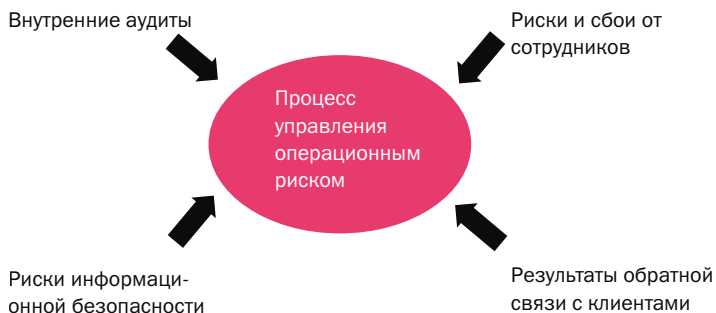
Общая логика системы управления операционным риском в соответствии с ISO 27001:2005 показана на рис. 4, из которого видно, что после интеграции системы ISO 27001:2005 операционные риски идентифицируются из четырех источников: «от сотрудников», по результатам анализа обратной связи с клиентом, на основе результатов внутренних аудитов, на основе идентификации рисков информационной безопасности. После того как риски идентифицированы, они проходят через стандартный процесс «отработки» риска (процесс управления риском типичен для всех видов рисков).

Управление рисками информационной безопасности

С организационной точки зрения процедуры управления рисками информационной безопасности курируются группой координации информационной безопасности, которая включает в себя представителей различных функциональных подразделений и занимается разработкой политик, целей в области информационной безопасности, систематическим анализом работы системы. Для идентификации рисков информационной безопасности в системе ISO 27001:2005 функционируют два процесса: управление информационными активами и управление информационными рисками. Эти два процесса задают общую логику системы (рис. 5).

Рис. 4

Система управления операционным риском



спечивающая функционирование системы. Логика здесь очень проста: поскольку информационные активы – это объекты, к изменению свойств которых приводит реализация рисков информационной безопасности, перечень этих объектов вместе с их свойствами должен быть перед глазами как у сотрудников отдела и группы координации информационной безопасности, так и у собственников бизнеса.

В банке разработан реестр информационных активов – это список, в котором отражены уровни конфиденциальности, целостности и доступности каждого актива и получающийся из них общий уровень критичности актива. Наряду с этим для каждого актива в реестре определен сотрудник (или подразделение), несущий ответственность за этот актив (то есть владелец информационного актива), и сотрудники (подразделения), которые этим активом пользуются. Процесс управления информационными активами – это процесс актуализации реестра. В общем виде он представлен в табл. 1.

Рис. 5

Логика системы менеджмента информационной безопасности



Управление информационными рисками

После получения ответа на вопрос «Что мы защищаем?» необходимо понять «От чего мы защищаем?». Для этого в системе функционирует процесс «Управление информационными рисками». По каждому информационному активу систематически определяются информационные риски, причем применяется как регулярная, системная, так и спонтанная идентификация рисков (когда любой сотрудник, который видит риск, может его зарегистрировать). Систематическая идентификация рисков информационной безопасности проходит в банке регулярно под эгидой отдела информационной безопасности. «Под эгидой» означает, что риски активов определяют их владельцы, а группируют и обрабатывают информацию сотрудники отдела информационной безопасности. Они же проводят количественную оценку и анализ рисков и в результате получают проранжированный перечень рисков, по каждому из которых (совместно с владельцами информационных активов) определяют стратегии управления. Отчет о рисках рассматривается группой координации информационной безопасности. Основная роль данной группы заключается в выделении ресурсов, необходимых для внедрения процедур, помогающих смягчить риски.

Внедрение мер управления рисками

Поняв, от чего мы защищаем активы, можно перейти к определению адекватных мер защиты – к внедрению стратегий управления рисками, которые определяются на основе анализа

рисков. Действия по смягчению информационных рисков внедряются в практику точно так же, как и любые другие стратегии управления операционными рисками, – через общий механизм.

В большинстве случаев смягчение рисков информационной безопасности подразумевает внедрение процедур: например, для смягчения риска несанкционированного доступа внедряется процедура «управление правами доступа пользователей». В приложении А к стандарту ISO 27001:2005 приведен перечень контролей – процедур, которые должны быть внедрены в организации для систематического смягчения рисков информационной безопасности. Это типовые методы смягчения некоторых рисков. Если организация соответствует риски не принимает, то эти процедуры обязательны к внедрению. Без детализации перечень процедур выглядит следующим образом:

- организация информационной безопасности;
- обеспечение безопасности персонала;
- обеспечение физической безопасности;
- операционный менеджмент;
- управление правами доступа;
- управление инцидентами информационной безопасности;
- приобретение, разработка и поддержка информационных систем;
- управление непрерывностью бизнеса;
- обеспечение соответствия законодательным требованиям.

Результат процесса управления рисками информационной безопасности можно свести в таблицу (табл. 2).

Если для управления риском в стандарте предусмотрено внедрение процедуры (контроля), в таблице делается ссылка на соответствующий пункт стандарта. Также важно, что при определении стратегии управления риском оценивается остаточный риск – то есть риск после внедрения процедур по его смягчению.

Как и в ситуации с любыми другими рисками, управление рисками информационной безопасности требует инвестиций. В принципе такие риски могут быть приняты высшим руководством (в «Банке24.ру» это председатель координации группы информационной безопасности). В этом случае в реестре рисков делается соответствующая отметка.

Таким образом, по результатам процесса управления рисками в банке был внедрен ряд процедур, направленных на систематическое адекватное обеспечение информационной безопасности. Эти процедуры регулярно оцениваются в ходе внутренних аудитов, что гарантирует их функционирование и задает основу для непрерывного повышения их эффективности.

Сертификация системы

Проект внедрения системы менеджмента

информационной безопасности в «Банке24.ру» реализовывался в течение 15 месяцев силами консалтинговой компании и сотрудников отдела информационной безопасности банка. В ходе проекта были идентифицированы тысячи информационных активов, было отработано около 380 рисков. Сегодня действие системы распространяется только на процессы обслуживания клиентов через интернет – услуги, для которых обеспечение информационной безопасности наиболее критично. В дальнейшем система будет распространена на все услуги банка. В проекте было задействовано 18 структурных подразделений банка, которые так или иначе участвовали во внедрении процедур, определенных международным стандартом ISO 27001:2005. Все эти действия были направлены на реальное предотвращение информационных рисков и на внедрение процессов, которые сделают управление информационными рисками системной деятельностью. Когда стало очевидно, что система менеджмента информационной безопасности созрела для сертификации, в банк были приглашены

посмотреть, не выкидывают ли сотрудники банка конфиденциальные документы в мусорные корзины. Для этого потребовалось довольно тщательно исследование последних. Со стороны процесс выглядел весьма забавно, но что поделать – в этом хлеб аудитора. Возможно, такая доскональность была навеяна получившим широкую огласку случаем, когда администрация Белого дома выкинула в помойку подробный график перемещения президента Буша во время одной из его поездок, документ, естественно, секретный. Всего в результате аудита была выявлено около 10 несоответствий, которые затем были зарегистрированы в системе, что означало, что по ним началась работа и что они пройдут стандартный цикл управления риском. В ходе следующего надзорного аудита работа по выявленным несоответствиям будет проанализирована в первую очередь. Внешние аудиты помогают реализовать процесс непрерывного улучшения менеджмента информационной безопасности. Международная сертификация в случаях, когда аудит проводится на высоком

ТАБЛИЦА 1 РЕЕСТР ИНФОРМАЦИОННЫХ АКТИВОВ

Name	Конфиденциальность	Целостность	Доступность	Критичность	Владелец	Пользователи
База данных по клиентам	Высокая	Высокая	Высокая	Высокая	Начальник отдела продаж	Отдел продаж

ТАБЛИЦА 2. РЕЗУЛЬТАТЫ ПРОЦЕССА УПРАВЛЕНИЯ РИСКАМИ

Риск	Мера, предложенная владельцем актива	Стоимость, руб.	Ответственный	Сроки	№ контроля
Проникновение неавторизованных лиц в закрытые зоны	Внедрение биометрической системы контроля доступа	X руб.	Служба безопасности	дд.мм.гггг – дд.мм.гггг	A 9/1

международные аудиторы для проведения независимой оценки – компания Bureau Veritas Certification (BVC). В ходе четырехдневного аудита были проанализированы все процедуры обеспечения информационной безопасности и все процессы, входящие в область сертификации.

В роли главного аудитора выступил сотрудник израильского отделения BVC Ярив Диамант, который выявил несколько слабых мест системы. Такая информация очень важна, поскольку внедрение системы – лишь начало пути ее непрерывного совершенствования, и информация о слабых местах системы необходима для повышения ее эффективности.

Аудит был проведен на высокопрофессиональном уровне – помимо прочего, оценивая обеспечение сохранности конфиденциальной информации, ведущий аудитор потрудился

профессиональном уровне, служит экспертизой, которая позволяет организации все время быть «в тонусе», а это необходимо для постоянного повышения конкурентоспособности бизнеса.

Внедрение и сертификация системы менеджмента информационной безопасности вовсе не гарантирует избавления компании от рисков. Главным результатом проекта стало не столько выявление конкретных рисков, сколько организация процесса систематического управления рисками информационной безопасности. Это означает, что банк готовится к возможной реализации рисков и внедряет механизмы, которые позволяют смягчить их последствия. Кроме того, за время реализации проекта сотрудники банка осознали важность информационной безопасности и знают, как действовать, если произошел инцидент. ■