

РОЛЕВАЯ МОДЕЛЬ СОТРУДНИКОВ БАНКОВСКОЙ ОРГАНИЗАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Введение

Цель любой организации достигается в результате скоординированных действий ее сотрудников. При этом сами действия, как правило, заранее планируются и распределяются между сотрудниками организации в виде отдельных задач (функций, обязанностей). При определении внутренних угроз информационной безопасности (ИБ) полномочия сотрудников, решающих эти задачи, определяют риски ИБ для организации. Одним из способов снижения таких рисков является целенаправленный контроль над распределением полномочий в организации, что связывают с управлением системой ролей с целью предотвращения угроз ИБ от персонала [1].

Особую важность приобретает решение проблемы рационального распределения ролей ИБ, что подтверждает базовый стандарт Банка России, определяющий общие требования по обеспечению информационной безопасности организаций банковской системы РФ, в том числе и при назначении и распределении ролей [2]. При этом под ролью понимается заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом. К субъектам относятся лица из числа руководителей банковской организации, ее персонала, клиентов или иницируемые от их имени процессы по выполнению действий над объектами. Объектами могут быть аппаратное средство, программное средство, программно-аппаратное средство, информационный ресурс, услуга, процесс, система, над которыми выполняются действия.

Сформулированные в стандарте требования носят общий характер и нуждаются в дальнейшей конкретизации с целью разработки рекомендаций по выделению и назначению ролей ИБ сотрудников банковской организации с учетом особенностей создания и функционирования ее системы обеспечения ИБ (СОИБ). В качестве методической разработки таких рекомендаций может быть использована соответствующая модель, описанная в данной работе.

1. Структура ролевой модели

Структуру ролевой модели сотрудника банковской организации в области ИБ можно определить на основе рассмотрения особенностей выполнения им своих обязанностей, отраженных в должностных инструкциях, которые непосредственно связаны с определением его функций, правил и ограничений при взаимодействии с различными объектами. Исходя из этого можно сформулировать расширенное понятие роли как совокупности функций работника (лица из числа персонала банковской организации), для выполнения которых необходим совокупный (по функциям — видам работ, выполняемых или планируемых к выполнению работником) набор полномочий. Такое определение роли позволяет предложить следующую модель ее описания (структура ролевой модели показана на рис. 1).

Каждой роли может соответствовать одна или несколько функций, связанных с обеспечением ИБ. Для выполнения определенной функции необходимы полномочия, каждое из которых устанавливает совокупность правил и ограничений, направленных на:

- информационный актив организации (тип информационных активов);
- объект среды информационной инфраструктуры организации (тип объектов среды);
- операцию, выполняемую или планируемую к выполнению над информационным активом путем использования объекта среды (типовая операция, выполняемая или планируемая к выполнению над типом информационных активов путем использования типов объектов среды).

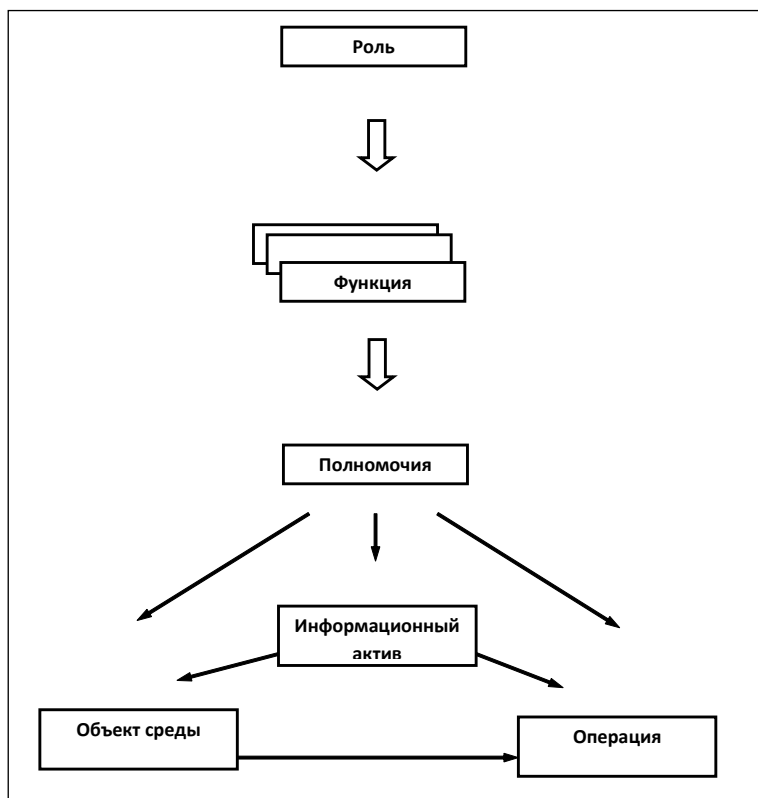


Рис. 1. Структура ролевой модели

Таким образом, роль можно рассматривать как некоторую совокупность полномочий, предоставленных одному или нескольким работникам банковской организации и имеющих ограничения (или запреты). При назначении и распределении ролей в области обеспечения ИБ целесообразно реализовать принцип разделения полномочий: формирование перечня полномочий, не допустимых для включения в одну роль, и совокупности ролей, не допустимых для назначения одному работнику.

2. Классификация ролей сотрудников банковской организации в области информационной безопасности

Разделение ролей на группы (категории) возможно с учетом особенностей структуры системы обеспечения ИБ, функций обеспечения ИБ и связанных с ними бизнес-процессов (рис. 2).

Базовый стандарт Банка России в области обеспечения ИБ [2] включает в структуру СОИБ систему информационной безопасности (СИБ – совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение) и систему менеджмента информационной безопасности (СМИБ – часть менеджмента банковской организации, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования СОИБ).

В банковской организации можно выделить две группы сотрудников, у которых основные должностные обязанности или не связаны, или связаны с обеспечением ИБ. Например, бухгалтер, обрабатывающий банковскую информацию с использованием автоматизированных рабочих мест (основные бизнес-процессы банка), реализует процессы защиты информации от несанкционированного доступа и от воздействия вредоносных программ (дополнительные обязанности). Сотрудник подразделения ИБ выполняет функции, связанные с обеспечением ИБ (основные обязанности, вспомогательные процессы в поддержку непрерывности основных бизнес-процессов банка). Следует отметить, что выделенные две группы сотрудников должны

обладать профессиональными компетенциями в области ИБ, существенно отличающимися по функциям, полномочиям и соответствующим им уровням знаний и умений.

Исходя из этого в банковской организации можно выделить две категории ролей ее работников, имеющих отношение к обеспечению ИБ (рис. 2):

1. Функциональные роли, выполняемые сотрудниками банка в качестве дополнительных обязанностей;
2. Роли ИБ, связанные с непосредственным обеспечением ИБ банковской организации (для сотрудников это основные функциональные обязанности).

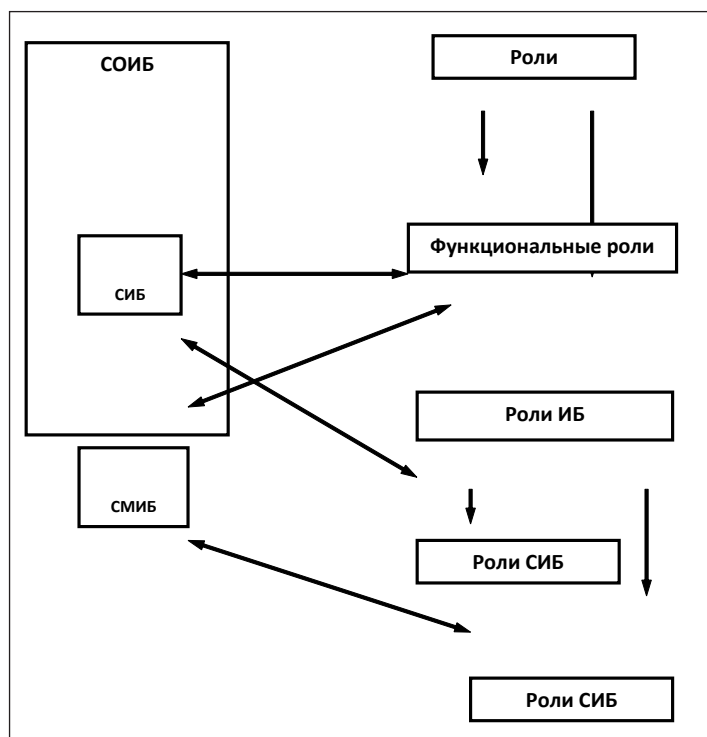


Рис. 2. Категории ролей

Функциональные роли связаны с функционированием СИБ (вышеприведенные примеры) или функционированием СМИБ. Последнее, например, относится к ролям администратора ИБ функционального подразделения банка. Целью выделения и назначения функциональных ролей является снижение риска инцидентов ИБ, связанных с недопустимой концентрацией полномочий, предоставленных работнику, а также с преднамеренным или случайным превышением полномочий, предоставленных работнику.

Роли ИБ могут быть разделены на две группы, связанные с СИБ и СМИБ соответственно. Основной целью выделения и назначения ролей ИБ является унификация, упорядочивание и, как следствие, повышение качества выполнения деятельности по обеспечению ИБ банковской организации.

Предлагаемое в данной работе категорирование ролей позволяет повысить эффективность контроля над распределением полномочий в банковской организации.

Все выделенные в банковской организации роли документируются. При этом для каждой из ролей

- назначаются ответственные за их выполнение из числа работников банковской организации;
- формируются и документируются квалификационные требования, определяющие необходимые знания, образование и (или) опыт работников, назначаемых на роль.

Рекомендуемым местом документирования квалификационных требований для работников, назначаемых на роль, являются документы, содержащие описание процессов деятельности, положения о структурных подразделениях и документация на автоматизированные банковские системы (АБС) организации.

Роли, назначенные работнику, а также ответственность за их выполнение фиксируются в документах, определяющих его должностные обязанности. Работникам не только определяются их функции и полномочия, но и выделяются ресурсы, необходимые и достаточные для выполнения назначенных им ролей.

Перейдем к более подробному рассмотрению выделенных категорий ролей.

3. Выделение и назначение функциональных ролей

В основу выделения и назначения функциональных ролей работников банковской организации можно положить принцип, определяющий, что эти работники выполняют всю свою деятельность (совокупность выполняемых функций) путем использования только тех полномочий, которые необходимы для выполнения предварительно назначенных работникам функциональных ролей. При этом использование работниками каких-либо дополнительных полномочий нежелательно.

В соответствии с положениями базового стандарта Банка России [2], выделение и назначение функциональных ролей является составной частью СМИБ банковской организации и, следовательно, может быть описано циклической моделью Деминга (на рис. 3 циклическое выполнение этапов планирования, реализации, проверки и совершенствования) [2, 3].

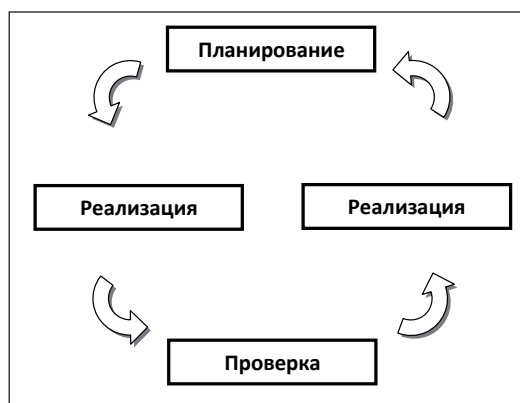


Рис. 3. Модель выделения и назначения функциональных ролей

На этапе «Планирование» выполняются определение и описание: области выделения и назначения функциональных ролей; различных перечней (*функций*, выполняемых работниками банковской организации в рамках области выделения и назначения функциональных ролей; *полномочий*, необходимых работникам банковской организации для выполнения этих функций; *ограничений*, которые содержат перечни полномочий, не допустимых для включения в одну функциональную роль; *ролей* и состава включенных в каждую роль полномочий; *ограничений*, которые содержат перечни ролей, не допустимых для назначения одному работнику; *работников* банковской организации, деятельность которых осуществляется в рамках области выделения и назначения функциональных ролей).

На этапе «Реализация» выполняются: административные операции (реализация операций просмотра и манипулирования перечнями, перечисленными выше); реализация элементов этих перечней; включение полномочий в роли; назначение и описание назначения функциональных ролей.

На этапе «проверка» выполняются контроль и анализ выделения и назначения функциональных ролей, контроль реализации административных операций.

На этапе «совершенствование» выполняется деятельность по принятию решения о реализации улучшений в выделении и назначении функциональных ролей и реализации административных операций.

Далее этапы периодически повторяются для снижения риска инцидентов ИБ, связанных с деятельностью работников функциональных подразделений банка. При этом целесообразно ориентироваться на следующие рекомендации, направленные на повышение качества процессов выделения и назначения функциональных ролей:

1. Каждому этапу сопоставить решение отдельных задач и связанных с этим процедур.
2. По каждой задаче (процедуре) определить исполнителей. Ими могут быть работники функциональных подразделений банковской организаций, вовлеченные в область выделения и назначения функциональных ролей (все этапы), работники подразделений информатизации (первый и второй этапы), работники службы ИБ (все этапы).

3. Работники банковской организации не должны обладать полномочиями для бесконтрольного создания, авторизации, уничтожения и изменения платежной информации, проведения несанкционированных операций по изменению состояния банковских счетов, модификации записей и полей баз данных.

4. Способ определения и описания перечня работников банковской организации (этап «Планирование») определяется способом задания области выделения и назначения функциональных ролей.

5. Способ реализации административных операций (этап «Реализация») определяется областью выделения и назначения функциональных ролей. Для автоматизированных банковских систем организации указанные операции могут быть реализованы как функциональные элементы их программной составляющей. Для процессов деятельности банковской организации или ее структурных подразделений указанные операции могут быть реализованы в виде документально определенного набора организационных мероприятий, выполняемых работниками банковской организации. Вне зависимости от способа реализации административных операций должны быть назначены ответственные из числа работников банковской организации за их выполнение. К административным операциям просмотра относятся следующие: операция получения всех элементов перечней работников банковской организации, ролей, полномочий, ограничений; операция получения перечня работников, которым назначена некоторая роль; операция получения перечня ролей, назначенных некоторому работнику; операция получения перечня полномочий, включенных в некоторую роль; операция получения перечня полномочий, которыми обладает некоторый работник; операция получения подмножества полномочий или ролей, не допустимых для использования в рамках одной роли или для назначения одному работнику соответственно и входящих в состав некоторого ограничения. К административным операциям манипулирования относятся следующие: операция создания/удаления элементов общих перечней работников банковской организации, ролей, полномочий, ограничений; операция назначения / отмены назначения работнику роли; операция включения/исключения полномочия в роль / из роли; операция включения/исключения полномочия в ограничение / из ограничения; операция включения/исключения роли в ограничение / из ограничения.

6. Назначение функциональных ролей работникам осуществляется путем связывания отдельных работников с отдельными ролями с учетом всех выделенных ограничений.

7. В целях контроля и анализа выделения и назначения функциональных ролей работникам банковской организации (этап «Проверка») целесообразно выполнять периодический контроль соответствия реальных полномочий работников банковской организации полномочиям, назначенным им в рамках выполнения процедур назначения функциональных ролей, а также проводить анализ назначенных работникам банковской организации функциональных ролей с целью выявления у них недопустимой концентрации полномочий и ролей.

3. Выделение и назначение функциональных ролей информационной безопасности работников банковской организации

В соответствии со структурой системы обеспечения ИБ банковской организации (рис. 2) состав ролей в организации, связанных с непосредственным обеспечением информационной безопасности организации, представляется целесообразным разделить на следующие две большие группы: роли ИБ для СИБ и роли ИБ для СМИБ. При этом исходя из требований к СИБ и к СМИБ, содержащихся в базовом стандарте Банка России [2], можно определить базовый состав ролей ИБ для каждой из этих групп:

для СИБ банковской организации:

- роли по назначению и распределению ролей и обеспечению доверия к персоналу;
- роли по обеспечению ИБ АБС на стадиях жизненного цикла;
- роли по обеспечению ИБ при управлении доступом и регистрации;
- роли по обеспечению ИБ средствами антивирусной защиты;
- роли по обеспечению ИБ при использовании ресурсов сети Интернет;
- роли по обеспечению ИБ средствами криптографической защиты информации;
- роли по обеспечению ИБ банковских платежных технологических процессов;
- роли по обеспечению ИБ банковских информационных технологических процессов;

для СМИБ банковской организации:

- роли службы ИБ;
- роли по определению/коррекции области действия СОИБ;
- роли по выбору/коррекции подхода к оценке рисков нарушения ИБ и проведению оценки рисков;
- роли по разработке планов обработки рисков нарушения ИБ;
- роли по разработке/коррекции внутренних документов, регламентирующих деятельность в области обеспечения ИБ;
- роли руководства банковской организации по принятию решений о реализации и эксплуатации СОИБ;
- роли по организации реализации планов внедрения СОИБ;
- роли по разработке и организации реализации программ по обучению и повышению осведомленности в области ИБ;
- роли по организации обнаружения и реагирования на инциденты безопасности;
- роли по организации обеспечения непрерывности бизнеса и его восстановления после прерывания;
- роли по мониторингу и контролю защитных мер;
- роли по проведению самооценки ИБ;
- роли по организации внешнего аудита ИБ;
- роли по проведению анализа функционирования СОИБ;
- роли по проведению анализа СОИБ со стороны руководства;
- роли по принятию решений по тактическим улучшениям СОИБ;
- роли по принятию решений по стратегическим улучшениям СОИБ.

Конкретный состав групп ролей ИБ для СИБ и СМИБ определяется на основе анализа их реализации в конкретной банковской организации, в том числе с учетом ресурсного и административного обеспечения.

Следующим этапом разработки ролевой модели сотрудников банковской организации в области обеспечения ИБ, структуры которой представлены на рис. 1 и 2, должна быть разработка для каждой из перечисленных выше ролей перечня функций и соответствующего им перечня полномочий.

4. Контроль выделения и назначения ролей ИБ работников банковской организации

Контроль выделения и назначения ролей ИБ банковской организации может быть осуществлен на основе требований базового стандарта Банка России [2]. Основными формами проведения контроля являются: проверка со стороны службы ИБ банковской организации, самооценка ИБ, внешний аудит ИБ, анализ функционирования СОИБ (в том числе со стороны руководства банковской организации).

Основными целями проведения контроля выделения и назначения ролей ИБ являются: контроль полноты выделения и назначения ролей ИБ, контроль выполнения ролей ИБ и контроль соответствия состава выделенных ролей требованиям комплекса стандартов Банка России в области обеспечения ИБ банковской организации.

Заключение

Учет требований комплекса стандартов Банка России «Обеспечение ИБ организаций банковской системы РФ» и анализ особенностей обеспечения ИБ в типовой банковской организации позволил описать ролевую модель ИБ сотрудников такой организации.

Модель базируется на определении категорий ролей работников банковской организации и включает описание функциональных ролей работников банковской организации с определением взаимосвязи между функциональными ролями, работниками, функциями и полномочиями и описание ролей ИБ работников банковской организации, структурированных на две группы (роли ИБ для СИБ и роли ИБ для СМИБ). Модель задает перечень типовых ролей ИБ, относящихся к этим группам.

Описание модели дополнено рекомендациями по выполнению этапов выделения и назначения функциональных ролей и по контролю выделения и назначения ролей ИБ работников банковской организации.

Представленные результаты целесообразно применить при разработке рекомендаций по созданию и эксплуатации системы обеспечения ИБ банковской организации в части определения влияния персонала организации на уровень обеспечения ИБ и снижения рисков ИБ, а также при разработке квалификационных требований, необходимых для подбора кадров и проведения аттестации, к сотрудникам банковской организации, имеющим отношение к обеспечению ИБ.

Описанная модель может стать основой для разработки профессиональных стандартов и формулирования профессиональных компетенций в качестве целевых показателей для образовательных учреждений, ведущих подготовку профессионалов в области обеспечения ИБ банковских систем.

СПИСОК ЛИТЕРАТУРЫ:

1. Андрианов В. В., Зефирова С. Л., Голованов В. Б., Голдусов Н. А. Обеспечение информационной безопасности бизнеса / Под общей ред. А. П. Курило. М.: ЦИПСИР; Альпина Паблишерз, 2011. — 373 с.
2. Стандарт Банка России СТО БР ИББС-1.0-2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
3. Нив Г. Пространство доктора Деминга. М.: Альпина Бизнес Букс, 2007. — 370 с.