*А. П. Курило (к. т. н., доцент), Н. Г. Милославская (к. т. н., доцент),*
*А. И. Толстой (к. т. н., доцент)*
Московский инженерно-физический институт (государственный университет)

# ПОДГОТОВКА СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ БАНКОВСКОЙ СФЕРЫ

Организации банковской сферы являются наиболее распространенными объектами, для которых актуальными являются требования по обеспечению информационной безопасности (ИБ). Потери от нарушения состояния защищенности банковской информации (конфиденциальности, целостности и доступности) могут иметь широкий диапазон последствий: от финансовых потерь отдельных физических или юридических лиц до кризиса финансовой системы отдельного государства.

Банковскую сферу (систему) Российской Федерации образуют Банк России, различные кредитные организации, включая Сбербанк, Внешторгбанк, Внешэкономбанк, региональные и др. банки, а также представительства и филиалы иностранных банков. Эти организации, решающие различные бизнес-задачи, обладают различными структурами, например, имеют или не имеют филиальную сеть.

Объединяющим для различных объектов банковской сферы являются банковская информация и банковские информационные технологии. Особенности банковской информации и банковских технологий позволяют выделить организации банковской сферы в отдельную типовую разновидность информационных объектов, для которых требуются отдельные подходы к обеспечению информационной безопасности как объекта в целом, так и отдельных его систем, например автоматизированных банковских платежных систем, информационных банковских систем, телекоммуникационных банковских систем, а также требуется отдельная целевая подготовка специалистов в области ИБ.

Подготовку специалистов с высшим образованием в области ИБ осуществляют в настоящее время более ста университетов России. Анализ опыта, накопленного при подготовке специалистов по ИБ в одном из ведущих университетов России — Московском инженерно-физическом институте (государственном университете), в котором на факультете «Информационная безопасность» имеется кафедра «Информационная безопасность банковских систем», позволяет сформулировать основные требования к уровню подготовки специалистов для банковской сферы. Для их формулирования целесообразно рассмотреть виды и задачи профессиональной деятельности выпускников университета, а также сформулировать их квалификационные характеристики.

В данной работе формулируются квалификационные характеристики специалистов по ИБ для организаций банковской сферы.

## 1. Определение квалификационных характеристик

Основные квалификационные характеристики специалиста с высшим образованием формулируются на основе определения его специальных (профессиональных) компетенций, важнейшей из которых является способность в рамках своей области деятельности решать определенные задачи и выполнять определенную работу.

Таким образом, формулирование квалификационных характеристик возможно только в случае рассмотрения отдельных типовых объектов, на которых решаются задачи обеспечения информационной безопасности и для этого привлекаются специалисты в области ИБ.

Такие квалификационные характеристики могут быть сформулированы на основе экспертных оценок ведущих специалистов в области информационной безопасности либо могут быть получены от конкретных организаций. К сожалению, второй подход на практике редко реализуем из-за отсутствия четкой системы, позволяющей объединять усилия отдельных типовых организаций по выработке конкретных квалификационных требований.

Следует отметить, что этот недостаток, относящийся к организациям банковской сферы России, в настоящее время преодолен с выходом в 2006 г. Стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». В тексте стандарта достаточно информации для формулирования квалификационных требований к специалистам, обеспечивающим функционирование системы защиты банковской информации.

**2. Исходная информация для формулирования квалификационных характеристик**

Сформулировать квалификационные характеристики можно на основе анализа

- тем работ, выполняемых студентами в конкретной организации банковской сферы во время практики и подготовки выпускной квалификационной работы (дипломного проекта);
- должностных обязанностей специалистов по информационной безопасности, работающих на конкретных объектах банковской сферы.

Рассмотрим более подробно эти два подхода.

1. В университетах России при подготовке специалистов по информационной безопасности общая длительность периода практики и выполнения выпускной квалификационной работы может достигать одного года. Например, для студентов МИФИ этот период составляет десятый и одиннадцатый семестры обучения и длится один год. Опыт выпуска специалистов с высшим образованием, накопленный с 1995 г., позволяет сгруппировать темы практики и дипломных проектов следующим образом:

- разработка технологий защиты информации;
- проектирование средств защиты информации;
- администрирование отдельных технологий обеспечения информационной безопасности;
- администрирование подсистемы информационной безопасности;
- проектирование подсистемы информационной безопасности конкретной автоматизированной системы;
- проектирование системы управления информационной безопасностью объекта в целом.

Необходимо отметить, что для информационных объектов банковской сферы характерными являются темы, относящиеся к администрированию отдельных информационных технологий и технологий защиты информации, к проектированию и администрированию подсистем информационной безопасности конкретных автоматизированных систем, а также проектирование систем управления информационной безопасностью объекта в целом. Проектирование средств защиты информации специально для информационных объектов банковской сферы не является актуальным.

2. Для того чтобы определить должностные обязанности специалистов по информационной безопасности, работающих на объектах банковской сферы, необходимо определить место информационной безопасности на этих объектах, роль службы информационной безопасности и направления деятельности таких специалистов. Такую информацию можно получить при анализе содержания Стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». Перед проведением такого анализа представляется целесообразным дать общую характеристику этого Стандарта.

**3.1. Общая характеристика Стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»**

В структуре Стандарта можно выделить следующие три части:

1. Формирование целей обеспечения информационной безопасности организации банковской системы Российской Федерации (базируется на определении исходной концептуальной схемы (парадигмы) обеспечения ИБ, основных принципов обеспечения ИБ, описании модели угроз и нарушителей ИБ и формулировании политики ИБ организации).

2. Реализация достижения целей обеспечения информационной безопасности организации. Эта часть стандарта определяет роль процессов управления (менеджмента) информационной безопасности организации.

3. Контроль за достижением целей информационной безопасности организации, базирующийся на проверке и оценке ИБ организации (мониторинг и аудит) и определении зрелости процессов менеджмента ИБ организации (описание модели зрелости).

При разработке рассматриваемого стандарта использовалось большое количество международных (14) и российских (11) стандартов и нормативных документов, причем часть российских стандартов имеет аналоги зарубежных стандартов. В их числе

- ISO/IEC IS 27001-2005 Information technology. Security techniques. Information security management systems. Requirements;
- ISO/IEC IS 27002-2007 Information Technology. Code of practice for information security management.

Приведем перечень разделов Стандарта:

1. Область применения.
2. Нормативные ссылки.
3. Термины и определения.
4. Обозначения и сокращения.
5. Исходная концептуальная схема (парадигма) обеспечения ИБ организаций БС РФ.
6. Основные принципы обеспечения ИБ организаций БС РФ.
7. Модели угроз и нарушителей ИБ организаций БС РФ.
8. Политика ИБ организаций БС РФ.
9. Система менеджмента ИБ организаций БС РФ.
10. Проверка и оценка ИБ организаций БС РФ.
11. Модель зрелости процессов менеджмента ИБ организаций БС РФ.
12. Направления развития стандарта.

Библиография

Анализ содержания отдельных разделов Стандарта позволяет получить исходную информацию для формулирования квалификационных характеристик специалистов по ИБ для организаций банковской сферы.

Далее рассмотрим некоторые положения Стандарта.

### 3.2. Место информационной безопасности на объекте

Стандарт определяет место информационной безопасности на объекте банковской системы (п. 5.2 Стандарта): *процессы по обеспечению ИБ — вид вспомогательных процессов, реализующих поддержку (обеспечение) процессов основной деятельности организации в целях достижения ею максимально возможного результата. При этом определяется, что деятельность организации осуществляется через реализацию трех групп высокоуровневых процессов: основные процессы (процессы основной деятельности), вспомогательные процессы (процессы по видам обеспечения) и процессы менеджмента (управления) организацией.*

Таким образом, все процессы, связанные с обеспечением ИБ на информационном объекте, должны способствовать основному бизнесу организации. Следовательно, при подготовке специалистов по информационной безопасности должны учитываться особенности объектов защиты, что должно отражаться на квалификационных характеристиках.

*Целью ИБ на объекте является выстраивание оптимальной системы защиты, обеспечивающей необходимый уровень защищенности информационных ресурсов. Этот уровень определяется на основе анализа рисков ИБ, которые должны быть согласованы с рисками основной (бизнес) деятельности организации* (п. 5.1 Стандарта).

При этом необходимо учитывать тот факт, что любая целенаправленная деятельность организации порождает риски, сущность которых — естественная неопределенность будущего. Это — объективная реальность, и понизить эти риски можно лишь до уровня неопределенности сущностей, характеризующих природу бизнеса. Оставшаяся часть риска, определяемого факторами среды деятельности организации,

на которые организация не в силах влиять, должна быть неизбежно принята. В данном случае обеспечение ИБ на объекте должно реально снижать риски безопасности до заданного уровня.

### 3.3. Роль службы информационной безопасности на объекте

Для того чтобы уточнить роль службы ИБ в организации, необходимо определить объекты, которые могут взаимодействовать друг с другом в условиях появления рисков, связанных с информационной безопасностью. В данном случае Стандарт определяет в качестве таких объектов владельца информационными активами организации и злоумышленника, стремящегося оказать воздействие на эти активы.

К информационным активам организации банковской системы Российской Федерации Стандарт относит различного вида банковскую информацию (платежную, финансово-аналитическую, служебную, управляющую и пр.) на всех фазах ее жизненного цикла (генерация (создание), обработка, хранение, передача, уничтожение).

Роль службы ИБ в организации определяется задачами, которые она должна выполнять в условиях противоборства собственника и злоумышленника за контроль над информационными активами.

Обеспечение информационной безопасности на объекте — это процесс, которым необходимо эффективно управлять. Основная роль службы ИБ определяется стратегией обеспечения ИБ организации, которая *заключается в развертывании, эксплуатации и совершенствовании системы менеджмента ИБ (СМИБ)* (п. 5.17 Стандарта).

При этом менеджмент ИБ есть часть общего корпоративного менеджмента организации, которая ориентирована на содействие достижению целей деятельности организации через обеспечение защищенности ее информационных ресурсов. Менеджмент ИБ не должен рассматриваться как самостоятельный вид деятельности в организации. Система менеджмента ИБ организаций — часть общей системы менеджмента, основывающаяся на подходе бизнес-риска, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения ИБ организации (ISO/IEC IS 27001).

### 3.4. Направления деятельности специалистов по ИБ

При определении основных направлений деятельности специалистов по ИБ в организации банковской сферы необходимо учитывать следующее:

1. Наиболее правильный и эффективный способ добиться минимизации рисков нарушения ИБ для собственника — разработать на основе точного прогноза, базирующегося в том числе и на анализе и оценке рисков ИБ, политику ИБ организации и в соответствии с ней реализовать, эксплуатировать и совершенствовать систему менеджмента ИБ организации (п. 5.8 Стандарта). Такой прогноз может и должен составляться с учетом опыта ведущих специалистов банковской системы, а также с учетом международного опыта в этой сфере (п. 5.10 Стандарта).

2. Политика ИБ организаций БС РФ разрабатывается на основе принципов обеспечения ИБ организаций БС РФ, моделей угроз и нарушителей, идентификации активов, подлежащих защите, оценки рисков с учетом особенностей бизнеса и технологий, а также интересов конкретного собственника (п. 5.9 Стандарта).

3. Соблюдение политики ИБ в значительной степени является элементом корпоративной этики, поэтому на уровень ИБ в организации серьезное влияние оказывают отношения как в коллективе, так и между коллективом и собственником или менеджментом организации, представляющим интересы собственника. Поэтому этими отношениями необходимо управлять (п. 5.11 Стандарта).

4. Обеспечение ИБ организации включает реализацию и поддержку процесса осознания ИБ и процессов менеджмента ИБ (п. 5.16 Стандарта). Осознание ИБ обеспечивает основу эффективного функционирования СМИБ организации, где под эффективностью понимается соотношение между достигнутым результатом и использованными ресурсами.

5. Для реализации задач развертывания и эксплуатации СМИБ организации рекомендуется иметь в своем составе службу ИБ (п. 9.7.1 Стандарта).

6. Для администрирования подсистем ИБ отдельных автоматизированных банковских систем Стандарт предполагает наличие в организации банковской сферы специалистов, выполняющих обязанности администраторов информационной безопасности (п. 8.2.9.5 Стандарта), и формулирует основные требования к таким специалистам.

С учетом этого, а также с учетом определенных ранее места ИБ и роли службы ИБ на объекте можно сформулировать основные направления деятельности и квалификационные характеристики специалиста по ИБ в организациях банковской сферы.

**4. Основные направления деятельности и квалификационные характеристики**

Основные направления деятельности специалистов по ИБ в организациях банковской сферы определяются видами их профессиональной деятельности. Учет требований Стандарта и тематики выпускных квалификационных работ позволяет определить следующие основные виды профессиональной деятельности:
- технологическая (обеспечение функционирования основных технологий защиты информации);
- организационно-технологическая (обеспечение функционирования системы менеджмента ИБ).

Квалификационные требования определяются видами решаемых задач и требованиями к уровню знаний и умений.

Решаемые задачи (специальные компетенции):
- Формирование целей обеспечения ИБ на объекте на основе идентификации активов объекта, анализа угроз, оценки рисков ИБ, определения основных принципов обеспечения ИБ и формулирования политики ИБ объекта.
- Реализация целей обеспечения ИБ на объекте на основе развертывания, эксплуатации и совершенствования системы менеджмента ИБ.
- Контроль за достижением целей обеспечения ИБ на объекте на основе реализации процессов мониторинга, проведения самооценки уровня ИБ объекта и обеспечения поддержки эффективного аудита текущего уровня ИБ объекта и определения уровня зрелости менеджмента ИБ объекта.

При этом специалисты по ИБ должны

*знать:*
- нормативную базу, связанную с обеспечением ИБ;
- принципы обеспечения ИБ;
- методы оценки рисков ИБ;
- основные методы менеджмента ИБ организации;

*уметь:*
- описать модели угроз и нарушителей ИБ;
- разработать политику информационной безопасности;
- проводить анализ рисков ИБ на объекте;
- проектировать, развертывать, эксплуатировать и совершенствовать систему менеджмента ИБ;
- администрировать подсистемы ИБ отдельных информационных технологий и автоматизированных систем;

*иметь представление:*
- о методах построения систем управления объектами;
- о методах мониторинга и аудита систем;
- об особенностях психологии и этики отношений в коллективе.

В качестве примера можно привести перечень работ, которые должен выполнять специалист по ИБ, работающий в службе безопасности организации банковской сферы (п. 9.7.1 Стандарта):
- управлять всеми планами по обеспечению ИБ организации;
- разрабатывать и вносить предложения по изменению политики ИБ организации;
- изменять существующие и принимать новые нормативно-методические документы по обеспечению ИБ организации;

- выбирать средства управления и обеспечения ИБ организации;
- контролировать пользователей, в первую очередь пользователей, имеющих максимальные полномочия;
- контролировать активность, связанную с доступом и использованием средств антивирусной защиты, а также связанную с применением других средств обеспечения ИБ;
- осуществлять мониторинг событий, связанных с ИБ;
- расследовать события, связанные с нарушениями ИБ, и в случае необходимости выходить с предложениями по применению санкций в отношении лиц, осуществивших противоправные действия, например нарушивших требования инструкций, руководств и т. п. по обеспечению ИБ организации;
- участвовать в действиях по восстановлению работоспособности автоматизированных систем после сбоев и аварий;
- создавать, поддерживать и совершенствовать систему управления ИБ организации.

**Заключение**

На основе анализа содержания Стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» определены квалификационные требования к специалистам с высшим образованием в области информационной безопасности, которые могут быть востребованы для работы в организациях банковской сферы. Эти квалификационные требования обладают универсальностью и не зависят от особенностей национальных банковских систем. Кроме этого, процесс формулировки квалификационных требований может быть использован и для составления квалификационных требований для специалистов, относящихся к другим типовым объектам. На базе сформулированных квалификационных требований можно определить требования к конкретным учебным планам и к содержанию обучения.