А. И. Толстой

ПОЛИТИКА КАДРОВОГО ОБЕСПЕЧЕНИЯ РЕШЕНИЯ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Введение

Эффективное решение задач обеспечения информационной безопасности (ИБ) на конкретном объекте во многом зависит от организации профессиональной деятельности, которая определяется уровнем формирования необходимых служб и уровнем соответствия квалификации исполнителей содержанию этих задач.

Необходимо отметить, что практическая деятельность по кадровому обеспечению решения задач ИБ на данном временном этапе отличается существенным дефицитом рынка труда в профессионалах определенного уровня. Поэтому создание условий оптимизации этой деятельности может быть отнесено к факторам, непосредственно влияющим на оптимальность достижения защищенности информационных активов. В данном случае можно говорить о необходимости разработки политики кадрового обеспечения решения задач ИБ. Причем эта политика может быть разработана исключительно для конкретной организации, имеющей свои бизнес-интересы, функционирующей для достижения конкретных бизнес-целей и реализующей определенные бизнес-процессы в условиях существования актуальных угроз в информационной сфере.

Данная работа посвящена определению основных требований, которые необходимо учесть при разработке политики кадрового обеспечения решения задач ИБ конкретной организации (далее — Политика).

1. Понятие политики применительно к кадровому обеспечению решения задач ИБ

Под политикой организации, как правило, понимается система правил, в соответствии с которой действуют люди, входящие в организацию. Важнейшая составная часть стратегически ориентированной политики организации — ее кадровая политика, представляющая собой в широком смысле систему осознанных и определенным образом сформулированных и закрепленных правил и норм, приводящих человеческий ресурс в соответствие с долговременной стратегией организации. Цель кадровой политики — обеспечение оптимального баланса процессов обновления и сохранения численного и качественного состава кадров в соответствии с потребностями самой организации, требованиями действующего законодательства и состоянием рынка труда [1].

Частью кадровой политики является политика кадрового обеспечения задач, решаемых в организации. В ней формулируются нормы и правила формирования и поддержания на определенном уровне кадрового состава соответствующих подразделений организации. Причем в организации может существовать несколько политик кадрового обеспечения в зависимости от специфики и разнообразия решаемых задач.

Таким образом, можно говорить о наличии иерархии политик организации, характеризуемой структурой, представленной на рис. 1. Ее анализ показывает, что политику кадрового обеспечения решения задач ИБ можно отнести к категории частных политик организации. Совокупность политик кадрового обеспечения по отдельным тематическим группам задач составляет политику кадрового обеспечения организации, которая определяет принципы подбора и адаптации трудовых ресурсов, принципы подготовки, обучения и аттестации сотрудников организации, а также требования к реализации этой политики.

Кадровая политика организации образуется добавлением к политике кадрового обеспечения следующих аспектов, относящихся ко всей организации [1]:

- общие принципы кадровой политики, определение и приоритеты целей;
- создание и поддержка системы движения кадровой информации;

- принципы распределения средств, обеспечения эффективной системы стимулирования труда;
- анализ соответствия кадровой политики и стратегии организации, выявление проблем в кадровой работе, оценка кадрового потенциала.

При разработке политики кадрового обеспечения должны быть реализованы основные принципы: тесная ее связь с политикой более высокого уровня, направленность ее реализации на достижение основных бизнес-целей организации.

Рис. 1. Структура иерархии политик организации

2. Структура политики кадрового обеспечения решения задач ИБ

Формулирование норм и правил формирования и поддержания на определенном уровне кадрового состава подразделений организации, решающих задачи ИБ, возможно в рамках следующих разделов Политики, определяющих ее структуру:

1. Цели и задачи Политики;
2. Принципы формирования Политики;
3. Цели формирования подразделений организации, решающих задачи обеспечения ИБ (подразделения ИБ);
4. Принципы формирования задач ИБ, которые должны решать сотрудники подразделений ИБ организации;
5. Требования к номенклатуре должностей сотрудников подразделений ИБ;
6. Требования к должностным обязанностям сотрудников подразделений ИБ;
7. Порядок подбора кадров;
8. Порядок поддержки квалификации кадров;
9. Порядок аттестации кадров;
10. Требования к реализации Политики.

3. Рекомендации по разработке политики кадрового обеспечения решения задач ИБ

Политика непосредственно связана с кадровой политикой организации. Поэтому их цели близки. В данном случае цели Политики следуют из целей кадровой политики [1]: достижение оптимального баланса процессов обеспечения численного и качественного состава кадров, решающих задачи ИБ, в соответствии с потребностями самой организации, требованиями действующего законодательства и состоянием рынка труда.

Задачи, решаемые Политикой, должны обеспечить оптимальный путь достижения ее целей:

- определение целей формирования подразделений ИБ организации;
- формулирование принципов формирования задач ИБ, которые должны решать сотрудники подразделений ИБ организации;

• определение требований к номенклатуре должностей сотрудников подразделений ИБ организации и требований к их должностным обязанностям;

• определение порядка подбора кадров, поддержки их квалификации и проведения аттестации;

• определение требований к реализации Политики.

Следует отметить, что структура Политики, представленная выше, непосредственно следует из перечня ее задач.

К принципам формирования Политики можно отнести:

• согласованность штатного состава сотрудников подразделений ИБ организации и их квалификации с задачами ИБ, которые должны решаться в организации;

• оптимальность баланса процессов обеспечения численного и качественного состава кадров, решающих задачи ИБ;

• согласованность с требованиями действующего законодательства;

• согласованность с состоянием рынка труда в области ИБ;

• адаптивность процессов кадрового обеспечения решения задач ИБ в организации к изменению состава и содержания этих задач;

• управляемость процессами кадрового обеспечения решения задач ИБ в организации.

Необходимость реализации первых двух принципов позволяет определить цели формирования подразделений ИБ организации — это достижение согласованности штатного состава сотрудников подразделений ИБ организации и их квалификации с задачами ИБ, которые должны решаться в организации, достижение оптимальности баланса процессов обеспечения их численного и качественного состава, а также оптимизация финансирования деятельности подразделений ИБ.

Задачи по обеспечению ИБ в организации должны быть структурированы с учетом объектов защиты, выделенных в организации (например, таких, как автоматизированные системы обработки информации, информационные системы, информационные технологии, информационные активы), с учетом разнообразия мер защиты информации, используемых на объектах защиты (например, организационные меры, криптографические, технические, программные и программно-аппаратные методы и средства) и с учетом методов управления информационной безопасностью, а также с учетом рекомендаций различных стандартов и нормативных документов. Такое структурирование позволяет оптимизировать процессы, связанные с определением номенклатуры должностей сотрудников подразделений организации, с определением их должностных обязанностей и с определением требований к уровню их квалификации.

Взаимосвязанность этих процессов поясняет рис. 2. Если задать границы области определения задач ИБ, которые должны решаться в организации, области должностных обязанностей сотрудников организации, решающих эти задачи, и области квалификационных характеристик, которыми они должны обладать, то идеальным вариантом будет случай, когда эти области будут совпадать: должностные обязанности точно соответствуют задачам, а квалификация сотрудников полностью соответствует задачам и требуемым должностным обязанностям. В противном случае возможны следующие варианты:

1. Область должностных обязанностей не покрывает область задач ИБ. Следствием является снижение уровня обеспечения ИБ за счет отсутствия решения определенных задач.

2. Область должностных обязанностей покрывает область задач ИБ. Следствием является избыток должностных обязанностей, что приводит к отсутствию оптимальности штатного расписания подразделений ИБ и неоправданным финансовым тратам.

3. Область квалификационных характеристик не покрывает область должностных обязанностей. Это приводит к тому, что часть сотрудников из-за своей неподготовленности не может выполнять

определенные должностные обязанности и, соответственно, решать задачи ИБ. Выходом из этого положения является или замена персонала подразделения, или проведение его обучения.

4. Область квалификационных характеристик превышает область должностных обязанностей. Несмотря на то что квалификация сотрудников подразделения достаточна для решения задач ИБ и полностью соответствует должностным обязанностям, ситуацию можно назвать неоптимальной. В этом случае появляются риски нарушения ИБ как следствия возможного «перерождения» в нарушителей ИБ тех сотрудников, которые обладают более обширными квалификационными характеристиками, из-за недовольства занимаемой должностью и оплатой своего труда. Выходом из положения могут быть повышенное внимание к работе с кадрами, внедрение дополнительных контрольных мероприятий и оптимизация распределения должностных обязанностей.

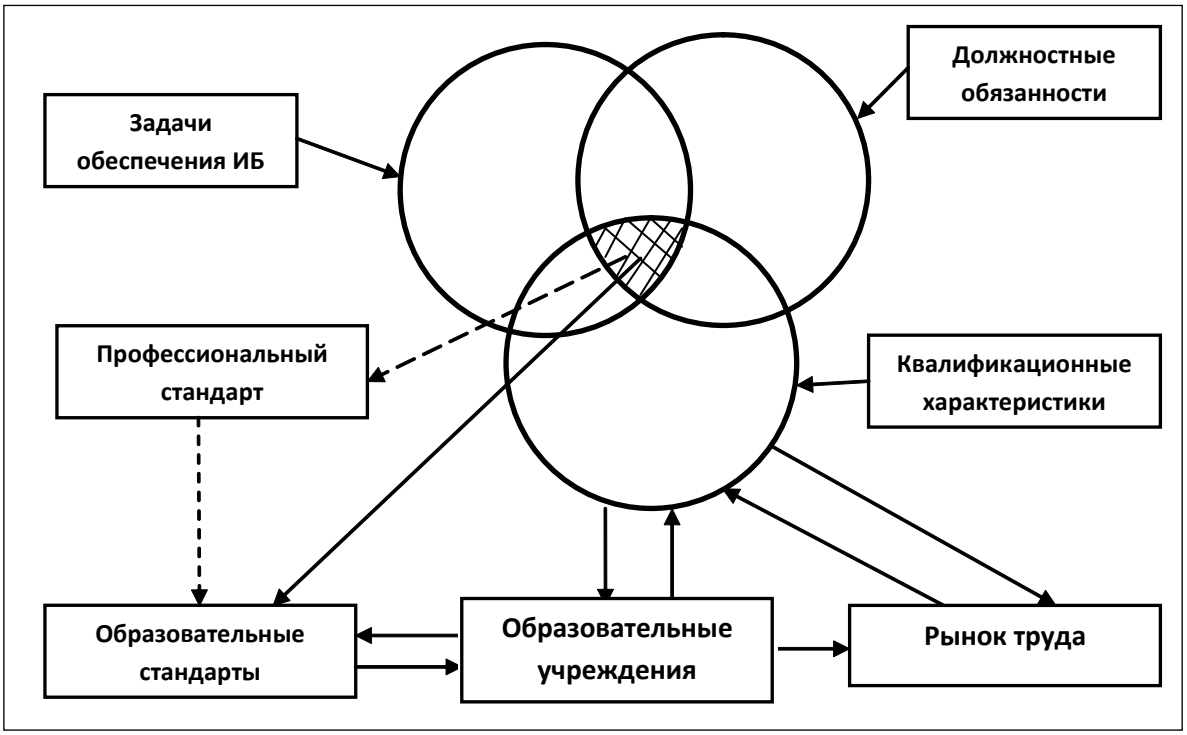

Рис. 2. Структура процессов кадрового обеспечения

Рассмотрение взаимосвязей процессов, относящихся к определению номенклатуры должностей сотрудников подразделений организации, их должностных обязанностей и квалификационных требований (рис. 2), позволяет с учетом специфики организации сформулировать в Политике соответствующие требования и к номенклатуре должностей, и к должностным обязанностям сотрудников подразделений ИБ, и к порядку подбора кадров. При этом целесообразно учесть опыт, накопленный различными организациями и отраженный в существующих нормативных документах.

Следует отметить, что роль базового нормативного документа может быть отдана профессиональному стандарту, содержащему информацию о должностях сотрудников подразделений, решающих задачи ИБ, соответствующих им должностных обязанностях и требуемых для этого квалификационных характеристиках (на рис. 2 этому соответствует пересечение трех областей). К сожалению, в области ИБ таких профессиональных стандартов пока нет.

Определенную информацию можно получить из следующих источников:

1. Единый квалификационный справочник должностей руководителей, специалистов и служащих, раздел «Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации» [2].

В этом документе для ограниченной области, относящейся к обеспечению ИБ (что затрудняет его широкое использование), определены две группы должностей (таблица 1) и для каждой должности сформулированы:

- должностные обязанности (основные трудовые функции, которые могут быть поручены полностью или частично работнику, занимающему данную должность, с учетом технологической однородности и взаимосвязанности работ, позволяющих обеспечить оптимальную специализацию служащих);
- требования к уровням знаний, предъявляемые к работнику в отношении специальных знаний, а также знаний законодательных и иных нормативных правовых актов, положений, инструкций и других документов, методов и средств, которые работник должен применять при выполнении должностных обязанностей (что специалист должен знать);
- требования к квалификации (определяют уровень профессиональной подготовки работника, необходимый для выполнения должностных обязанностей, требования к прохождению повышения квалификации и квалификационной аттестации, а также требования к стажу работы).

Таблица 1. Группы должностей и должности работников

Группы должностей	**Должности**
Руководители	Главный специалист по технической защите информации
	Начальник отдела (лаборатории, сектора) по противодействию техническим разведкам
	Начальник отдела (лаборатории, сектора) по технической защите информации
Специалист	Специалист по обеспечению безопасности информации в КСИИ
	Специалист по противодействию техническим разведкам
	Специалист по технической защите информации
	Администратор по обеспечению безопасности информации
	Инженер по технической защите информации
	Инженер-программист по технической защите информации
	Техник по технической защите информации

Эта информация может быть использована для решения вопросов, связанных с регулированием трудовых отношений, управлением персоналом организаций в сфере компетенции ФСТЭК России независимо от форм собственности и организационно-правовых форм, что должно способствовать правильному подбору и расстановке кадров, повышению их деловой квалификации, рациональному разделению труда, созданию действенного механизма разграничения функций, полномочий и ответственности между определенными категориями работников, а также установлению единых подходов в определении их должностных обязанностей и предъявляемых к ним квалификационных требований [2].

2. Комплект Федеральных государственных образовательных стандартов (ФГОС) третьего поколения укрупненного образовательного направления 090000 – «Информационная безопасность». ФГОСы предназначены для организации и методической поддержки в образовательных учреждениях подготовки кадров с высшим профессиональным образованием (бакалавры, магистры, специалисты по семи специальностям) и со средним профессиональным образованием (три специальности). Место образовательных стандартов в структуре процессов кадрового обеспечения показано на рис. 2.

В каждом ФГОСе сформулированы профессиональные компетенции, которыми должен обладать выпускник, успешно освоивший основную образовательную программу определенного образовательного уровня [3]. Под компетенцией понимается способность применять знания, умения и личностные качества для успешной деятельности в определенной области. Профессиональные компетенции базируются на определении области, объектов, видов и задач профессиональной деятельности и на сопоставлении профессиональным компетенциям квалификационных характеристик в виде требований к уровням знаний, умений и владения определенными навыками.

К сожалению, во ФГОСах отсутствует достаточная детализация и профессиональных компетенций, и связанных с ними характеристик (что соответствует направленности этих документов), а также нет привязки к должностям, которые могут занимать выпускники образовательных учреждений. Кроме этого, разработка ФГОСов не базировалась на профессиональных стандартах (по причине их отсутствия в области ИБ). Следствием этого являются ограниченные возможности этих документов для использования при кадровом обеспечении выполнения задач ИБ.

3. Нормативные документы международного уровня и иностранных государств, в которых обобщены лучшие практики в рассматриваемой области.

В данном случае как пример рассмотрим рекомендации нормативного документа, разработанного в Департаменте национальной безопасности США [4]. При этом некоторые определения мы дадим не в дословном переводе, а адаптированными к принятым в отечественной практике.

В цитируемом документе выделено десять обобщенных должностей, на которые обычно нанимают работников — специалистов в области ИБ государственные и коммерческие организации. Каждая такая должность представляет собой группу должностей под общим названием, в соответствии с которыми на рабочих местах выполняются схожие функции, что требует у работников наличия одинаковых компетенций в области обеспечения ИБ. Эти должности разбиты на три легко контролируемые и управляемые группы: исполнительные, функциональные и дополнительные. Рассмотрим эти должности с привязкой к конкретной группе.

Исполнительные должности:

1. *Главный специалист по ИБ* (англ. *Chief Information Security Officer, CISO*) решает в организации стратегические задачи по обеспечению ИБ и отвечает в пределах организации за стратегическое использование и управление информацией, информационными системами (ИС) и информационными технологиями (ИТ). Он устанавливает и следит за показателями (метриками) выполнения программы реализации корпоративной политики обеспечения информационной безопасности, включая оценку ее согласованности, эффективности и результативности. Он руководит оценкой новых и только появляющихся технологий обеспечения ИБ. Возможный вариант названия должности: Главный специалист по рискам ИБ.

2. *Специалист по ИБ* (англ. *Information Security Officer, ISO*) специализируется в области реализации стратегий обеспечения ИБ в пределах организации. На него возлагается ответственность за разработку и последующее приведение в исполнение в организации частных политик и процедур обеспечения ИБ, обеспечения непрерывности бизнеса и планов восстановления после аварий, ответственность за контроль соответствия принятых решений в организации требованиям вышестоящих уровней, а также за реализацию программ обучения сотрудников организации в области ИБ. Возможный вариант названия должности: Руководитель отдела ИБ; Специалист по кибербезопасности; Специалист по безопасности; Старший специалист отдела ИБ.

3. *Специалист по проверке соответствия обеспечения ИБ* (англ. *IT Security Compliance Professional*) несет ответственность за наблюдение, оценку и обеспечение соблюдения международной, национальной, ведомственной нормативно-правовой базы, имеющей отношение к организации. Работники на данной должности решают множество задач, охватывающих

проблемы соблюдения норм и выполнения требований внутренних и внешних нормативных документов, включая руководство и проведение внутренних обследований, помощь работникам в соблюдении внутренних политик и процедур, а также предоставление информации специалистам, ответственным за вопросы соблюдения внешних норм во время независимой внешней оценки (аудита). Данный специалист обеспечивает руководство и автономную оценку организации с точки зрения выполнения требований по ИБ и предоставляет информацию для принятия управленческих решений на уровне всей организации. Возможный вариант названия должности: Аудитор ИБ; Генеральный инспектор; Инспектор/Исследователь; Аналитик по нормативным делам.

Функциональные должности:

4. *Специалист по компьютерной форензике* (англ. *Digital Forensics Professional*) выполняет множество высокотехничных видов анализа и процедур по сбору, обработке, сохранению, анализу и представлению доказательств компьютерных преступлений, включая поиск данных, взлом паролей и нахождение спрятанной или невидимой информации, но не ограничиваясь этим. Возможный вариант названия должности: Специалист-аналитик по компьютерной форензике; Специалист по компьютерной форензике, Специалист-практик по компьютерной форензике; Инженер по компьютерной форензике.

5. *Инженер по защите информации* (англ. *IT Security Engineer*) применяет междисциплинарные знания в области обеспечения ИБ для создания систем, использующих ИТ, которые устойчивы к различным злоумышленным действиям, ошибкам и непредвиденным ситуациям. Возможный вариант названия должности: Инженер по обеспечению ИБ; Специалист-аналитик по требованиям в области обеспечения ИБ; Специалист-аналитик по вопросам безопасности; Разработчик защиты; Криптоаналитик; Инженер по безопасности; Разработчик ПО; Системный инженер.

6. *Специалист по защите информации* (англ. *IT Security Professional*) сосредотачивает свою деятельность на защите информации и ИС от несанкционированного доступа, использовании методов и средств для обеспечения конфиденциальности, целостности и доступности. Возможный вариант названия должности: Специалист по обеспечению ИБ; Директор программы обеспечения ИБ (Директор по ИБ); Разработчик безопасности организации; Специалист по защите информационных систем; Специалист по ИБ; Управляющий программой обеспечения ИБ; Управляющий защитой ИС.

7. *Специалист по защищенному функционированию и эксплуатации компьютерных систем* (англ. *IT Security Operations and Maintenance Professional*) обеспечивает защиту информации и ИС на стадиях их жизненного цикла. Возможный вариант названия должности: Специалист по защищенному функционированию и эксплуатации ИТ-систем; Специалист по защищенному функционированию и эксплуатации ИС; Администратор баз данных; Администратор служб каталогов; Сетевой администратор; Сотрудник группы обслуживания; Системный администратор; Сотрудник группы технической поддержки.

Дополнительные должности:

8. *Специалист по физической защите* (англ. *Physical Security Professional*) защищает физическими методами и средствами компьютерные системы, помещения, где они размещаются, и оборудование от вторжений, огня и других естественных или стихийных опасностей. Возможный вариант названия должности: Специалист по защите аппаратуры; Администратор физической защиты; Специалист по физической защите.

9. *Специалист режимно-секретного отдела* (англ. *Privacy Professional*) отвечает в организации за разработку и управление программой в области соблюдения конфиденциальности. Он организует секретное делопроизводство, устанавливает систему должного обращения с персональными данными, а также обеспечивает управление ими на всех стадиях их жизненного цикла, начиная со сбора

и заканчивая уничтожением. Возможный вариант названия должности: Главный специалист режимно-секретного отдела; Специалист по правовым актам в области режима секретности; Специалист по соблюдению режима секретности; Специалист по персональным данным.

10. *Специалист по снабжению* (англ. *Procurement Professional*) закупает или ведет переговоры по продуктам (например, по программному или аппаратному обеспечению) и услугам (например, по гарантийному обслуживанию), обеспечивающим реализацию политики ИБ организации, а также функционирование ИТ организации. В контексте обеспечения ИБ специалист по снабжению должен гарантировать, что требования ИБ учтены при проведении тендеров и отражены в договорах и закупаются только те продукты и услуги, которые отвечают таким требованиям. Он должен быть хорошо осведомлен о своей отрасли и своей организации и успешно взаимодействовать с поставщиками и договариваться об условиях обслуживания. Возможный вариант названия должности: Управляющий отдела снабжения; Менеджер по снабжению; Снабженец; Специалист по договорам (контрактам); Технический представитель специалиста по договорам.

Сотрудники организации, занимающие эти должности, могут выполнять следующие виды профессиональной деятельности:

- организационно-управленческая (управление);
- проектная (разработка);
- эксплуатационная (реализация, внедрение);
- контрольно-аналитическая (оценка);
- научно-исследовательская (наука — теория и методология, проведение научных исследований, защита диссертации);
- педагогическая (преподавательская деятельность).

Для реализации этих видов профессиональной деятельности специалисты должны обладать профессиональными компетенциями, которые можно объединить в следующие группы (название каждой группы может быть рассмотрено как укрупненная задача ИБ, которую может решать профессионал, обладающий компетенциями, входящими в эту группу):

1) «Стратегическое управление ИБ»;
2) «Обеспечение непрерывности бизнеса (НБ)»;
3) «Управление рисками ИБ»;
4) «Управление инцидентами ИБ»;
5) «Защита активов»;
6) «Разработка защищенных ИТ-систем и приложений»;
7) «Функционирование и эксплуатация ИТ-систем»;
8) «Безопасность сетей и телекоммуникаций (ИТТ)»;
9) «Физическая защита и защита от воздействия окружающей среды»;
10) «Безопасность персонала»;
11) «Обучение и осведомленность в области ИБ»;
12) «Компьютерная форензика (криминалистика)»;
13) «Соответствие нормативным актам и стандартам»;
14) «Снабжение (закупки)».

Взаимосвязь обобщенных должностей, групп компетенций и направлений профессиональной деятельности в области обеспечения ИБ (за исключением научно-исследовательской и педагогической ПД) можно наглядно представить в виде матрицы (таблица 2) [4].

Таблица 2. Взаимосвязь должностей, групп компетенций и видов профессиональной деятельности специалистов в области ИБ

Виды ПД: организационно-управленческая (У); проектная (П); реализация (Р); контрольно-аналитическая (О)		Должности в области обеспечения ИБ																			
		Исполнительные						Функциональные								Дополнительные					
		Главный специалист по ИБ		Специалист по ИБ		Специалист по проверке соответствия обеспечения ИБ		Специалист по компьютерной форензике		Специалист по защищенному функционированию и эксплуатации компьютерных систем		Специалист по защите информации		Инженер по защите информации		Специалист по физической защите		Специалист режимно-секретного отдела		Специалист по снабжению	
Группы компетенций в области обеспечения ИБ	**1. Стратегическое управление ИБ**	**У**	**П**	**У**	**П**																
			О	**Р**	**О**		**О**														
	2. Обеспечение НБ	**У**		**У**							**П**						**П**				
					О		**О**			**Р**			**О**			**Р**					
	3. Управление рисками ИБ	**У**		**У**	**П**								**П**					**У**	**П**		
			О		**О**	**Р**	**О**	**Р**		**Р**		**Р**	**О**	**Р**		**Р**		**Р**	**О**		
	4. Управление инцидентами ИБ	**У**		**У**	**П**						**П**		**П**					**У**	**П**		
					О		**О**	**Р**		**Р**	**О**		**О**			**Р**		**Р**	**О**		
	5. Защита активов	**У**		**У**	**П**									**У**	**П**				**П**		
					О		**О**			**Р**	**О**		**О**		**О**				**О**		
	6. Разработка защищенных ИТ-систем и приложений	**У**		**У**											**П**						
					О		**О**			**Р**				**Р**	**О**						
	7. Функционирование и эксплуатация ИТ-систем								**П**	**У**	**П**				**П**						
							О	**Р**	**О**	**Р**	**О**			**Р**							
	8. Безопасность ИТТ								**П**	**У**	**П**				**П**						
							О	**Р**		**Р**	**О**			**Р**							
	9. ФЗ и защита от воздействия окружающей среды	**У**		**У**									**П**			**У**	**П**				
					О		**О**						**О**			**Р**	**О**				
	10. Безопасность персонала	**У**		**У**											**П**				**П**		
							О								**О**		**О**	**Р**			
	11. Обучение и осведомленность в области ОИБ	**У**		**У**									**П**						**П**		
					О		**О**					**Р**	**О**						**О**		
	12. Компьютерная форензика (криминалистика)			**У**	**П**			**У**	**П**												
							О	**Р**	**О**	**Р**											
	13. Соответствие нормативным актам и стандартам	**У**		**У**	**П**		**П**											**У**	**П**		
			О		**О**	**Р**	**О**					**Р**						**Р**	**О**		
	14. Снабжение (закупки)	**У**	**П**	**У**	**П**															**У**	**П**
					О		**О**		**О**		**О**						**О**			**Р**	**О**

Ее анализ позволяет определить связь между должностью, занимаемой сотрудником организации, видом профессиональной деятельности и группой профессиональных компетенций.

Например, Главный специалист по ИБ в основном связан с организационно-управленческой деятельностью. Причем он должен обладать профессиональными компетенциями, относящимися к одиннадцати группам из четырнадцати (исключением являются группы 7 — «Функционирование и эксплуатация ИТ-систем», 8 — «Безопасность сетей и телекоммуникаций (ИТТ)» и 12 — «Компьютерная форензика (криминалистика)»). Кроме этого, он может проявить себя в контрольно-аналитической деятельности (группы компетенций: 1 — «Стратегическое управление ИБ», 3 — «Управление рисками ИБ» и 13 — «Соответствие нормативным актам и стандартам») и проектной деятельности (1 — «Стратегическое управление ИБ» и 14 — «Снабжение (закупки)»).

Организационно-управленческая деятельность также характерна для других должностей:
- для Специалиста по ИБ (должен обладать профессиональными компетенциями из 12 групп (кроме седьмой и восьмой));
- для Специалиста по защищенному функционированию и эксплуатации компьютерных систем (профессиональные компетенции из групп 7 — «Функционирование и эксплуатация ИТ-систем» и 8 — «Безопасность сетей и телекоммуникаций (ИТТ)»);
- для Специалиста по форензике (профессиональные компетенции из группы 12 — «Компьютерная форензика (криминалистика)»);
- для Инженера по защите информации (профессиональные компетенции из группы 5 — «Защита активов»);
- для Специалиста по физической защите (профессиональные компетенции из группы 9 — «Физическая защита и защита от воздействия окружающей среды»);
- для Специалиста режимно-секретного отдела (профессиональные компетенции из групп 3 — «Управление рисками ИБ», 4 — «Управление инцидентами ИБ» и 13 — «Соответствие нормативным актам и стандартам»);
- для Специалиста по снабжению (профессиональные компетенции из группы 14 — «Снабжение (закупки)»).

Из таблицы 2 следует, что одному виду профессиональной деятельности могут быть сопоставлены профессиональные компетенции из различных групп или к одной группе могут относиться профессиональные компетенции, определяющие различные виды профессиональной деятельности.

Профессиональные компетенции в виде подробного перечня функциональных обязанностей, который должен выполнять сотрудник при определенном виде профессиональной деятельности, можно найти в работе [4].

При этом для каждой группы профессиональных компетенций определены требования к уровню знаний, умений и требования к навыкам, которыми должен обладать профессионал для реализации профессиональных компетенций, включенных в данную группу, и которые могут быть рассмотрены в качестве квалификационных требований.

Приведенная выше информация может быть полезна при разработке разделов Политики, связанных с определением требований к номенклатуре должностей и к должностным обязанностям сотрудников подразделений ИБ, а также с порядком подбора кадров.

В дополнение к этому необходимо отметить, что возможны варианты, когда к выполнению определенной задачи ИБ привлекаются несколько сотрудников организации или одному сотруднику поручается решение нескольких задач ИБ. В этом случае рекомендуется организовать деятельность по решению задач ИБ на основе определения и назначения ролей ИБ [5]. Под термином «роль» понимается [5] заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом. К субъектам относятся лица из числа руководителей организации, ее персонала или инициируемые от их имени процессы по выполнению действий над

объектами. Объектами могут быть аппаратное, программное или программно-аппаратное средство, информационный ресурс, услуга, процесс, система, над которыми выполняются действия.

Требования к определению и назначению ролей должны быть отражены в Политике. К ним можно отнести следующие рекомендации (на примере организаций банковской системы РФ [5]):

1. Роли ИБ следует персонифицировать с установлением ответственности за их выполнение. Ответственность должна быть документально зафиксирована в должностных инструкциях.

2. С целью снижения рисков нарушения ИБ не рекомендуется, чтобы в рамках одной роли совмещались следующие функции: разработки и сопровождения системы или программного обеспечения, их разработки и эксплуатации, сопровождения и эксплуатации, администратора системы и администратора ИБ, выполнения операций в системе и контроля их выполнения.

3. В организации должны быть документально определены и выполняться процедуры контроля деятельности работников, обладающих совокупностью полномочий (ролями), позволяющих получить контроль над защищаемым информационным активом организации.

Таким образом, каждому сотруднику организации, занимающему определенную должность, может быть поручено выполнение одной или нескольких ролей, связанных с решением конкретных задач. Успешность выполнения ролей зависит от наличия у исполнителя требуемого квалификационного уровня, что необходимо учитывать при подборе кадров.

При определении в Политике порядка подбора кадров необходимо учитывать (рис. 2) состояние рынка труда, возможности образовательных учреждений (ОУ) среднего и высшего профессионального образования по подготовке необходимых кадров. При взаимодействии с такими ОУ возможны два варианта: пассивный (прием на работу выпускников исходя из квалификационных характеристик, указанных в соответствующем ФГОСе) и активный (формирование для ОУ целевого заказа на подготовку кадров определенного профессионального уровня с обеспечением контроля на выходе обучения). Первому варианту присущи риски несоответствия у выпускника ОУ реального уровня квалификационных характеристик уровню, заявленному во ФГОСе, что в итоге отразится на качестве выполнения им своих должностных обязанностей.

В любом случае целесообразно выполнение следующие требований [5]:

1. В организации должны быть документально определены процедуры приема на работу, влияющую на обеспечение ИБ, включающие проверку подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических фактов, проверку в части профессиональных навыков и оценку профессиональной пригодности. Указанные процедуры должны предусматривать документальную фиксацию результатов проводимых проверок.

2. Все работники организации при приеме на работу должны давать письменное обязательство о соблюдении конфиденциальности.

3. Обязанности персонала по выполнению требований по обеспечению ИБ должны включаться в трудовые контракты (соглашения, договоры) и (или) должностные инструкции. Невыполнение работниками организации требований по обеспечению ИБ должно приравниваться к невыполнению должностных обязанностей и приводить как минимум к дисциплинарной ответственности.

Деятельность любой современной организации, как правило, связана с изменениями ее основных бизнес-процессов, с совершенствованием систем обработки информации, с появлением новых уязвимостей, с необходимостью периодически пересматривать перечень актуальных угроз в информационной сфере. Все это приводит к изменению задач обеспечения ИБ по содержанию и по номенклатуре и, как следствие, к необходимости совершенствования квалификационного уровня сотрудников, решающих эти задачи. Поэтому в Политике должен быть определен порядок поддержки квалификации кадров, который должен учитывать возможности осуществления их повышения квалификации или переподготовки (периодичность обучения, учебные программы,

наличие корпоративного обучения, взаимодействие с внешними образовательными учреждениями дополнительного профессионального образования).

Это направление кадрового обеспечения решения задач ИБ непосредственно связано с контролем профессионального уровня сотрудников организации. Признано целесообразным [5] иметь и периодически осуществлять процедуры регулярной проверки (с документальной фиксацией результатов) в части профессиональных навыков и оценки профессиональной пригодности работников. Эти проверки могут быть оформлены в виде аттестации сотрудников организации. Политика должна сформулировать требования к проведению аттестации (периодичность, программы аттестации, связь аттестации с карьерным ростом и т. д.).

При проектировании Политики обязательно должны быть сформулированы требования к ее реализации. Кадровое обеспечение, как реализация Политики, является процессом, которым необходимо управлять. Поэтому в Политике должны быть сформулированы требования, выполнение которых обеспечит требуемый уровень кадрового обеспечения. В данном случае можно воспользоваться положениями национального стандарта [6], в котором содержится ряд требований к реализации процессного подхода, основными из которых являются следующие:

- осуществление планирования самого процесса;
- планирование и обеспечение ресурсами и информацией, необходимыми для осуществления процесса и управления им;
- определение необходимой степени документированности и документирование процессов;
- наличие критериев и методов оценки осуществления процесса и управления им;
- осуществление мониторинга, оценки и анализа процесса;
- проведение корректирующих и предупреждающих (превентивных) действий по результатам анализа процесса, включая совершенствование процесса, осуществляемого в организации;
- определение методов и осуществление управления процессом, результаты которых нельзя проверить посредством последовательного мониторинга и измерения.

При этом процесс кадрового обеспечения должен быть циклическим, многократно проходя этапы проектирование — реализация — проверка — совершенствование (разновидность цикла Деминга [7]).

Политика кадрового обеспечения решения задач ИБ, как внутренний нормативный документ организации, должна пройти в организации определенные процедуры согласования и утверждения. Точное исполнение требований этого документа непосредственно влияет на эффективность решения задач обеспечения ИБ в организации.

СПИСОК ЛИТЕРАТУРЫ:

1. Управление персоналом: Учебник для вузов / Под ред. Т. Ю. Базарова, Б. Л. Еремина. 2-е изд., перераб. и доп. М.: ЮНИТИ, 2002. — 560 с.
2. Приказ Министерства здравоохранения и социального развития РФ от 22 апреля 2009 г. № 205 «Об утверждении Единого квалификационного справочник должностей руководителей, специалистов и служащих», раздел «Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации».
3. *Толстой А. И.* Основы формирования профессиональных компетенций выпускников учебных заведений по направлениям и специальностям подготовки, входящим в укрупненное направление 090000 — Информационная безопасность // Безопасность информационных технологий. 2008. № 4. С. 46—55.
4. Information Technology (IT) Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development (National Cyber Security Division, United States Department of Homeland Security, October 2008).
5. Стандарт Банка России СТО БР ИББС-1.0-2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
6. ГОСТ Р ИСО 9000-2001 «Системы менеджмента качества. Основные положения и словарь».
7. *Нив Г.* Пространство доктора Деминга. М.: Альпина Бизнес Букс, 2007. — 370 с.