2. СТАНДАРТИЗАЦИЯ СИСТЕМ И ПРОЦЕССОВ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Международная Организация по Стандартизации ISO (ИСО) и Международная Электротехническая Комиссия IEC (МЭК) формируют специализированную систему всемирной стандартизации.

На текущий момент можно с уверенностью сказать, что мировое сообщество проделало существенную работу в направлении стандартизации СУИБ и отдельных процессов управления ИБ, и по-прежнему весьма активно продолжает эту работу. В соответствие с этими стандартами ОИБ в любой организации заключается в выполнении следующих действий:

- определение целей ОИБ;
- создание эффективной СУИБ;
- расчет совокупности детализированных не только качественных, но и количественных показателей для оценки соответствия уровня ИБ заявленным целям;
- применение инструментария ОИБ и оценки ее текущего состояния;
- использование методик (с понятной системой критериев и защитных мер, или мер ОИБ) в процессе анализа и управления рисками, позволяющих объективно оценить текущее состояние дел в организации.

Основоположником подобной стандартизации стала серия стандартов ISO 9000, предъявляющих требования к системам менеджмента качества, соблюдение которых позволяет контролировать качество выпускаемой продукции или предоставляемых услуг. При разработке стандартов на СУИБ многое было взято за основу именно из стандартов серии ISO 9000, например, основной подход – процессный подход и использование циклической модели PDCA для непрерывного совершенствования как самой системы, так и отдельных ее процессов. Помимо этого отличительной особенностью стандартов ISO 9000, которая была перенята при стандартизации СУИБ, является то, что они устанавливают степень ответственности руководства компании за качество. Причем руководство предприятия отвечает как за разработку политики в области качества, так и за внедрение и поддержание в рабочем состоянии системы менеджмента качества. Очень большое количество процессов управления из систем менеджмента качества с некоторыми изменениями присутствует и в СУИБ, например, внутренние аудиты ИБ, корректирующие и предупреждающие действия и т. д.

В данной главе рассматриваются существующие международные стандарты (серии стандартов) и национальные стандарты (российские ГОСТы), относящиеся как к СУИБ в целом, так и к отдельным процессам управления ИБ в организации.

2.1. Серия стандартов ISO/IEC 27000 «Информационные технологии. Методы обеспечения безопасности»

История развития серии стандартов 27000 началась в 1999 г., когда обновленная первая часть британского стандарта BS 7799:1995 (BS 7799–1:1999) была передана в ИСО и в 2000 г. впервые утверждена в качестве международного стандарта как ISO/IEC 17799:2000. Следующей его версией стал стандарт ISO/IEC 17799:2005.

В том же 1999 г. вышла в свет вторая часть стандарта BS 7799 – BS 7799–2:1999 «Information Security Management. Specification for ISMS» для СУИБ (Information Security Management System). В 2002 г. стандарт был усовершенствован и выпущена его новая редакция – BS 7799–2:2002. На ее основе в 2005 г. был разработан и принят стандарт ISO/IEC 27001:2005.

Дальнейшее развитие стандартов серии 27000 включает в себя появление стандартов, более подробно раскрывающих требования к отдельным процессам управления ИБ. Базируясь на единой структуре и методологии, заложенной в ISO/IEC 27001:2005, они предоставляют руководства по управлению ИБ для различных сфер деятельности, включая финансовый и страховой сектор, здравоохранение, телекоммуникации и т. д.

На начало 2012 г. существуют и планируются к ближайшему принятию международные стандарты серии 27000, перечень которых приведен в табл. 2.1.

Таблица 2.1. Перечень международных стандартов серии 27000

Номер и год принятия	*Название*
27000:2009	СУИБ. Определения и основные принципы
27001:2005	СУИБ. Требования (на основе BS 7799–2:2005)
27002:2005	Практические правила управления ИБ (ранее ISO/IEC 17799:2005)
27003:2010	Руководство по внедрению СУИБ
27004:2009	Управление ИБ. Оценка СУИБ
27005:2011	Управление рисками ИБ (на основе BS 7799–3:2006)
27006:2007	Требования к органам, обеспечивающим аудит и сертификацию СУИБ
27007:2011	Руководство по аудиту СУИБ
27008:2011	Руководство по аудиту средств управления ИБ, реализованных в СУИБ
27010	Управление ИБ при коммуникации между секторами (в нескольких частях, предоставляющих руководство по совместному использованию информации о рисках ИБ, средствах управления, проблемах и/или инцидентах ИБ, выходящих за границы отдельных секторов экономики и государств, особенно в части, касающейся критичных инфраструктур)

Номер и год принятия	*Название*
27011:2008	Руководство по управлению ИБ для телекоммуникационных компаний на основе ISO/IEC 27002
27013	Руководство по интегрированному внедрению ISO 20000 и ISO 27001. Выпуск планируется в 2012 г.
27014	Базовая структура управления ИБ
27015	Руководство по внедрению СУИБ для финансовых сервисов (банков, страховых компаний, кредитных организаций и т. д.)
27031:2011	Руководство по готовности информационных и телекоммуникационных технологий для обеспечения непрерывности бизнеса (на основе BS 25699:2006/2007)
27032	Руководство по обеспечению кибербезопасности
27033	27033–1:2009 Безопасность сетей. Часть 1. Общие положения и концепции. 27033–2 Руководство по проектированию и внедрению системы обеспечения безопасности сетей. Выпуск планируется в 2012 г. 27033–3:2010 Базовые сетевые сценарии – угрозы, методы проектирования и средства управления. 27033–4 Обеспечение безопасности межсетевых взаимодействий при помощи шлюзов безопасности – угрозы, методы проектирования и средства управления. 27033-5 Обеспечение безопасности виртуальных частных сетей – угрозы, методы проектирования и средства управления. 27033–6 Конвергенция в IP-сетях (Определение угроз, методов проектирования и средств управления в IP-сетях с конвергенцией данных, голоса и видео). 27033–7 Руководство по обеспечению безопасности беспроводных сетей – риски, методы проектирования и средства управления
27034	27034–1:2011 Безопасность приложений. Часть 1. Обзор и основные концепции в области обеспечения безопасности приложений. 27034–2 Нормативная база организации. 27034–3 Процесс управления безопасностью приложений. 27034-4 Оценка безопасности приложений. 27034–5 Протоколы и структура управляющей информации для обеспечения безопасности приложений (XML-схема). 27034–6 Руководство по обеспечению безопасности конкретных приложений
27035:2011	Управление инцидентами безопасности (заменит ISO/IEC TR 18044)
27036	Руководство по аутсорсингу безопасности. Выпуск планируется в 2012 г.
27037	Руководство по идентификации, сбору и/или получению и обеспечению сохранности свидетельств, представленных в электронной форме (на основе BS 10008:2008)
27799:2008	Управление ИБ в сфере здравоохранения

Что касается собственно российских стандартов по управлению ИБ, то сначала были приняты стандарт ГОСТ Р ИСО/МЭК 17799–2005, идентичный ISO/IEC 17799:2000 и актуализированный 01.01.2008, и стандарт ГОСТ Р ИСО/МЭК 27001–2006, идентичный ISO/IEC 27001:2005. В настоящее время российская стандартизация в области

управления ИБ проходит некоторую промежуточную стадию своего формирования и является еще недостаточно зрелой, однако, уже сейчас намечаются положительные тенденции в развитии данной области. После некоторого перерыва были приняты национальные стандарты, идентичные 27006, 27005, 27004 и 27033–1.

Взаимосвязь российских, международных и британских стандартов, посвященных СУИБ, отражена в табл. 2.2.

Таблица 2.2. Взаимосвязь стандартов, посвященных СУИБ

Российский стандарт	*Международный стандарт*	*Британский стандарт*
ГОСТ Р ИСО/МЭК 17799–2005	ISO/IEC 27002:2005	BS 7799–1:2005
-	ISO/IEC 17799:2005	
ГОСТ Р ИСО/МЭК 27001–2006	ISO/IEC 27001:2005	BS 7799–2:2005
ГОСТ Р ИСО/МЭК 27006–2008	BS ISO/IEC 27006:2007	
ГОСТ Р ИСО/МЭК 27005–2010	ISO/IEC 27005:2011	BS 7799–3:2005
ГОСТ Р ИСО/МЭК 27004–2011	BS ISO/IEC 27004:2009	
ГОСТ Р ИСО/МЭК 27033–1–2011	BS ISO/IEC 27033–1:2009	

Также проблематикой СУИБ занимается и Федеральное агентство по ИБ немецкого правительства BSI (Bundesamt fur Sicherheit in der Informationstechnik), которое является одним из признанных разработчиков решений в области ИБ, предоставляющим бесплатный доступ к своим документам через сайт BSI [www.bsi.bund.de]. Методика IT-Grundschutz позволяет создать СУИБ, соответствующую требованиям ISO/IEC 27001, поскольку эта методика полностью совместима с подходами, использованными в стандарте 27001, и рекомендациями стандарта ISO/IEC 27002. Но методика IT-Grundschutz описывает некоторые вопросы, затронутые в стандарте, более детально и поэтому предоставляет более дидактический подход для организаций, внедряющих у себя СУИБ.

Агентство разработало и регулярно обновляет четыре стандарта в области ОИБ (рис. 2.1) [16–19]:

1. BSI-Standard 100-1 «Information Security Management Systems» содержит общие требования к СУИБ.

2. BSI-Standard 100-2 «IT-Grundschutz Methodology» освещает вопросы поэтапного построения СУИБ и ее дальнейшего использования на практике и содержит подробные руководства по ОИБ применительно к различным аспектам функционирования ИС и различным областям ИТ. В стандарте выделяются функции СУИБ и организационная структура ОИБ, даются подробные практические рекомендации по разработке по-

литики ИБ и выбору защитных мер, а также рассматриваются сопровождение и усовершенствование деятельности по ОИБ в повседневной практике организации.

3. BSI-Standard 100-3 «Risk Analysis based on IT-Grundschutz» посвящен анализу рисков ИБ на основе методики IT-Grundschutz.

4. BSI-Standard 100-4 «Business Continuity Management» рассматривает вопросы управления непрерывностью бизнеса (УНБ).

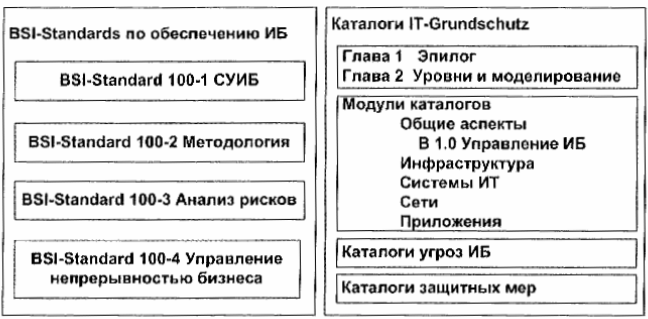

Рис. 2.1. Серия стандартов BSI

Кроме того, BSI составило сборник IT-Grundschutz Catalogues (Каталоги по безопасности ИТ), являющийся самым объемным (более 4 тыс. страниц) и детальным из существующих. Каталоги типовых информационных активов, связанных с ними угроз ИБ и защитных мер, содержат конкретные практические рекомендации для оценки рисков ИБ, выбора и применения защитных мер, включая технические аспекты их использования.

2.1.1. ISO/IEC 27000:2009 – СУИБ: ОПРЕДЕЛЕНИЯ И ОСНОВНЫЕ ПРИНЦИПЫ

Международный стандарт ISO/IEC 27000:2009 «Information technology. Security techniques. Information security management systems. Overview and vocabulary» (Информационная технология. Методы и средства обеспечения безопасности. Обзор и определения) содержит термины и определения, которые используются во всех стандартах серии 27000 [20]. Основная цель ISO/IEC 27000:2009 – подробное описание основных принципов, концепций и определений для серии документов ISO/IEC 27000, регламентирующих все то, что связано с СУИБ.

В стандарте приведен обзор серии 27000 (рис. 2.2); представлено введение в СУИБ, являющееся предметом рассмотрения данной серии стандартов, определены требования к СУИБ и к их оценке соответствия, в том числе для тех, кто сертифицирует эти системы; описан цикл

PDCA со всеми процессами и требованиями к ним, а также введены термины и определения, использующиеся в стандартах серии 27000.

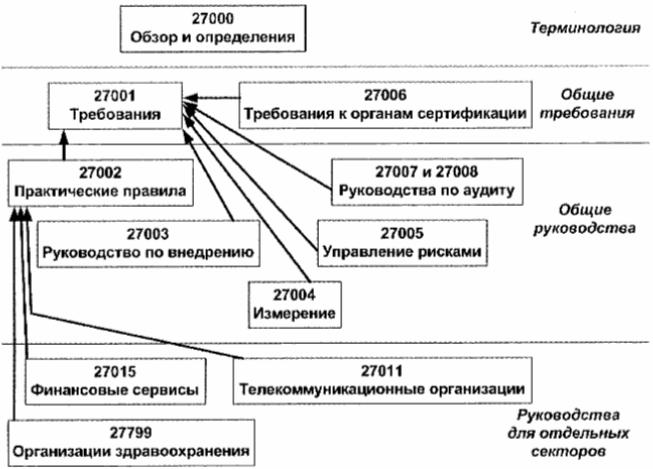

Рис. 2.2. Логическая взаимосвязь стандартов серии 27000

В ISO/IEC 27000:2009 ***СУИБ определяется как часть общей системы управления, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, сопровождения (поддержания) и совершенствования (улучшения) ИБ.*** Далее уточняется, что СУИБ определяет модель защиты информационных активов организации для достижения ее бизнес-целей на основе оценки рисков и установления уровня приемлемых для организации рисков, отражающих эффективное устранение и управление рисками. При этом под ИБ понимается сохранение конфиденциальности, целостности и доступности информации, а под системой управления – совокупность политик, процедур, руководящих принципов и ресурсов, необходимых для достижения бизнес-целей организации. Эта система включает в себя организационную структуру, политики, деятельность по планированию, распределение ответственности, практическую деятельность, процедуры, процессы и ресурсы.

При разработке стандарта ISO/IEC 27000:2009 были учтены основные положения следующих документов: ISO/IEC Guide 2:1996 «Стандартизация и смежная деятельность. Основные определения» и ISO/IEC Guide 73:2002 «Управление рисками. Определения. Рекомендации по использованию в стандартах», а также проведена унификация со стандартами COBIT и ITIL.

В России Ассоциацией ЕВРААС и ООО «НИИ СОКБ» осенью 2011 г. была подготовлена первая редакция проекта национального стандарта ГОСТ Р ИСО/МЭК 27000–201x.

2.1.2. ISO/IEC 27001:2005 и ГОСТ Р ИСО/МЭК 27001–2006 – ТРЕБОВАНИЯ К СУИБ

Международный стандарт ISO/IEC 27001:2005 «Information technology. Security techniques. Information security management systems. Requirements» (Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента ИБ. Требования) содержит модель создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования СУИБ [21].

В России принят ГОСТ Р ИСО/МЭК 27001–2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», идентичный 27001:2005 [14]. Основной объект рассмотрения стандарта в этом документе переведен как «система менеджмента ИБ» (СМИБ). Целью построения такой системы является выбор соответствующих мер управления ИБ, предназначенных для защиты информационных активов и гарантирующих доверие заинтересованных сторон.

ГОСТ Р ИСО/МЭК 27001–2006 определяет общую организацию СУИБ, требования к ней, разработку и управление СУИБ, требования к документации СУИБ, ответственность руководства в контексте управления ИБ (его обязанности и управление ресурсами), внутренний аудит СУИБ, анализ СУИБ и направления усовершенствования СУИБ и т. д. Применение этого стандарта позволит на основе процессного подхода управлять конфиденциальностью, целостностью и доступностью важного актива компании – информации, и может с одинаковым успехом применяться в компаниях разного размера – от индивидуальных предпринимателей до предприятий с численностью сотрудников в десятки тысяч человек, типа (коммерческих компаний, государственных и некоммерческих структур) и сферы деятельности.

ГОСТ Р ИСО/МЭК 27001–2006 может использоваться для защиты любых видов информации, включая финансовую, персональные данные, информацию по поставщикам и клиентам, другие данные компании и, что немаловажно, информацию, принадлежащую ее партнёрам/клиентам, – всё, что является значимым информационным активом, и всё, что подвержено угрозам ИБ. Требования стандарта не накладывают каких-либо технических требований на ИТ-средства или СЗИ – стандарт не устанавливает ограничения на выбор программно-аппаратных средств и оставляет организации полную свободу выбора технических решений по защите информации. Таким образом, основную цель ГОСТ Р ИСО/МЭК 27001–2006 можно сформулировать как создание общей методологии разработки, внедрения и оценки эффективности СУИБ.

Решение о создании СУИБ является стратегическим решением организации. На проектирование и внедрение СУИБ оказывают влияние потребности и бизнес-цели компании, используемые бизнес-процессы, а также ее структура и размер, что, в свою очередь, ведет к выработке конкретных требований по обеспечению безопасности бизнеса в широком смысле его понимания. СУИБ объединяет воедино людей, процессы и ИТ-системы, а также обеспечивает согласованную работу службы безопасности, ИТ-отдела и руководства компании.

При использовании СУИБ реализуется системный подход к управлению «чувствительной» (англ. *sensitive*) для компании информацией с целью обеспечения ее конфиденциальности, целостности и доступности. В связи с этим особую значимость приобретают следующие факторы:

1) понимание требований по ОИБ организации и необходимости установления политики и целей ИБ;

2) внедрение и использования мер для управления рискам ИБ наряду с общими бизнес-рисками организации;

3) мониторинг и проверка производительности и эффективности СУИБ;

4) непрерывное улучшение СУИБ, основанное на результатах объективных измерений.

Начиная с 2005 г. к августу 2011 г. более 7300 организаций во всем мире успешно прошли официальные процедуры сертификации СУИБ по требованиям ISO/IEC 27001:2005 и еще сотни тысяч организаций активно внедряют международные стандарты серии 27000 без прохождения официальных процедур сертификации [www.iso27001security.com]. Сертифицируя СУИБ на соответствие стандарту ISO/IEC 27001:2005, организация демонстрирует своим партнерам применение проверенного международными компаниями методологического подхода к ОИБ, показывает прочность и стабильность своего положения, повышает степень доверия инвестиционных и страховых компаний. Следование требованиям стандарта позволяет существенно повысить прозрачность и защищенность внутренних процессов. Несмотря на рекомендательный статус стандарта ISO/IEC 27001, правительства ряда стран поддерживают его на государственном уровне.

2.1.3. ISO/IEC 27002:2005 и ГОСТ Р ИСО/МЭК 17799–2005 – ПРАКТИЧЕСКИЕ ПРАВИЛА УПРАВЛЕНИЯ ИБ

Стандарт ISO/IEC 17799:2005 «Информационные технологии. Управление ИБ. Практические правила» включен в серию стандартов 27000, не претерпев существенных изменений и получив номер ISO/IEC 27002:2005. Международный стандарт менеджмента ИБ 27002:2005 «Information technology. Security techniques. Code of practice for information security management» (Информационная технология. Методы и средства обеспечения безопасности. Практические правила управле-

ния ИБ) [22] разработан на базе первой части британского стандарта BS 7799, который предназначен для управления ИБ организации вне зависимости от сферы ее деятельности.

В России стандарт ISO/IEC 17799 начал активно применяться на практике экспертами в области управления ИБ начиная с 2001–2002 гг. и в 2005 г. был принят ГОСТ Р ИСО/МЭК 17799–2005, идентичный 17799:2000, содержащий 10 основных разделов: ПолИБ; организационные вопросы безопасности; классификация и управление активами; вопросы безопасности, связанные с персоналом; физическая защита и защита от воздействий окружающей среды; управление передачей данных и операционной деятельностью; контроль доступа; разработка и обслуживание систем; управление непрерывностью бизнеса; соответствие требованиям. После введения в действие этот ГОСТ был актуализирован и переиздан в январе 2008 г. с учетом изменений, появившихся в редакции ISO/IEC 17799:2005.

ГОСТ Р ИСО/МЭК 17799–2005 является совокупностью практических правил по управлению ИБ и может быть использован в качестве критериев для оценки механизмов безопасности. В соответствии со стандартом при создании эффективной системы безопасности особое внимание следует уделить комплексному подходу к управлению ИБ. По этим причинам в качестве элементов управления рассматриваются не только технические, но и организационно-административные меры, направленные на обеспечение следующих требований к информации: конфиденциальность, целостность, доступность, аутентичность.

В последней редакции стандарта 17799 определяются и рассматриваются 139 средств управления ИБ (англ. *controls*), включающих меры по собственно управлению ИБ и контролю за этим управлением, по следующим направлениям управления ИБ:

1) управление рисками ИБ (включая оценку, анализ и снижение рисков ИБ);

2) ПолИБ (определяются требования к поддержке заданного уровня ИБ; вводятся принципы и аксиомы, описываются некоторые политики, стандарты, руководящие принципы и процедуры в области ОИБ);

3) организация защиты (управление ИБ при взаимодействии с внешними объектами, включая структуру, анализ и взаимосвязи);

4) управление активами (обеспечение защиты активов организации, включая их инвентаризацию, классификацию и владельцев);

5) безопасность персонала (снижение риска «человеческих ошибок» и преднамеренных нарушений, а также средства управления выполнением правил ПолИБ со стороны пользователей, их обучения и повышения осведомленности в вопросах ИБ);

6) физическая защита и защита от воздействия окружающей среды (предотвращение несанкционированного доступа (НСД), изменений, кражи и повреждения средств защиты и информации при физическом

доступе; также рассматриваются системы вентиляции, пожаротушения, водоснабжения и электропитания);

7) администрирование систем и коммуникаций (снижение риска возникновения системных сбоев, предотвращение повреждения сетевого оборудования, а также средства управления сохранением конфиденциальности, целостности, доступности и аутентичности при передаче информации; включая архивирование, резервное копирование, журналирование и оповещение, установку обновлений, мониторинг и конфигурирование);

8) управление доступом (контроль доступа к информационным ресурсам и предоставляемым услугам, а также противодействие несанкционированной активности в части физического доступа, сетевого доступа, доступа к системам, приложениям, функциям и данным);

9) приобретение, развитие и сопровождение ИС (обеспечение выполнения функций защиты информации в операционных системах (ОС) и приложениях на всех стадиях их жизненного цикла, начиная с требований, проектирования, развития, приобретения, тестирования, внедрения, и заканчивая сопровождением и поддержкой);

10) управление инцидентами ИБ (включая планирование, идентификацию, собственно реагирование, управление и сохранение собранной информации, устранение последствий и извлечение уроков на будущее);

11) управление непрерывностью бизнеса организации (обеспечение защиты критически важных бизнес-процессов от сбоев и нарушений на основе повышения его устойчивости и восстановления после сбоев и аварий);

12) соответствие систем ИБ требованиям нормативных и руководящих документов (обеспечение соблюдения общепринятых и внутренних правил, норм, национальных и международных стандартов, законов, требований третьих лиц, аудиторов и т. д.).

ГОСТ Р ИСО/МЭК 17799–2005 не является техническим стандартом и не зависит от конкретных средств защиты или технологий. Он описывает концептуальные основы управления ИБ и является признанным набором «лучших практик» по ОИБ.

2.1.4. ISO/IEC 27003:2010 – РУКОВОДСТВО ПО ВНЕДРЕНИЮ СУИБ

Стандарт ISO/IEC 27003:2010 «Information Technology. Security Techniques. Information Security Management Systems Implementation Guidance» (Информационная технология. Методы и средства обеспечения безопасности. Руководство по внедрению систем менеджмента ИБ) [23] является общим руководством по практическому применению стандартов серии 27000 и базируется на ISO/IEC 27000 и 27001, которые полезны для всех организаций, независимо от их размера, типа, сферы деятельности, сложности и имеющихся рисков ИБ. Основная цель стандарта – обеспечение руководства по проектированию такой

СУИБ, на основе которой риски ИБ для информационных активов поддерживаются в пределах приемлемых границ, с учетом реализации требований, предъявляемых к СУИБ в ISO/IEC 27001.

В России Ассоциацией ЕВРААС и ООО «НИИ СОКБ» осенью 2011 г. подготовлена первая редакция проекта национального стандарта ГОСТ Р ИСО/МЭК 27003–201x.

ISO/IEC 27003:2010 не рассматривает функционирование СУИБ, а описывает только стадии проектирования деятельности, которая начнет осуществляться после создания СУИБ. Основным результатом применения стандарта является разработанный окончательный план внедрения проекта СУИБ в организации.

Данный стандарт описывает процесс разработки спецификации и проектирования СУИБ с самого начала, включая:

1) поддержку со стороны руководства организации;

2) установление целей и приоритетов внедрения СУИБ, границ ее действия и политики использования;

3) анализ требований по ОИБ и требований к процессам, поддерживаемым СУИБ, с идентификацией защищаемых активов и критериев оценки ИБ;

4) оценку рисков ИБ и их снижение с определением требований к средствам управления и до момента внедрения плана проектирования СУИБ с учетом подготовки и планирования деятельности по ее фактической реализации и внедрению, включая:

- стадии проектирования СУИБ;
- проектирование организации ОИБ;
- проектирование обеспечения защиты ИТ и физической безопасности;
- учет некоторых других аспектов использования СУИБ;
- разработку окончательного плана проектирования СУИБ.

В приложениях к стандарту представлены роли и обязанности сотрудников организации по ОИБ, информация по внутреннему аудиту ИБ, структура ПолИБ и процессы мониторинга и измерения успешности функционирования СУИБ.

2.1.5. ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004–2011 – ОЦЕНКА ФУНКЦИОНИРОВАНИЯ СУИБ

Стандарт ISO/IEC 27004:2009 «Information technology. Security techniques. Information security management. Measurement» (Информационная технология. Методы и средства обеспечения безопасности. Менеджмент ИБ. Измерение) [24] предназначен для помощи организациям в оценке результативности деятельности по управлению ИБ в рамках имеющихся у них СУИБ за счет предоставления единого руководства по применению механизмов получения оценки в результате измерений и введения показателей. На основе полученных показателей, их анализа

и принятия соответствующих решений по устранению выявленных проблем организациям удастся повысить результативность функционирования их СУИБ. Эта информация крайне важна для обоснования всех решений, связанных с СУИБ, при внедрении СУИБ и необходимости внесения изменений в существующую СУИБ для ее дальнейшего совершенствования (улучшения).

С января 2012 г. в России введен в действие ГОСТ Р ИСО/МЭК 27004–2011 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения» [25], идентичный ISO/IEC 27004:2009. В стандарте содержатся общее руководство и рекомендации по разработке и использованию измерений и мер измерений и их сбору для оценки эффективности и результативности внедренной в организации СУИБ, а также мерам и средствам управления ИБ (и их группам), определенным в ISO/IEC 27001, включая политику, управление рисками ИБ, задачи средств управления, сами средства управления, процессы и процедуры, поддержку процесса их пересмотра, помощи в определении необходимости изменения или усовершенствования процессов или средств управления СУИБ.

ГОСТ Р ИСО/МЭК 27004–2011 содержит следующие основные разделы:

1) обзор измерений, связанных с ИБ (цели, программа, факторы успеха, модель измерений);

2) обязанности руководства;

3) разработка измерений и мер измерений (процессов их сбора и показателей);

4) процесс измерений;

5) анализ данных и отчетность по результатам измерений;

6) оценивание и совершенствования программы измерений в организации.

В приложениях к стандарту предложен шаблон (типовая форма) описания измерений и приведены некоторые рабочие примеры.

ГОСТ Р ИСО/МЭК 27004–2011 подразумевает, что начальной точкой для разработки измерений и мер измерений является правильное понимание организацией рисков ИБ, с которыми она сталкивается, и того, что деятельность в данном направлении осуществляется корректно (например, на основе ISO/IEC 27005), как того требуется ISO/IEC 27001. Для проведения данных мероприятий требуется разработка программы измерений, связанных с ИБ. Полученные во время измерений результаты позволят выявить прогресс (или отсутствие такового) в достижении целей ОИБ за некоторый период времени как одного из элементов процесса непрерывного совершенствования СУИБ организации.

Стандарт содержит достаточно детальное описание процессов измерения, использование операции агрегирования полученных мер измерений, математического вычисления производных (от двух и более

основных) мер и последующего применения аналитических методов и методов принятия решений для выявления «индикаторов» совершенствования СУИБ. Но, к сожалению, не указывается, какие именно основные и производные меры измерений и индикаторы могут на практике наилучшим образом повлиять на это совершенствование.

Само измерение определяется как процесс получения информации об эффективности СУИБ и элементах управления ИБ с использованием метода измерения, функций измерения, аналитической модели и критериев принятия решений.

Механизмы, описанные в стандарте, применимы к различным организациям с различными СУИБ. Подход организации для выполнения требований к измерениям, определенных в ISO/IEC 27001, зависит от ряда существенных факторов, включая риски ИБ, величину организации, имеющиеся ресурсы и применимые правовые, нормативные и договорные требования, и важен для обеспечения того, чтобы для этой деятельности СУИБ не выделялись чрезмерные ресурсы в ущерб другой необходимой деятельности. В идеальном случае текущая деятельность, связанная с постоянными измерениями, должна быть интегрирована в обычную деятельность организации с привлечением минимальных дополнительных ресурсов.

Для организаций небольшого размера число мер измерений может быть невелико и для них необходимо разработать одну программу измерений, в то время как для крупных организаций таких программ может быть создано несколько.

На основе ГОСТ Р ИСО/МЭК 27004–2011 организация сможет разработать для себя документацию, которая будет свидетельствовать, что в ней ведется контроль за ОИБ и производится его всесторонняя оценка.

2.1.6. ISO/IEC 27005:2011 и ГОСТ Р ИСО/МЭК 27005–2010 – УПРАВЛЕНИЕ РИСКАМИ ИБ

Стандарт ISO/IEC 27005:2011 «Information technology. Security techniques. Information security risk management» (Информационная технология. Методы и средства обеспечения безопасности. Управление рисками ИБ) [26] содержит общее руководство по управлению рисками ИБ, которое может быть использовано в различных типах организаций – коммерческих, некоммерческих, государственных. ISO/IEC 27005:2011 предназначен для организации адекватного бизнес-потребностям ОИБ на основе риск-ориентированного подхода. Для правильного применения этого стандарта необходимо знание концепций, моделей, процессов и терминологии, введенных в ISO/IEC 27001 и 27002.

В ISO/IEC 27005:2011 развиты основные идеи, ранее представленные в теперь уже недействующих стандартах ISO/IEC 13335–3:1998 [27] и 13335–4:2000 [28], посвященных управлению безопасностью информационных и телекоммуникационных технологий (ИТТ). Вторая редак-

ция стандарта ISO/IEC 27005 гармонизирована с ISO/IEC 27000:2009 [20]. Также он опирается на следующие стандарты управления рисками, перечисленные в его библиографическом списке: ISO Guide 73:2009 (словарь из более чем 50 терминов в области управления рисками; на основе его более ранней редакции был создан ГОСТ Р 51897–2002 «Менеджмент риска. Термины и определения» [29]), ISO 16085, AS/NZS 4360 и NIST SP 800–30. Кроме этого были предприняты определенные усилия по его адаптации в соответствии с принятыми в 2009 г. стандартами ISO 31000:2009 (Управление рисками. Принципы и руководящие указания) и ISO 31010:2009 (Управление рисками. Методики оценки рисков).

Считается, что ISO/IEC 27005:2011 был разработан на основе британского стандарта BS 7799–3:2006 «Information security management systems. Guidelines for information security risk management» (Системы менеджмента ИБ. Руководство по управлению рисками ИБ) [30], определяющего процессы оценки и управления рисками как составные элементы системы управления организации, при этом используя процессную модель PDCA. BS 7799–3:2006 носит концептуальный характер, что позволяет экспертам по ИБ реализовать любые методы, средства и технологии оценки, обработки и управления рисками ИБ. С другой стороны стандарт не содержат рекомендаций по выбору какого-либо аппарата оценки риска ИБ, а также по разработке мер, средств и сервисов защиты, используемых для минимизации рисков ИБ. BS 7799–3:2006 допускает использование как количественных, так и качественных методов оценки рисков ИБ, но, к сожалению, в документе нет обоснования и рекомендаций по выбору математического и методического аппарата оценки рисков ИБ.

Стандарт BS 7799–3:2006 придерживается самого общего понятия риска ИБ, под которым понимают комбинацию вероятности события и его последствий (стоимости компрометируемого ресурса). Управление риском ИБ сформулировано как скоординированные непрерывные действия по управлению и контролю рисков в организации. Непрерывный процесс управления делится на четыре фазы: оценка рисков ИБ, включающая анализ и вычисление рисков; обработка риска ИБ (выбор и реализация мер и средств защиты); контроль рисков ИБ путем мониторинга, тестирования, анализа механизмов безопасности и аудита ИБ системы; оптимизация рисков ИБ путем модификации и обновления правил, мер и средств защиты.

Помимо определения основных факторов риска и подходов к его оценке и обработке, стандарт также описывает взаимосвязи между рисками ИБ и другими рисками организации, содержит требования и рекомендации по выбору методологии и инструментов для оценки рисков, определяет требования, предъявляемые к экспертам по оценке рисков, менеджерам, отвечающим за процессы управления рисками, владельцам

активов и руководству организации, содержит соображения по выбору законодательных и нормативных требований безопасности, отмечает необходимость использования принципа осведомленности о процессах оценки, отработки, контроля и оптимизации рисков ИБ в организации и многое другое. На каждом этапе управления рисками ИБ предусмотрено информирование всех участников процесса управления ИБ, а также фиксирование событий СУИБ. В приложениях приведены примеры активов, угроз ИБ, уязвимостей, методов оценки рисков ИБ.

К основным документам по управлению рисками ИБ в BS 7799–3:2006 отнесены описание методологии оценки рисков ИБ, отчет об оценке рисков ИБ, план обработки рисков ИБ. Кроме того, в непрерывном цикле управления рисками ИБ задействовано множество рабочей документации: реестры активов, реестры рисков, декларации применимости, списки проверок, протоколы процедур и тестов, журналы безопасности, аудиторские отчеты, планы коммуникаций, инструкции, регламенты и т. п.

С декабря 2011 г. в России введен в действие ГОСТ Р ИСО/МЭК 27005–2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» [31], идентичный ISO/IEC 27005:2008 и заменяющий ГОСТ Р ИСО/МЭК ТО 13335–3–2007 «Методы менеджмента безопасности информационных технологий» и ГОСТ Р ИСО/МЭК ТО 13335–4–2007 «Выбор защитных мер».

В целом ГОСТ Р ИСО/МЭК 27005–2010 носит описательный характер и не содержит какой-либо конкретной методологии и даже не называет конкретные методы управления рисками ИБ, хотя и устанавливает структурированный, систематический и строгий метод анализа рисков ИБ посредством создания плана их обработки. Стандарт позволяет применяющей его организации самостоятельно учесть различные аспекты СУИБ, идентифицировать уровни своих рисков, определить критерии для принятия риска, идентифицировать приемлемые риски и т. д. Организация сама должна выбрать из имеющихся свой подход к управлению рисками ИБ, зависящий, например, от целей использования СУИБ, области ее действия, содержания процесса управления рисками ИБ и сферы своей деятельности.

ГОСТ Р ИСО/МЭК 27005–2010 состоит из следующих основных разделов:

1) обзор процесса управления рисками ИБ как непрерывного процесса;

2) установление контекста управления рисками ИБ;

3) оценка рисков ИБ (общее описание оценки рисков ИБ, анализ рисков ИБ, включая идентификацию, оценивание значительности и вычисление рисков ИБ);

4) обработка рисков ИБ (общее описание обработки рисков, снижение, сохранение, избежание и передача рисков);

5) принятие рисков ИБ;

6) коммуникация рисков ИБ;

7) мониторинг и пересмотр рисков ИБ.

В приложениях к стандарту содержится ряд сведений информативного характера: определение целей и границ процесса управления рисками ИБ, определение и оценка активов и воздействия на них, примеры типичных угроз ИБ, уязвимости и методы их оценки, подходы к оценке рисков ИБ, ограничения для снижения рисков.

В стандарте риск ИБ определяется как потенциальная возможность того, что установленная угроза воспользуется уязвимостью актива или группы активов и тем самым нанесет ущерб организации. Измеряется риск ИБ как сочетание последствий, вытекающих из возникновения нежелательного события, и вероятности возникновения этих событий. Указывается, что процесс анализа рисков ИБ требует выполнения следующих действий: определения информационных активов, которые подвержены рискам, потенциальных угроз ИБ и их источников, потенциальных уязвимостей и потенциальных последствий при реализации рисков ИБ. Упоминаются как качественные, так и количественные методы оценки рисков ИБ, но никакому из них не отдается предпочтение. Но отмечается, что процесс оценки рисков ИБ сильно зависит от исходных данных и поэтому может быть итеративным, если полученные результаты будут признаны неудовлетворительными. Также наглядно представлен весь процесс управления рисками ИБ и более детально рассмотрены оценка рисков ИБ, обработка рисков ИБ и остаточные риски ИБ.

ГОСТ Р ИСО/МЭК 27005–2010 предназначен для руководителей и сотрудников организация, занимающихся управлением рисками ИБ, и на сотрудников внешних организаций, задействованных в данной деятельности.

2.1.7. ISO/IEC 27006:2011 и ГОСТ Р ИСО/МЭК 27006–2008 – ТРЕБОВАНИЯ К ОРГАНАМ, ОСУЩЕСТВЛЯЮЩИМ АУДИТ И СЕРТИФИКАЦИЮ СУИБ

Стандарт ISO/IEC 27006:2011 «Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems» (Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента ИБ) [32] является руководством по формализованному процессу сертификации или регистрации СУИБ организаций для органов, осуществляющих такую сертификацию. Этот стандарт включает и заменяет EA7/03 – руководство по процессам сертификации аккредитованными для этого органами и в первую очередь предназначен для поддержки аккредитации органов сертификации, осуществляющих сертификацию СУИБ. Стандарт ISO 17026, упомянутый как нормативная ссылка в ISO/IEC

27006:2011, был недавно обновлен, поэтому потребуется пересмотр некоторых положений 27006, но такая работа пока не проведена.

ГОСТ Р ИСО/МЭК 27006–2008 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента ИБ», идентичный более ранней редакции международного стандарта ISO/IEC 27006:2007, введен в действие в России с ноября 2009 г. [33].

Цель ГОСТ Р ИСО/МЭК 27006–2008 – установить общие требования к сертификации или регистрации СУИБ организаций, которым должны удовлетворять их СУИБ, чтобы быть признанными достаточными и надежными для выполнения заявленных функций по управлению ИБ, а также способствовать проведению аккредитации органов сертификации. Определяются требования и дается руководство по осуществлению аудита и сертификации СУИБ, дополняющие требования ISO/IEC 27001 и стандарта 17021–1 (Оценка соответствия. Требования к органам, проводящим аудит и сертификацию систем управления), давшего начало стандарту 27006. Вторая редакция ISO/IEC 17021:2011 устанавливает новые требования к аудиту систем управления, направленные на повышение ценности сертификации системы управления для государственных и частных организаций по всему миру, и к квалификации аудиторов, выполняющих сертификацию, а также способов организации их работы.

ГОСТ Р ИСО/МЭК 27006–2008 содержит следующие основные разделы:

1) принципы;

2) общие требования (правовые и договорные вопросы, управление объективностью, обязательства и финансирование);

3) требования к структуре (организационная структура и руководство, комитет по охране объективности);

4) требования к ресурсам (компетентность руководства и персонала, привлекаемый к сертификации персонал, привлечение внешних индивидуальных аудиторов и технических экспертов, учет кадров, аутсорсинг);

5) требования к информации (общедоступная информация, сертификационные документы, каталог сертифицированных клиентов, ссылка на сертификацию и использование знаков, конфиденциальность, обмен информацией между органом сертификации и его клиентами);

6) требования к процессу (общие требования, первоначальный аудит и сертификация, надзорная деятельность, повторная сертификация, специальные аудиты, приостановка, отмена или уменьшение области сертификации, апелляции, совместимость, учет заявителей и клиентов);

7) требования системы управления к органам сертификации.

В приложениях информативного характера приведены анализ сложности сертифицируемых организаций и их областей деятельности, при-

меры компетенций аудиторов, продолжительность аудитов, руководство по анализу реализованных мер управления на основе ISO/IEC 27001:2005.

2.1.8. ISO/IEC 27007:2011 и ISO/IEC 27008:2011 – руководства по аудиту СУИБ и средств управления ИБ, реализованных в СУИБ

Стандарт ISO/IEC 27007:2011 «Information technology. Security techniques. Guidelines for Information Security Management Systems auditing» (Информационная технология. Методы и средства обеспечения безопасности. Руководство по аудиту систем менеджмента ИБ) [34] содержит руководство для аккредитованных органов сертификации, внутренних аудиторов, внешних аудиторов/третьих лиц и других организаций, проводящих аудит СУИБ на соответствие требованиям стандарта ISO/IEC 27001 (например, аудит на совместимость с требованиями данного стандарта) или советы по аудиту или анализу имеющейся в организации СУИБ на ее соответствии стандарту ISO/IEC 27002 (например, проводящим аудит средств управления на их применимость к управлению рисками ИБ).

ISO/IEC 27007:2011 в значительной степени основывается на пересматриваемом в настоящее время стандарте ISO 19011:2002, содержащем руководящие указания по аудиту систем менеджмента качества и систем менеджмента окружающей среды, и стандарте ISO 17021–2 «Оценка соответствия. Требования к сертификационному аудиту систем управления, проводимым третьей стороной». В отличие от ISO 19011, в ISO/IEC 27007:2011 сформулированы специальные рекомендации для аудиторов в следующих областях:

- подтверждение области действия СУИБ;
- проверка того, что был использован соответствующий подход оценки рисков ИБ;
- исследование результатов оценки рисков ИБ;
- проверка того, что был осуществлен выбор таких средств управления, которые соответствуют принятому решению в области обработки рисков ИБ;
- сбор объективных доказательств реализации контрольных мероприятий;
- разработка путей аудита СУИБ;
- сопровождение сертификационного аудита СУИБ согласно ISO/IEC 27006:2011.

В ISO/IEC 27007:2011 рассматриваются такие вопросы, как принципы аудита, управление программой аудита (включая постановку задач, определение ответственности, необходимых ресурсов и процедур, реа-

лизацию, документы, мониторинг и анализ), деятельность в рамках проводимого аудита (начиная с инициализации процесса, проведения анализа предоставленных документов, подготовки к аудиту на месте, и заканчивая подготовкой отчета по результатам аудита, завершению аудита и последующих действий), компетентность и оценка аудиторов.

Стандарт ISO/IEC 27008:2011 «Information technology. Security techniques. Guidance for auditors on ISMS controls» (Информационная технология. Методы и средства обеспечения безопасности. Руководство для аудиторов системы менеджмента ИБ) [35] дополняет ISO/IEC 27007:2011 в части аудита средств управления ИБ, используемых в рамках СУИБ. Такой аудит выявляет, насколько хорошо СУИБ справляется с выполнением функций по ОИБ в организации любого размера и типа – общественной и частной, государственной и некоммерческой и т. п. Основой рассматриваемого в стандарте аудита выбран риск-ориентированный подход к управлению ИБ.

В то время как ISO/IEC 27007:2011 ориентирован на аудит всей СУИБ в целом, как это описано в ISO/IEC 27001, стандарт ISO/IEC 27008:2011 фокусируется на проверке средств управления ИБ, используемых в рамках СУИБ, описанных в ISO/IEC 27002 и перечисленных в приложении А ISO/IEC 27001. Стандарт ISO/IEC 27008:2011 не предназначен для аудита систем управления в целом, поскольку он ориентирован на процесс управления рисками ИБ в рамках СУИБ, определенный в ISO/IEC 27001 и 27005, и средства управления ИБ, перечисленные в ISO/IEC 27002. Он предоставляет собой руководящие указания по анализу реализации и функционирования средств управления ИБ, включая техническую проверку их соответствия вышеназванным стандартам и установленным в организации стандартам ИБ.

Проведенный в соответствии ISO/IEC 27008:2011 аудит позволит удостовериться, что СУИБ существует не только «на бумаге», но и предоставляет реальные свидетельства своего функционирования, поддающиеся проверке. Полученные результаты аудита могут быть использованы для усовершенствования СУИБ за счет оптимизации взаимодействия между отдельными процессами в рамках функционирования СУИБ и необходимым контролем уровня ИБ, обеспечиваемого этой СУИБ. В качестве примера таких мероприятий можно привести реализацию механизмов снижения вреда, причиненного сбоями в защите информации, за счет чего возможно появление ошибочных финансовых отчетов и некорректных документов, выпущенных организацией, а также негативное воздействие на нематериальные ценности, такие как репутация и имидж организации, частная жизнь, навыки и опыт людей.

2.1.9. ISO/IEC 27011:2008 – РУКОВОДСТВО ПО УПРАВЛЕНИЮ ИБ ДЛЯ ТЕЛЕКОММУНИКАЦИОННЫХ КОМПАНИЙ НА ОСНОВЕ ISO/IEC 27002

Стандарт ISO/IEC 27011:2008 «Information technology. Security techniques. Information security management guidelines for telecommunications organizations based on ISO/IEC 27002» (Информационная технология. Методы и средства обеспечения безопасности. Руководство по менеджменту ИБ для телекоммуникационных компаний, основанное на ISO/IEC 27002) [36] разработан совместно Международным союзом электросвязи (сектором стандартизации электросвязи) ITU-T и ИСО и опубликован как ISO/IEC 27011 и Рекомендации ITU-T X.1051 (СУИБ. Требования к телекоммуникационным компаниям) [37]. Он основан на следующих документах: ITU-T Recommendation X.800 (1991 г.) (Архитектура безопасности для взаимодействия открытых систем для CCITT-приложений), ITU-T Recommendation X.805 (2003) (Архитектура безопасности для систем, обеспечивающих сквозные коммуникации), ISO 9001:2000 (Системы менеджмента качества. Требования), ISO 14001:1996 (Системы менеджмента окружающей среды. Спецификация с руководством по использованию), ISO/IEC 27001, ISO/IEC 27002, ISO/IEC Guide 73:2002 (Управление рисками. Словарь. Руководство по использованию в стандартах).

Основное назначение стандарта ISO/IEC 27011:2008 – определить руководящие принципы, обеспечивающие реализацию управления ИБ для телекоммуникационных компаний (ТК) и соблюдение ими базовых требований конфиденциальности, целостности, доступности и любых других соответствующих свойств ИБ. Целевая аудитория стандарта не ограничивается только ТК. Он рассчитан на всех тех, кто отвечает за ОИБ, продавцов (вендоров), аудиторов, поставщиков телекоммуникационных терминалов, поставщиков (провайдеров) прикладного контента и т. д.

Конфиденциальность в ISO/IEC 27011:2008 определяется как то, что информация, с которой работает ТК, должна быть защищена от несанкционированного раскрытия. Это означает неразглашение информации о коммуникациях в терминах существования, содержания, источника, места назначения и даты и времени передачи информации. Очень важно, чтобы ТК обеспечивали соблюдение неразглашения информации о коммуникациях, обрабатываемой ими. Лица, привлеченные ТК, должны сохранять конфиденциальность любой информации обо всем, что, возможно, стало им известно во время выполнения ими своих трудовых обязанностей.

Целостность понимается как то, что инсталляция и использование телекоммуникационных средств должны контролироваться, обеспечи-

вать подлинность, точность и полноту информации, переданной или полученной по проводам, радиоканалам или любыми другими методами.

Доступность означает, что при необходимости должен быть обеспечен только авторизированный доступ к информации, передаваемой с помощью телекоммуникаций, самим телекоммуникационным средствам и среде, используемой для функционирования средств связи, независимо от того, какими методами она передается или получается – по проводам, радиоканалам и т. п. Расширяя доступность, в случае чрезвычайных ситуаций ТК должны предоставлять приоритет наиболее важным средствам связи и соблюдать требования соответствующих нормативных документов.

Для ТК сети, линии связи, хранимая, обрабатываемая и передаваемая информация являются важными активами. Для эффективного управления этими активами и успешного ведения бизнеса ТК необходимо управление ИБ, независимо от способа связи – проводного, беспроводного или широковещательного. Архитектура и реализация СУИБ продиктованы потребностями бизнеса, требованиями по ОИБ, используемыми процедурами, а также размером и структурой ТК. Предполагается, что со временем все эти характеристики и поддерживающие их системы изменяются. Поэтому реализация СУИБ будет масштабироваться в соответствии с изменяющимися потребностями организации.

Если управление и средства управления ИБ реализованы не должным образом, то риск нарушения конфиденциальности, целостности и доступности может возрасти.

Поскольку ТК предоставляют телекоммуникационные сервисы, используя средства связи и сервисы посредников совместно с другими организациями, то к передаваемой ими информации имеют доступ не только их сотрудники, но и другие пользователи вне этих организаций. Поэтому управление ИБ для ТК охватывает все области сетевой инфраструктуры, сервисные приложения и многое другое.

Стандарт ISO/IEC 27011:2008 содержит следующие основные разделы:

1) обзор (структура рекомендаций, система управления ИБ в телекоммуникационной сфере);

2) ПолИБ;

3) организацию ИБ (внутренняя организация, внешние стороны);

4) управление активами (ответственность за активы, классификация информации);

5) безопасность персонала (до приема на работу, работа, увольнение или смена работы);

6) физическую и экологическую безопасность (защищаемые области, безопасность оборудования);

7) управление средствами связи и их функционированием (процедуры функционирования и обязанности, управление сервисами доставки третьим лицам, планирование систем и их приемка, защита от вредо-

носного и мобильного кода, резервирование, управление безопасностью сетей, управление средой, обмен информацией, сервисы электронной коммерции, мониторинг);

8) управление доступом (бизнес-требования к управлению доступом, управление доступом пользователей, обязанности пользователей, управление сетевым доступом, управление доступом к ОС, приложениям и информации, мобильные вычисления и дистанционная работа);

9) приобретение, развитие и сопровождение ИС (требования по ОИБ для ИС, корректная обработка в приложениях, управление с использованием криптографии, защита файловых систем, безопасность процессов разработки и поддержки, устранение технических уязвимостей);

10) управление инцидентами ИБ (подготовка отчетов о событиях ИБ и уязвимостях, процесс управления инцидентами ИБ и его усовершенствование);

11) управление непрерывностью бизнеса (с учетом аспектов ИБ);

12) соответствие.

ITU-T предложил расширить ISO/IEC 27011:2008 двумя новыми частями:

1) руководящие принципы управления безопасностью для малых и средних ТК: руководство по реализации управления ИБ на основе рекомендаций X.1051 (стандарта ISO/IEC 27011);

2) руководящие принципы управления активами: руководство по хорошим практикам в области управления активами для ТК.

2.1.10. ISO/IEC 27013 – РУКОВОДСТВО ПО ИНТЕГРИРОВАННОМУ ВНЕДРЕНИЮ СТАНДАРТОВ ISO/IEC 20000 И 27001

Проект стандарта ISO/IEC 27013 «Information technology. Security techniques. Guideline on the integrated implementation of ISO/IEC 20000–1 and ISO/IEC 27001» (Информационная технология. Методы и средства обеспечения безопасности. Руководство по интегрированному внедрению стандартов ISO/IEC 20000–1 и ISO/IEC 27001) [38], публикация которого ожидается в 2012 г. и совпадает с пересмотром стандарта ISO/IEC 20000-1, представляет собой руководство по системам интегрированного управления ИБ и ИТ-сервисами как взаимодополняющих и поддерживающих друг друга систем управления. Этот стандарт поможет организациям осуществить реализацию систем интегрированного управления ИБ и ИТ-сервисами и обеспечить необходимое документальное сопровождение этого процесса в соответствии с основными положениями стандартов ISO/IEC 27001 и ISO/IEC 20000:2005 «IT Service Management System» (Система менеджмента ИТ-сервисов). Стандарт ISO/IEC 20000 посвящен управлению и обслуживанию ИТ-сервисов, учитывающим лучшие существующие практики, и состоит из двух частей.

Первая часть ISO/IEC 20000–1:2005 «Information technology service management. Specification for Service Management» (Менеджмент ИТ-

сервисов. Спецификация управления сервисом) содержит подробное описание требований к системе менеджмента ИТ-сервисов (на основе документов библиотеки ITIL (Information Technology Infrastructure Library) и устанавливает ответственность за инициирование, выполнение и поддержку таких систем в организациях [39]. В стандарте рассматривает пять основных групп процессов:

1) предоставления сервисов, включая управление уровнем сервисов, управление непрерывностью и доступностью, управление мощностями, отчётность по предоставлению сервисов, управление ИБ, распределение бюджета и учёт затрат);

2) взаимодействия, включая управление взаимодействием с бизнесом и управление сервис-провайдерами (поставщиками сервисов);

3) разрешения, включая управление проблемами и инцидентами;

4) контроля, включая управление изменениями и конфигурациями;

5) управления релизами (новыми версиями и откорректированными имеющимися решениями).

Вторая часть ISO/IEC 20000–2:2005 «Information technology service management. Code of Practice for Service Management» (Менеджмент ИТ-сервисов. Практические правила управления сервисом) дает практические рекомендации по процессам, требования к которым сформулированы в ISO/IEC 20000–1, и является руководством для аудиторов и компаний, намеренных пройти сертификацию [40].

Стандарт ISO/IEC 27013 создаст основу для организации и приоритезации деятельности в следующих направлениях:

- координация задач усовершенствования и управления для ИБ и сервисов;
- координация междисциплинарной деятельности, ведущей к внедрению интегрированного подхода (например, при управлении инцидентами);
- создание общей системы процессов и их документирования (включая политики, процедуры и многое другое);
- выработка единой терминологии и единых точек зрения;
- объединение преимуществ для бизнеса клиентов и сервис-провайдеров и извлечение дополнительной выгоды, появляющейся при интеграции двух систем управления – ИБ- и ИТ-сервисами;
- совместный аудит этих систем управления в одно время и сокращение затрат на его проведение.

2.1.11. ISO/IEC 27014 – ИНФРАСТРУКТУРА РУКОВОДСТВА ИБ

Разрабатываемый в настоящее время проект стандарта ISO/IEC 27014 «Information technology. Security techniques. Information security governance framework» (Информационная технология. Методы и средства обеспечения безопасности. Инфраструктура руководства ИБ) станет руководством, помогающим организациям руководить (англ. *govern*) их

ИБ, определяющим для них базовую инфраструктуру эффективного управления ИБ и показывающим, как ее использовать для оценки, задания основных направлений деятельности и мониторинга функционирования СУИБ [41].

Такое руководство должно установить задачи, принципы и процессы в рамках инфраструктуры руководства ИБ и должно учесть следующие важные факторы:

- бизнес-стратегии, политики и задачи организации в отношении ИБ, рисков и средств управления ИБ;
- соответствие надлежащими государственным нормативным документам и законам в отношении обязательств в области ИБ;
- соблюдение соответствия контрактным и другим правовым обязательствам в отношении третьих лиц и самими третьими лицами в области ИБ;
- требования к аудиту и, возможно, сертификации с целью обеспечения гарантий (в смысле уверенности относительно владения ситуацией в области ИБ) для третьих лиц.

Ожидается, что стандарт рассмотрит следующие аспекты руководства:

- управление рисками – особенно управление рисками ИБ;
- средства управления – применительно к СУИБ, являющейся основой для всех средств управления ИБ в организации;
- деятельность в области соблюдения соответствий и предоставления гарантий – особенно для сертифицирующих аудитов, внутренних аудитов, составления отчетов по СУИБ для руководства организации и т. п.;
- взаимосвязь руководств ИБ, ИТ и всеми информационными активами организации;
- различия между «руководством» и «менеджментом»;
- подотчетность и ответственность за ОИБ, владение информационными активами внутри организации.

Данный стандарт будет учитывать потребности всех заинтересованных сторон: акционеров, регуляторов, аудиторов и руководства организаций, а также основные принципы, изложенные в стандарте ISO/IEC 38500:2008, посвященном руководству ИТ.

2.1.12. ISO/IEC 27015 – РУКОВОДСТВО ПО УПРАВЛЕНИЮ ИБ ДЛЯ ФИНАНСОВЫХ СЕРВИСОВ

Обсуждаемый в настоящее время проект стандарта ISO/IEC 27015 «Information technology. Security techniques. Information security management guidance for financial services» (Информационная технология. Методы и средства обеспечения безопасности. Руководство по управлению ИБ для финансовых сервисов) посвящен вопросам управления ИБ в сфере предоставления финансовых услуг и призван помочь

внедрять СУИБ в этой сфере с учетом требования стандартов серии 27000. Хотя уже существуют стандарты по ИБ и обработке рисков, такие как ISO TR 13569:2005 «Financial services. Information security guidelines» (Финансовые сервисы. Руководство по ИБ), SOX, Basel II (теперь и III) и т. п., стандарт ISO/IEC 27015 будет точно соответствовать всем требованиям к СУИБ, изложенным в ISO/IEC 27001 и ISO/IEC 27002.

ISO/IEC 27015 направлен на поддержку специфической деятельности финансовых организаций, особенно заинтересованных в ОИБ, для которых таким образом будет создана международно признанная и одобренная основа для ведения бизнеса, отвечающая всем правовым требованиям и требованиям регуляторов. В стандарте будет представлено руководство, позволяющее выполнять как основные требования по управлению ИБ и реализации средств управления ИБ по поддержке конфиденциальности, целостности и доступности, так и другие значимые требования по ОИБ.

Стандарт ISO/IEC 27015 рассчитан на организации финансового и страхового сектора, их бизнес-партнеров и клиентов. Он использует риск-ориентированный подход к СУИБ и, следовательно, позволяет достичь определенной гибкости при разработке защиты информационных активов конкретной организации. При этом учитываются следующие важные факторы: бизнес-стратегия организации и текущие возможности данного сегмента рынка, характеристики различных географических регионов, специфические сервисы и производимая продукция организации, применимые правовые ограничения и ограничения регуляторов.

ISO/IEC 27015 не претендует на определение обязательных требований. Скорее он будет служить руководством по обеспечению видимой наглядности деятельности по управлению ИБ в организации и доказательству бизнес-парнерам, клиентам и соответствующим регулирующим органам следования ею лучшим практикам в области управления и обеспечения ИБ.

2.1.13. ISO/IEC 27031:2011 – РУКОВОДСТВО ПО ГОТОВНОСТИ ИНФОРМАЦИОННЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ БИЗНЕСА

Стандарт ISO/IEC 27031:2011 «Information technology. Security techniques. Guidelines for information and communications technology readiness for business continuity» (Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности ИТТ к непрерывности бизнеса) содержит концепции и принципы, возлагаемые на ИТТ как на необъемлемую часть критической инфраструктуры любой организации по обеспечению непрерывности ее бизнеса [42]. Этот стандарт официально заменяет британский стандарт BS 25777:2008 «Information and communications technology continuity management. Code

of practice» (Управление непрерывностью ИТТ. Практические правила) [43], который в свою очередь был разработан на базе существующих стандартов обеспечения непрерывности бизнеса (ОНБ) BS 25999 и дополняющей их открытой спецификации PAS 77:2006 «IT Service Continuity Management. Code of practice» (Управление непрерывностью ИТ-сервисов. Практические правила) [44], обобщающей лучшую мировую практику в области обеспечения непрерывности ИТ-сервисов, а именно принципов и методов управления ИТ-сервисами, но не представляющее собой пошаговую инструкцию по внедрению процессов управления непрерывностью ИТ-сервисов. Управление непрерывностью ИТТ обеспечивает необходимую жизнеспособность ИТТ и сервисов и возможность их восстановления до заранее определенного уровня в необходимые сроки, согласованные с руководством организации. Эффективное УНБ зависит от управления непрерывностью ИТТ, чтобы гарантировать, что организация всегда способна достичь своих целей, особенно в моменты аварий и бедствий.

Сделаем важное замечание относительно терминологии. Термины «ИТ» (англ. *information technology*), «информационные и коммуникационные технологии» (англ. *information and communications technology*) и «информационные и телекоммуникационные технологии» (англ. *information and telecommunications technology*) часто применяются как синонимы и вкладываемый в эти понятия смысл одинаков. Эту же точку зрения разделяют и авторы данного учебного пособия. При изложении учебного материала используются два термина – ИТ и ИТТ, но так, как они упоминаются в англоязычном первоисточнике.

Предшественник ISO/IEC 27031:2011 британский стандарт BS 25777:2008 раскрывает такие вопросы как:

- управление программой управления непрерывности ИТТ;
- внедрение принципов управления непрерывностью ИТТ в культуру организации;
- документирование системы управления непрерывностью ИТТ;
- определение требований к непрерывности ИТТ;
- разработка и реализация стратегии обеспечения непрерывности ИТТ;
- разработка и тестирование планов обеспечения непрерывности ИТТ;
- проведение обучения и повышения осведомленности в области восстановления сервисов ИТТ (под ними понимается совокупность функциональных возможностей ИТТ, предоставляемая конечным пользователям в качестве услуги; примеры сервисов ИТТ – передача сообщений, бизнес-приложения, сервисы файлов и печати, сетевые сервисы и т. п.);
- сопровождение, анализ и совершенствование системы управления непрерывностью ИТТ.

В ISO/IEC 27031:2011 предложена базовая основа (методы и процессы) для любого типа организаций, определены и описаны все аспекты

(включая критерии, проектирование и реализацию), позволяющие улучшить готовность ИТТ (ГИТТ) в рамках СУИБ организации для обеспечения непрерывности ее бизнеса, а также последовательно и общепринятым способом измерить непрерывность, безопасность и готовность к преодолению аварий и бедствий. В этом стандарте сделана попытка объединить ИБ, восстановление после аварий и бедствий и УНБ по отношению к ГИТТ.

Область действия настоящего стандарта – все события и инциденты (в том числе связанные с ИБ), которые могут воздействовать на инфраструктуру и системы ИТТ. Системы ИТТ включают аппаратные, программные и программно-аппаратные средства компьютеров, телекоммуникационное и сетевое оборудование и другие электронные системы обработки информации и взаимосвязанное оборудование. Стандарт расширяет практику обработки и управления инцидентами ИБ на область планирования готовности и соответствующих сервисов ИТТ.

Готовность ИТТ к ОНБ (общий термин для процессов, описанных в стандарте) способствует УНБ путем обеспечения того, что «сервисы ИТТ настолько устойчивы, насколько это требуется, и могут быть восстановлены до заранее заданных уровней в течение сроков, необходимых и согласованных для организации». Это важно, поскольку во многих современных организациях ИТТ превалируют над другими технологиями и являются основными компонентами поддержания критически важных бизнес-процессов и процессов управления. Планирование непрерывности бизнеса без надлежащей защиты доступности и непрерывности функционирования ИТТ невозможно.

Готовность ИТТ должна снижать для организации негативное воздействие (масштаб, продолжительность и/или последствия) инцидентов ИБ и включает в себя:

- подготовку в организации ИТТ (то есть инфраструктуру, функционирование и приложения для ИТТ) и взаимосвязанных процессов и персонала к противодействию непредвиденным обстоятельствам, которые могут изменить риски и повлиять на непрерывность функционирования самих ИТТ и всего бизнеса организации;
- перераспределение и оптимизацию использования ресурсов между ОНБ, восстановлением после аварий/бедствий, реакцией на нештатные ситуации и инциденты, нарушающие безопасность ИТТ, и управленческой деятельностью.

Стандарт ISO/IEC 27031:2011 базируется на цикле PDCA, расширяя обычный процесс планирования непрерывности бизнеса за счет большего учета влияния на него ИТТ. Также используются такие методы оценки сценариев сбоев, как анализ отказов и их последствий FMEA (Failure Modes and Effects Analysis), при котором определяются «запускающие события» или «события-триггеры» (англ. *triggering events*), влекущие за собой серьезные инциденты.

Основная содержательная часть ISO/IEC 27031:2011 представлена следующими разделами: роль готовности ИТТ для ОНБ при УНБ; планирование готовности ИТТ; внедрение и использование, мониторинг и анализ, улучшение.

Если организация при создании СУИБ ориентируется на ISO/IEC 27001 и/или использует открытую спецификацию ISO 22399:2007 для разработки системы УНБ (СУНБ), планирование готовности ИТТ также должно основываться на данных стандартах и проводиться в рамках создания СУИБ и СУНБ, что позволит избежать дублирования одинаковых процессов в одной организации.

Есть отдельный стандарт ISO/IEC 24762:2008 по восстановлению ИТТ после аварий, который вышел вне рамок серии стандартов 27000. Также ведется работа по другим стандартам, касающимся непрерывности бизнеса, включая стандарт ISO 22301 (Общественная безопасность. Системы управления обеспечением готовности и непрерывности. Требования).

2.1.14. ISO/IEC 27033 – УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ СЕТЕЙ

Необходимость в обеспечении безопасности сетей особенно важна в современном информационном пространстве, так как многие организации объединяют свои сети. Сетевые соединения могут находиться в границах самой организации, между разными организациями и иногда между организацией и сетями общего пользования. Поэтому бизнес организаций сильно зависит от всех видов связи – от классических автоматизированных систем информационного обслуживания до беспроводного и радиодоступа. Их потребности в сетях должны быть удовлетворены, при этом обеспечению безопасности сетей придается все большее значение. Стандарт ISO/IEC 27033 «Information technology. Security techniques. Network security» (Информационная технология. Методы и средства обеспечения безопасности. Безопасность в сетях) как раз и освещает вопросы обеспечения безопасности в сетях.

В настоящее время планируется в составе ISO/IEC 27033 объединить семь частей, первая и третья из которых уже опубликованы:

ISO/IEC 27033–1:2009 «Общие положения и концепции» [45] и идентичный ему введенный в действие в России с 2012 г. ГОСТ Р ИСО/МЭК 27033–1–2011 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции» [46]. В стандарте определяются и описываются концепции, связанные с управлением безопасностью сетей и обеспечивающие такое управление. Приводится обзор вопросов, относящихся к безопасности сетей, вводятся основные определения, дается руководство по идентификации и анализу рисков ИБ в сетях, определяются основные требования по безопасности сетей и средствам управления ИБ в сетях. Также описывается, как достичь хорошего качества архитекту-

ры ОИБ с технической точки зрения. Стандарт содержит большой список определений и сокращений в области безопасности сетей. Кратко описан процесс планирования и управления безопасностью сетей и рассмотрены основы сетевого взаимодействия, после чего даны рекомендации по идентификации рисков ИБ для сетей и выделены возможные области управления безопасностью сетей. В качестве необходимых защитных мер выделены следующие: утверждение и следование ПолИБ для сетей, процедуры ОИБ и проверки ИБ, технические аспекты устранения уязвимостей, идентификация, аутентификация и авторизация, мониторинг и аудит безопасности, обнаружение и предотвращение вторжений, защита от вредоносного ПО, сервисы на основе криптографии, УНБ. Перечислены основные виды сетевых архитектур, для которых необходимы руководящие указания по проектированию и реализации защиты в сетях (более подробно угрозы для этих архитектур рассмотрены в третьей части стандарта). Связанные с этими вопросами технологические аспекты таковы (они представлены в приложении): локальные, глобальные, беспроводные, радио, широковещательные, виртуальные, голосовые сети, шлюзы безопасности, конвергенция IP, веб-хостинг, электронная почта Интернета, маршрутизируемый доступ к третьим организациям, центры обработки данных. Также отдельное внимание уделено разработке и тестированию решений по ОИБ в сетях, их функционированию, мониторингу и анализу.

ISO/IEC 27033–2 «Руководство по проектированию и внедрению системы обеспечения безопасности сетей». Определяет, как организация должна создавать архитектуру, проект и реализацию технической безопасности для сетей, которые будут обеспечивать эффективную, соответствующую бизнес-требованиям защиту, опирающуюся на базовые модели и понятную для всех сотрудников организации, вовлеченных в планирование, проектирование и внедрение архитектурных аспектов безопасности сетей.

ISO/IEC 27033–3:2010 «Базовые сетевые сценарии – угрозы, методы проектирования и средства управления» [47]. Определяет специфические риски, методики проектирования и вопросы управления, связанные с типичными сценариями использования сетей и понятные для всех сотрудников организации, вовлеченных в планирование, проектирование и внедрение архитектурных аспектов безопасности сетей. Риски рассматриваются в следующих областях предоставления сервисов: доступ в Интернет, взаимодействие различных организаций между собой (от англ. *Business to Business* – бизнес для бизнеса) и с клиентами (англ. *Business to Customer*), коллективная работа, сегментация сетей, сетевое взаимодействие для работы из дома и небольшими офисами, мобильная связь, удаленные пользователи, аутсорсинг. В приложениях приводятся политика использования Интернета и каталог угроз ИБ.

ISO/IEC 27033–4 «Обеспечение безопасности межсетевых взаимодействий при помощи шлюзов безопасности – угрозы, методы проектирования и средства управления». Определяет специфические риски, методики проектирования и средства управления для защиты информации, циркулирующей между сетями, соединенными шлюзами безопасности. Предназначен для всех сотрудников организации, вовлеченных в планирование, проектирование и внедрение шлюзов безопасности.

ISO/IEC 27033–5 «Обеспечение безопасности виртуальных частных сетей – угрозы, методы проектирования и средства управления». Определяет специфические риски, методики проектирования и средства управления для защиты соединений, устанавливаемых посредством использования виртуальных частных сетей (ВЧС) (англ. *Virtual Private Network, VPN*). Предназначен для всех сотрудников организации, вовлеченных в планирование, проектирование и внедрение ВЧС.

ISO/IEC 27033–6 «Конвергенция в IP-сетях (Определение угроз, методов проектирования и средств управления в IP-сетях с конвергенцией данных, голоса и видео)». Определяет специфические риски, методики проектирования и средства управления для защиты конвергентных IP-сетей, например, IP-сетей с конвергенцией данных, голоса и видео. Предназначен для всех сотрудников организации, вовлеченных в планирование, проектирование и внедрение таких сетей.

ISO/IEC 27033-7 «Руководство по обеспечению безопасности беспроводных сетей – риски, методы проектирования и средства управления». Определяет специфические риски, методики проектирования и средства управления для защиты беспроводных и радиосетей. Предназначен для всех сотрудников организации, вовлеченных в планирование, проектирование и внедрение таких сетей.

Со временем, возможно, будут разработаны и другие дополнительные части стандарта.

Стандарт ISO/IEC 27033 и соответствующий ГОСТ Р ИСО/МЭК 27033 постепенно (по мере принятия новых частей) заменяют международный стандарт сетевой безопасности ISO/IEC 18028, расширяющий разделы 10.6 и 11.4 стандарта ISO/IEC 27002 и руководство по управлению безопасностью ИТ стандарта ISO/IEC 13335 за счет более детальной спецификации основных операций и механизмов реализации мер защиты сетей и средств управления ИБ в различных сетевых средах, а также установления тесной взаимосвязи между внедрением управления безопасностью ИТ и техническими аспектами безопасности сетей. ISO/IEC 18028 состоит из пяти частей, опубликованных в 2005–2006 гг. и рассматривающих следующие вопросы: управление безопасностью сетей, архитектура безопасности сетей, защита сетевых взаимодействий при помощи шлюзов безопасности, защита удаленного доступа, защита сетевых взаимодействий при помощи ВЧС. Первая часть стандарта ISO/IEC 18028–1:2006 содержит руководство по созданию сетей и орга-

низации их взаимодействия с учетом аспектов безопасности и при удаленном доступе к сети. Руководство включает идентификацию и анализ факторов, связанных с сетевыми взаимодействиями, которые следует учитывать при определении требований к безопасности сетей, выделяет необходимые средства управления при подключении к сетям, включая проектирование и внедрение, которые подробно рассматриваются в остальных четырех частях стандарта.

2.1.15. ISO/IEC 27035:2011 – УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИБ

Никакие типовые ПолИБ или методы и средства ОИБ не могут гарантировать полную защиту информации, информационных систем, сервисов или сетей. Средства управления ИБ еще несовершенны и независимо от их форм могут быть на практике невыполнимы вообще, недостаточны или полностью отсутствовать. Даже превентивные защитные меры не могут предусмотреть заранее все и поэтому не вполне надежны. После внедрения защитных мер с большой долей вероятности останутся уязвимости, которые могут сделать ОИБ неэффективным, и, следовательно, способствовать реализации инцидентов ИБ, оказывающих прямое или косвенное негативное воздействие на бизнес организации. Кроме этого, в динамически изменяющемся современном мире будут неизбежно выявляться новые, ранее неизвестные угрозы ИБ. Поэтому недостаточная подготовка организации к обработке таких инцидентов делает практическую реакцию на инциденты ИБ малоэффективной, и это увеличивает ущерб для ее бизнеса. Управление инцидентами ИБ успешно сочетает детективные и корректирующие защитные меры, минимизируя негативные последствия инцидентов, по возможности позволяет собрать доказательства для дальнейшего расследования и извлечь уроки, улучшив СУИБ, особенно за счет внедрения превентивных мер. Инциденты ИБ обычно основаны на использовании ранее невыявленных и/или неконтролируемых уязвимостей, поэтому установка обновлений к ИС, устранение слабых мест в различных процедурах и прочее – это действия и превентивные и корректирующие одновременно.

Стандарт ISO/IEC 27035:2011 «Information technology. Security techniques. Information security incident management» (Информационная технология. Методы и средства обеспечения безопасности. Управление инцидентами ИБ) [48] содержит структурированный и планомерный подход:

- к обнаружению, составлению отчетов и оценке инцидентов ИБ;
- осуществлению ответной реакции и управлению инцидентами ИБ;
- обнаружению, оценке и устранению уязвимостей;
- постоянному улучшению управления ИБ и инцидентами ИБ.

После принятия в конце 2011 г. этот стандарт заменяет ISO/IEC TR 18044:2004 «Information technology. Security techniques. Information

security incident management» (Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов ИБ) [49]. В России был принят идентичный ISO/IEC TR 18044:2004 ГОСТ Р ИСО/МЭК ТО 18044–2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности» [50], который определяет формальную модель процессов управления инцидентами ИБ и устанавливает рекомендации по менеджменту инцидентов ИБ для руководителей подразделения по ИБ, информационных систем, сервисов и сетей.

В ISO/IEC 27035:2011 является достаточно емким и всесторонне рассматривает управление как уязвимостями (англ. *vulnerability management*), так и инцидентами ИБ. Приводятся шаблоны для подготовки отчетов по событиям, инцидентам ИБ и уязвимостям.

В стандарте после освещения основ управления инцидентами ИБ, его преимуществ и ключевых вопросов, некоторых примеров инцидентов ИБ и причин их возникновения процесс управления инцидентами ИБ рассматривается как включающий несколько подпроцессов:

1) планирование и подготовка к обработке инцидентов ИБ, включая составление документов, поддерживающих управление инцидентами;

2) обнаружение/идентификация и подготовка отчета по инциденту ИБ;

3) оценка инцидента и принятие решений по инциденту ИБ;

4) ответная реакция на инцидент ИБ;

5) извлечение уроков из инцидента ИБ.

Даются рекомендации по необходимым ресурсам и процедурам.

В приложениях содержатся примерные формы отчетов о событиях и инцидентах ИБ и некоторые примерные общие рекомендации для оценки негативных последствий инцидентов ИБ, включаемых в формы отчетов.

В ISO/IEC 27035:2011 и ГОСТ Р ИСО/МЭК ТО 18044–2007 описание процессов управления инцидентами ИБ, как и в стандарте ISO/IEC 27001, основано на использовании циклической модели PDCA. Поэтому в процессе разработки процесса управления инцидентами ИБ возможно связать требования ISO/IEC 27001 и представленную модель управления инцидентами ИБ и создать процесс, полностью удовлетворяющий требованиям ISO/IEC 27001. Целями следования этой модели является уверенность в том:

- что события и инциденты ИБ выявляются и обрабатываются эффективным образом, в особенности в части классификации событий ИБ;
- выявленные в организации инциденты ИБ учитываются и обрабатываются наиболее подходящим и эффективным для них образом;
- последствия инцидентов ИБ могут быть минимизированы в процессе реагирования на инциденты, возможно с привлечением процессов ОНБ;
- за счет анализа событий и инцидентов ИБ повышается вероятность предотвращения инцидентов в будущем, улучшаются механизмы и процессы ОИБ.

2.1.16. ISO/IEC 27037 – РУКОВОДСТВО ПО ИДЕНТИФИКАЦИИ, СБОРУ И/ИЛИ ПОЛУЧЕНИЮ И ОБЕСПЕЧЕНИЮ СОХРАННОСТИ СВИДЕТЕЛЬСТВ, ПРЕДСТАВЛЕННЫХ В ЭЛЕКТРОННОЙ ФОРМЕ

Область знаний, посвященная сбору доказательств для последующего расследования компьютерного преступления, в англоязычной литературе называется *компьютерной форензикой* (англ. *computer forensics*). В российских публикациях по данной теме используется термин «*технико-криминалистическая экспертиза*» (ТКЭ).

Наиболее критическими аспектами проведения ТКЭ являются сбор и сохранение доказательств, которые должны проводиться таким образом, чтобы обеспечить их целостность. Как и при сборе обычных физических доказательств, для определения первых и всех промежуточных звеньев совершения преступления решающее значение имеет забота о последовательном сохранении всех доказательств, представленных в электронной форме (англ. *digital evidence*). Это гарантирует, что они собирались и защищались с помощью строго структурированных процессов, признаваемых судами. Не просто обеспечивая целостность, такие процессы должны еще гарантировать, что с доказательствами ничего плохого не может произойти и в будущем. Для этого требуется соблюдение или даже превышение базового уровня защиты доказательств.

Доказательства в электронной форме как информация, которая может быть представлена в суде, порождается любым электронным хранилищем (базой) или средствами связи (например, мобильными телефонами, компьютерами, iPod'ами, консолями видеоигр и т. д.). По своей природе она очень непрочна, поскольку может быть легко уничтожена или изменена в случае недолжного обращения по неосторожности или со злым умыслом.

Недавние международные инициативы, такие как «Конвенция о киберпреступности», продемонстрировали, что международное сообщество признает важность совершенствования и совместного использования лучших практик в области доказательств, представленных в электронной форме.

Проект стандарта ISO/IEC 27037 «Information technology. Security techniques. Guidelines for identification, collection and/or acquisition and preservation of digital evidence» (Информационная технология. Методы и средства обеспечения безопасности. Руководство по идентификации, сбору и/или получению и обеспечению сохранности свидетельств, представленных в электронной форме) как раз предоставляет руководство по сбору и сохранению доказательств компьютерных преступлений, представленных в электронной форме. Ожидается, что его можно будет использовать при трансграничных преступлениях (когда жертва и атакующий находятся в различных государствах), когда собранные в одной стране доказательства должны быть признаны и приняты к рас-

смотрению в суде другой страны. В настоящее время юридические тонкости законов не позволяют добиться этого, поскольку в разных странах разработаны собственные руководства и процедуры сбора и сохранения доказательств в электронной форме. Кроме этого, события, классифицируемые как преступление в одной стране, в другой таковыми не считаются.

Проект ISO/IEC 27037 разработан на основе британского стандарта BS 10008:2008 «Evidential weight and legal admissibility of electronic information. Specification» (Допустимость электронной информации в качестве доказательств и её доказательная сила. Спецификации) [51], соблюдение требований которого обеспечивает максимальную доказательную силу электронной информации, используемой в качестве свидетельства деловых транзакций. В стандарте сформулированы требования к планированию, внедрению, оперативному использованию, мониторингу и совершенствованию систем управления электронной информацией, применяемых организацией, и к процессам электронной передачи информации из одной компьютерной системы в другую, в связи с задачей обеспечения целостности и аутентичности электронной информации.

Стандарт ISO/IEC 27037 будет содержать детальное руководство по идентификации, сбору и/или получению, пометке, хранению, транспортировке и сохранению доказательств в электронной форме, в частности, с точки зрения обеспечения их целостности. Будет определен и описан гармонизированный для разных стран процесс распознавания и идентификации, документирования «места преступления», сбора и сохранения, упаковки и транспортировки доказательств. Будут рассмотрены доказательства, порождаемые различными источниками: источниками статических данных, транзитными данными (например, перемещающимися по сетям), источниками данных, передаваемых беспроводным образом (например, мобильными телефонами) и т. д.

Для более широкого применения стандарт не будет использовать специальную юридическую терминологию. Он не будет анализировать доказательства в электронной форме, их конкретное наполнение, вес, релевантность и т. д., а также не будет обязывать использовать конкретные средства и методы.

2.2. Стандарты на отдельные процессы управления ИБ и оценку безопасности ИТ

2.2.1. ISO/IEC 13335 – МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Стандарт ISO/IEC 13335 «Information technology. Security techniques. Management of information and communications technology security» (Информационная технология. Методы и средства обеспечения безопасно-

сти. Менеджмент безопасности ИТТ), первоначально появившийся в статусе технического отчета, прежде чем стать полноценным стандартом ISO/IEC, объединил несколько руководящих документов по управлению безопасностью ИТ. Он состоит из четырех частей:

- ISO/IEC 13335–1:2004 «Концепции и модели менеджмента безопасности информационных и телекоммуникационных технологий» объясняет концепции и модели управления безопасностью ИТТ. Последняя переработанная версия ISO/IEC 13335–1–2004 содержит и вторую часть стандарта ISO/IEC 13335–2, которая после этого была отменена как самостоятельная часть стандарта 13335 [52].
- ISO/IEC TR 13335–3:1998 «Методы менеджмента безопасности информационных технологий» устанавливала методы управления ИБ ИТ, но в настоящее время эта часть стандарта отменена и заменена стандартом ISO/IEC 27005.
- ISO/IEC TR 13335–4:2000 «Методы и средства менеджмента безопасности информационных технологий» охватывала выбор защитных мер (в смысле технических средств управления ИБ, но в настоящее время эта часть стандарта также отменена и заменена стандартом ISO/IEC 27005.
- ISO/IEC TR 13335–5:2001 «Руководство по менеджменту безопасности сети» представляет собой руководство по управлению безопасностью сетей. В настоящее время и эта часть стандарта отменена и заменена стандартом ISO/IEC 18028–1, который, в свою очередь, стал частью стандарта ISO/IEC 27033 [53].

В России были приняты четыре стандарта, идентичные соответствующим частям ISO/IEC 13335:

1. ГОСТ Р ИСО/МЭК 13335–1–2006 «Информационная технология. Методы и средства обеспечения безопасности. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» (идентичный ISO/IEC 13335–1:2004) [54] представляет собой руководство по управлению безопасностью ИТТ, устанавливает концепцию и модели, лежащие в основе базового понимания безопасности ИТТ, и раскрывает общие вопросы управления, которые важны для успешного планирования, реализации и поддержки безопасности ИТТ. Отмечается, что для создания эффективной программы безопасности ИТТ фундаментальными являются следующие высокоуровневые принципы безопасности:

- менеджмент риска – активы должны быть защищены путем принятия соответствующих мер, которые должны выбираться и применяться на основании соответствующей методологии управления рисками, устанавливающей допустимые риски и учитывающей существующие ограничения, исходя из активов организации, угроз, уязвимостей и различных воздействий угроз;

- обязательства организации в области ОИБ ИТТ и в управлении рисками ИБ, для формирования которых следует разъяснить преимущества от реализации защиты ИТТ;
- служебные обязанности и ответственность за ОИБ активов, которые должны быть определены и доведены до сведения персонала;
- цели, стратегии и политика, которые должны учитываться при управлении рисками, связанными с защитой ИТТ организации;
- управление жизненным циклом – управление ИБ ИТТ должно быть непрерывным в течение всего их жизненного цикла.

2. ГОСТ Р ИСО/МЭК ТО 13335–3–2007 «Информационная технология. Методы и средства обеспечения безопасности. Методы менеджмента безопасности информационных технологий» [55] (идентичный ISO/IEC TR 13335–3:1998) устанавливает методы управления ИБ ИТ, в основе которых лежат общие принципы, установленные ISO/IEC 13335–1. В стандарте приведены общий обзор способов управления, цели, стратегия и политика обеспечения безопасности ИТТ, описание вариантов стратегии анализа рисков и детальное описание комбинированного подхода анализа рисков, вопросы применения защитных мер и ознакомления с ними персонала и процесса их одобрения, описание работ по последующему наблюдению за системой, необходимых для обеспечения эффективного действия средств защиты. В настоящее время заменен действующим ГОСТ Р ИСО/МЭК 27005–2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» [31].

3. ГОСТ Р ИСО/МЭК ТО 13335–4–2007 «Информационная технология. Методы и средства обеспечения безопасности. Выбор защитных мер» [56] (идентичный ISO/IEC TR 13335–4:2000) является руководством по выбору защитных мер с учетом потребностей и проблем безопасности организации. В стандарте описан процесс выбора защитных мер в соответствии с риском системы безопасности и с учетом особенностей окружающей среды, а также устанавливаются способы достижения соответствующей защиты на основе базового уровня безопасности. Приведенный в стандарте подход к выбору защитных мер согласован с методами управления ИБ ИТ, приведенными в ISO/IEC TR 13335–3. В настоящее время заменен действующим ГОСТ Р ИСО/МЭК 27005–2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» [31].

4. ГОСТ Р ИСО/МЭК ТО 13335–5–2006 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по менеджменту безопасности сети» [57] (идентичный ISO/IEC TR 13335–5:2001) представляет собой руководство по управлению безопасностью сетей для персонала, ответственного за эту деятельность, и содержит основные положения по выявлению и анализу факторов, имеющих от-

ношение к компонентам безопасности связи и учитываемых при установлении требований по безопасности сети и указании потенциальных средств управления. Отмечается, что для идентификации требований по ОИБ для сетей и соответствующих средств управления (их детальное проектирование и техническая реализация не рассматриваются) необходимо решить следующие задачи, каждой из которых посвящен отдельный раздел стандарта:

- анализ общих требований по ОИБ сетевых соединений, изложенных в ПолИБ организации;
- анализ сетевой структуры с сетевыми соединениями и ее применения как необходимой основы для выполнения последующих задач;
- идентификация типа (ов) рассматриваемых сетевых соединений;
- анализ характеристик предложенного объединения в сеть (используя при необходимости имеющуюся информацию о применении структуры сети) и связанные с этим доверительные отношения;
- определение видов рисков ИБ, если это возможно, с помощью анализа рисков и управления результатами проведенного анализа, включая оценки бизнес-операций и информацию, которую предполагается передавать через соединения, и любую другую информацию, потенциально доступную для несанкционированного получения через эти соединения;
- идентификация возможных средств управления, которые могут быть использованы, на основе анализа типа (ов) соединения и характеристик организации сети и связанных с этим доверительных отношений, а также видов установленных рисков ИБ;
- разработка документации и анализ вариантов структуры ОИБ;
- распределение задач по детальному выбору защитных мер, проектированию, реализации и их обслуживанию, используя идентифицированные возможные средства управления и согласованную структуру ОИБ.

2.2.2. ISO/IEC 15408 и ISO/IEC 18045:2008 – ОБЩИЕ КРИТЕРИИ И МЕТОДОЛОГИЯ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Состоящий из трех частей стандарт ISO/IEC 15408 «The Common Criteria for Information Technology Security Evaluation» (Общие критерии оценки безопасности ИТ) [58–60], в создании которого участвовали США, Канада, Великобритания, Франция, Германия, Нидерланды, – один из наиболее распространенных международных стандартов в области ИБ, в котором подробно рассмотрены общие подходы, методы и функции обеспечения защиты информации программно-технического

уровня в организациях. Его первая версия вышла в 1999 г., действующая в настоящее время – в 2008–2009 гг. (в зависимости от части).

Стандарт был создан для взаимного признания результатов оценки безопасности ИТ в мировом масштабе. Он позволяет сравнить результаты независимых оценок ИБ и допустимых рисков на основе множества общих требований к функциям безопасности средств и систем ИТ, а также гарантий, применяемых к ним в процессе тестирования.

Функции обеспечения безопасности ИТ, которых выделено в стандарте 11 классов (аудит, идентификация и аутентификация, криптографическая защита, конфиденциальность, передача данных, защита пользовательских данных, управление безопасностью, защита функций безопасности системы, использование ресурсов, доступ к системе, надежность средств), представлены в виде четырехуровневой иерархической структуры: класс – семейство – компонент – элемент. Оценка безопасности ИТ базируется на моделях системы безопасности, состоящих из перечисленных функций. В стандарте содержится ряд предопределенных моделей (профилей защиты), описывающих стандартные модули системы безопасности, например системы управления базами данных (СУБД) или межсетевого экрана (МЭ). Для профиля защиты определяются следующие характеристики: область применения; уровень надежности; статус сертификации. Сертифицированный профиль представляет собой полное описание определенной части (или функции) системы безопасности. В нем содержится анализ внутренней и внешней среды объекта, требования к его функциональности и надежности, логическое обоснование его использования, возможности и ограничения развития объекта. Также вводятся два основных вида требований безопасности: функциональные, предъявляемые к функциям безопасности и реализующим их механизмам, и требования доверия, предъявляемые к технологии и процессу разработки и эксплуатации. Требования безопасности объекта оценки определяются исходя из целей безопасности, которые, в свою очередь, основываются на анализе назначения объекта оценки и условий среды его использования (угроз, предположений, политики безопасности).

Отличаясь значительной полнотой, универсализмом и большим потенциалом развития, стандарт ISO/IEC 15408 получил признание во многих странах мира, в том числе и в России. Стандарт ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» также состоит из трех частей:

1. ГОСТ Р ИСО/МЭК 15408–1–2008 «Информационная технология. Методы и средства обеспечения безопасности. Введение и общая модель» (идентичный ISO/IEC 15408–1:2005) устанавливает общий подход к формированию требований к оценке безопасности, основные конструкции (профиль защиты, задание по безопасности) представления тре-

бований безопасности в интересах потребителей, разработчиков и оценщиков продуктов и систем ИТ [61].

2. ГОСТ Р ИСО/МЭК 15408–2–2008 «Информационная технология. Методы и средства обеспечения безопасности. Функциональные требования безопасности» (идентичный ISO/IEC 15408–2:2005) содержит универсальный систематизированный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определенным правилам [62].

3. ГОСТ Р ИСО/МЭК 15408–3–2008 «Информационная технология. Методы и средства обеспечения безопасности. Требования доверия к безопасности» (идентичный ISO/IEC 15408–3:2005) включает в себя систематизированный каталог требований доверия, определяющих меры, которые должны быть приняты на всех этапах жизненного цикла продукта или системы ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям. Здесь же содержатся оценочные уровни доверия, определяющие шкалу требований, которые позволяют с возрастающей степенью полноты и строгости оценить проектную, тестовую и эксплуатационную документацию, правильность реализации функций безопасности объекта оценки, уязвимости продукта или системы ИТ, стойкость механизмов защиты и сделать заключение об уровне доверия к безопасности объекта оценки [63].

Второй стандарт по данной тематике – это международный стандарт ISO/IEC 18045:2008 «Information technology. Security techniques. Methodology for IT security evaluation» [64] и идентичный ему ГОСТ Р ИСО/МЭК 18045–2008 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий» [65]. Он представляет собой нормативный документ, применяемый совместно с ГОСТ Р ИСО/МЭК 15408. ГОСТ Р ИСО/МЭК 18045–2008 описывает минимум действий, выполняемых оценщиком и органом сертификации, подтверждающим действия оценщика, при проведении оценки безопасности ИТ по ИСО/МЭК 15408 с использованием критериев и свидетельств оценки, определенных в ИСО/МЭК 15408. Стандарт также предназначен для заявителей оценки, разработчиков, авторов профилей защиты и заданий по безопасности и другим сторонам, заинтересованным в безопасности ИТ.

2.2.3. ISO 19011:2011 и ГОСТ Р ИСО 19011–2003 – РЕКОМЕНДАЦИИ ПО АУДИТУ СИСТЕМ МЕНЕДЖМЕНТА

Международные стандарты ISO серий 9000 (качество) и 14000 (экология, окружающая среда) придают особое значение аудитам в составе деятельности, относящейся к менеджменту, обеспечивающим проверку результативности внедрения политики организации в области менеджмента качества и/или окружающей среды (последние системы иногда

называются системами экологического менеджмента). Аудиты являются важной составляющей деятельности по оценке соответствия при сертификации/регистрации, оценке провайдеров, инспекционном контроле.

В конце 2011 г. вышла вторая редакция стандарта ISO 19011:2011 «Guidelines for auditing management systems» (Руководство по аудиту систем менеджмента) [66]. По сравнению с первой редакцией, опубликованной в 2002 г. и применявшейся только к стандартам ISO 9001 и ISO 14001, область применения ISO 19011:2011 расширилась и отразила современные точки зрения на проведение внешних и внутренних аудитов в соответствии с существующими многочисленными стандартами на системы менеджмента. Особое внимание уделено разработке, реализации и управлению программой аудита – при строгом соблюдении рекомендаций будут обеспечены все необходимые предпосылки для того, чтобы сделать аудит важнейшим инструментом достижения бизнес-целей организации. В ISO 19011:2011 было добавлено понятие риска и в явной форме установлены требования к компетентности команды аудиторов и отдельных аудиторов. Также признана важность применения технологий при удаленном аудите, например, проведении удаленных интервью и просмотре документации. Другое важное улучшение – более четкое описание разницы между стандартами ISO 19011:2011 и ISO/IEC 17021:2011.

Идентичный первой редакции ISO 19011:2002 российский стандарт ГОСТ Р ИСО 19011–2003 «Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента» [67] содержат руководящие указания по принципам аудита, управлению программами аудита, проведению аудитов названных систем менеджмента, по управлению программами аудита, проведению внутренних или внешних аудитов таких систем менеджмента, а также по компетентности и оценке аудиторов (экспертов). Он предназначен для потенциальных пользователей, включая аудиторов (экспертов); организаций, внедряющих системы менеджмента качества и/или окружающей среды; организаций, в которых необходимо провести аудиты таких систем менеджмента согласно договорам организаций, участвующих в сертификации или в обучении аудиторов (экспертов), а также для использования при сертификации/регистрации систем менеджмента; аккредитации или стандартизации в области оценки соответствия.

В разделе стандарта по управлению программой аудитов рассматриваются следующие вопросы: определение цели программы аудитов; определение объема программы аудитов; ответственность, ресурсы и процедуры программы аудитов; внедрение программы аудитов (информирование заинтересованных сторон, координация и подготовка графика аудитов, квалификация аудиторов и выбор аудиторских групп, предоставление необходимых ресурсов, поддержание протоколов (регистрационных записей); мониторинг и анализ программы аудитов.

Для процесса проведения аудитов в стандарте отдельно описываются следующие подпроцессы: инициализация аудита (назначение ведущего аудитора группы, определение целей, критериев и объема аудита, оценка осуществимости аудита, выбор аудиторской группы и установление начальных контактов); подготовка к аудиту (предварительный анализ документации, подготовка плана аудита и распределение обязанностей в группе, подготовка рабочих документов); проведение аудита на месте (вступительное совещание, общение в ходе аудита, сопровождающие и наблюдатели, сбор и проверка информации, выработка наблюдений аудита, подготовка заключений по результатам аудита, заключительное совещание); подготовка, утверждение и распространение отчета по аудиту; завершение аудита; проведение последующих действий.

При рассмотрении квалификации и оценки аудиторов выделяются следующие важные моменты: личные качества; знания и умения, включая способность применять их на практике; поддержание и повышение квалификации; оценка аудиторов.

В многочисленных приложениях к стандарту приведены следующие формы и указания по их заполнению: график проведения аудитов, отчет об анализе программы аудита, опросный лист, отчет о несоответствии, паспорт аудитора, план аудита, отчет по аудиту, журнал регистрации отчетов о несоответствии, журнал регистрации планов аудита, журнал регистрации графиков аудитов.

При совместном внедрении систем менеджмента (качества и окружающей среды) пользователь стандарта сам решает вопрос о проведении раздельных аудитов или комплексного аудита.

Указания стандарта являются гибкими. Их использование может быть различным в зависимости от размера, вида деятельности, сложности проверяемых организаций, а также целей и области аудита. В выделенных рамках представлены дополнительные указания или примеры по конкретным вопросам в виде практических рекомендаций.

Основным достоинством ГОСТ Р ИСО 19011–2003 является возможность применения или распространения данных руководящих указаний на другие виды аудитов, включая аудиты других систем менеджмента (например, как внутренний, так и внешний аудит СУИБ). Стандарт содержит общие указания, которые могут быть использованы для разработки собственных для какой-либо организации требований, связанных с аудитом.

2.2.4. BS 25999 и ГОСТ Р 53647 – УПРАВЛЕНИЕ НЕПРЕРЫВНОСТЬЮ БИЗНЕСА

ОНБ в случае глобального инцидента или локального сбоя является одним из основных требований к организации в рамках эксплуатации СУИБ.

Британские стандарты серии BS 25999 – первые, посвященные УНБ. Они были разработаны на основе передового опыта в данной области

большой группой специалистов-практиков мирового класса, в которую вошли представители разных отраслей и государств.

В серию BS 25999 входят два стандарта:

BS 25999–1:2006 «Business continuity management. Code of practice» (УНБ. Практические правила) [68] определяет процесс, принципы и терминологию в области УНБ, закладывая основы для понимания, разработки и внедрения системы УНБ в организации и поддержания уверенности в ее надежности со стороны клиентов и партнеров. Этот стандарт в десяти разделах описывает всеобъемлющий набор средств управления и охватывает весь жизненный цикл процесса УНБ, начиная со стратегии ОНБ и заканчивая учетом данных вопросов в культуре организации.

BS 25999–2:2007 «Business continuity management. Specification» (УНБ. Спецификация) [69].

В то время как BS 25999–1:2006 содержит общие рекомендации по УНБ, вторая часть устанавливает и детализирует конкретные требования к СУНБ, причем только те, соблюдение которых может быть объективно проверено. Используя эти требования, организации могут проводить оценку существующей СУНБ как самостоятельно, так и привлекая внешних консультантов. На основании именно второй части стандарта сертификационные органы выдают заключение о соответствии СУНБ требованиям стандарта BS 25999.

Среди национальных стандартов Великобритании также есть еще два, посвященных вопросам ОНБ:

1) BIP 2142:2007 «The Route Map to Business Continuity Management: Meeting the requirements of BS 25999» (Маршрутная карта менеджмента непрерывности бизнеса. Внедрение требований BS 25999).

2) BIP 2151:2008 «Auditing Business Continuity Management Plans» (Аудит планов в области непрерывности бизнеса).

В 2009 г. в России на основе британских стандартов вышли три документа:

1) ГОСТ Р 53647.1–2009 «Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство» [70] (идентичный BS 25999-1:2006).

2) ГОСТ Р 53647.2–2009 «Менеджмент непрерывности бизнеса. Часть 2. Требования» [71] (идентичный BS 25999–2:2007).

3) ГОСТ Р 53647.3–2010 «Менеджмент непрерывности бизнеса. Часть 3. Руководство по внедрению» [72] (разработан с учетом основных требований BIP 2142:2007).

В названных стандартах под УНБ принято понимать целостный процесс управления, в ходе которого выявляются потенциальные угрозы и определяются возможные последствия в случае их осуществления для организации, а также создается основа обеспечения способности организации восстанавливаться и эффективно реагировать на инциденты.

Такой подход гарантирует соблюдение интересов основных причастных сторон, сохранение репутации и дальнейшего функционирования организации в целом. УНБ включает управление восстановлением и продолжением деятельности в случае нарушения нормального хода бизнеса, а также управление общей программой УНБ посредством проведения обучения и повышения осведомленности персонала, а также анализа с целью поддержания плана (ов) ОНБ в актуальном состоянии.

Стандарты ГОСТ Р 53647, направленные на минимизацию рисков возникновения инцидентов и снижение потерь от сбоев в работе, дают четкие критерии и рекомендации по построению СУНБ и направлены на поддержание бесперебойной деятельности организации в самых сложных и неожиданных обстоятельствах. На базе изложенных требований можно построить процесс УНБ для целей обеспечения непрерывности ключевых бизнес-процессов в рамках области действия СУИБ.

Стандарты ГОСТ Р 53647 подходят для любой организации, независимо от размера и области деятельности. Они имеют особое значение для организаций, работающих в среде с высокой степенью риска, например в области финансов, телекоммуникаций, транспорта и в государственном секторе. Здесь возможность обеспечения непрерывной деятельности имеет первостепенное значение как для самой организации, так и для ее клиентов и заинтересованных сторон.

2.3. Отраслевые стандарты в области управления ИБ – стандарты банковской системы Российской Федерации

Для организаций банковской сферы задача ОИБ является одним из важных требований бизнеса, поскольку являясь объектом пристального внимания злоумышленников, банки ежедневно сталкиваются с инцидентами ИБ. Развитие и укрепление банковской системы (БС) Российской Федерации (РФ), включающей в себя Банк России, кредитные организации и филиалы и представительства иностранных банков, а также обеспечение эффективного и бесперебойного функционирования платежной системы РФ являются целями деятельности Банка России. Важнейшее условие реализации этих целей – обеспечение необходимого и достаточного уровня ИБ организаций БС РФ, включая их активы (в том числе информационные), который во многом определяется уровнем ИБ банковских технологических процессов – платежных, информационных и прочих, автоматизированных банковских систем (АБС), эксплуатирующихся организациями БС РФ, и т. д. Негативные последствия сбоев в работе отдельных организаций могут привести к быстрому развитию системного кризиса всей платежной системы РФ, нанести ущерб интересам ее собственников и клиентов. Поэтому для организаций БС РФ угрозы ИБ информационным активам и их реализация в виде инцидентов ИБ представляют реальную опасность. Для противостояния таким угрозам и обеспечения эффективности мероприятий по ликвидации не-

благоприятных последствий инцидентов ИБ (их влияния на операционные, кредитные и иные риски) в организациях БС РФ следует обеспечить достаточный уровень ИБ, который необходимо сохранить в течение длительного времени. По этим причинам ОИБ является для организаций БС РФ одним из основополагающих аспектов их деятельности [11].

Деятельность, относящаяся к ОИБ в организациях БС РФ, должна контролироваться за счет регулярного проведения оценки уровня ИБ, рисков ИБ и принятия мер, необходимых для управления этими рисками. Для этих целей был разработан комплекс документов, положенный в основу стандартизации обеспечения и управления ИБ для организаций БС РФ. Основные цели такой стандартизации [11]:

- повышение доверия к БС РФ;
- повышение стабильности функционирования организаций БС РФ и на этой основе – стабильности функционирования БС РФ в целом;
- достижение адекватности мер по защите от реальных угроз ИБ;
- предотвращение и/или снижение ущерба от инцидентов ИБ.

Основные задачи стандартизации по ОИБ организаций БС РФ:

- установление для них единых требований по ОИБ;
- повышение эффективности мероприятий по обеспечению и поддержанию ИБ организаций.

Комплекс документов по обеспечению и управлению ИБ организаций БС РФ состоит из отраслевых стандартов (СТО) и рекомендаций в области стандартизации (РС) (рис. 2.2). Уже разработаны следующие документы комплекса:

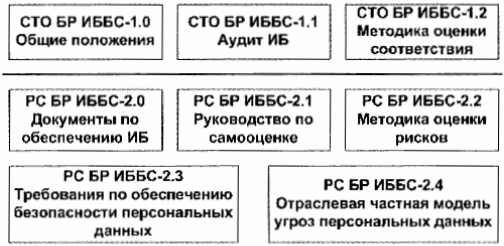

Рис. 2.2. Комплекс документов по ОИБ для организаций БС РФ

Стандарт Банка России СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» [11] – четвертая редакция введена в действие с 21 июня 2010 г.

Стандарт Банка России СТО БР ИББС-1.1 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности» [73] – первая редакция введена в действие с 1 мая 2007 г.

Стандарт Банка России СТО БР ИББС-1.2 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций БС РФ требованиям СТО БР ИББС-1.0» [74] – третья редакция введена в действие с 21 июня 2010 г.

Рекомендации в области стандартизации Банка России РС БР ИББС-2.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0» [75] – первая редакция введена в действие с 1 мая 2007 г.

Рекомендации в области стандартизации Банка России РС БР ИББС-2.1 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций БС РФ требованиям СТО БР ИББС-1.0» [76] – первая редакция введена в действие с 1 мая 2007 г.

Рекомендации в области стандартизации Банка России РС БР ИББС-2.2 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности» [77] – первая редакция введена в действие с 1 января 2010 г.

Рекомендации в области стандартизации Банка России РС БР ИББС-2.3. «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций БС РФ» [78] – первая редакция введена в действие с 21 июня 2010 г.

Рекомендации в области стандартизации Банка России РС БР ИББС-2.4. «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций БС РФ» [79] – первая редакция введена в действие с 21 июня 2010 г.

2.3.1. СТО БР ИББС-1.0 – ОБЩИЕ ПОЛОЖЕНИЯ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИБ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Стандарт СТО БР ИББС-1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» является базовым для развивающей и обеспечивающей его группы СТО и РС. С момента выхода в 2004 г. первой редакции стандарт претерпел ряд изменений и постоянно обновляется по результатам его применения. В настоящее время действует четвертая редакция стандарта.

В СТО БР ИББС-1.0–2010 СМИБ определяется как часть менеджмента организации БС РФ, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения ИБ (СОИБ). СОИБ организации БС РФ – это совокупность ее СМИБ и системы ИБ (СИБ). СИБ, в свою очередь, это совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение [11].

Процессы СМИБ сгруппированы в виде циклической модели PDCA: «*планирование – реализация – проверка – совершенствование*».

В стандарте отмечается, что для успешного функционирования СМИБ в организации БС РФ следует выполнить требования по следующим видам деятельности:

- организация и функционирование службы ИБ организации;
- определение/коррекция области действия СОИБ;
- выбор/коррекция подхода к оценке рисков нарушения ИБ и проведение оценки таких рисков;
- разработка планов обработки рисков нарушения ИБ и организация реализации этих планов;
- разработка/коррекция внутренних документов, регламентирующих деятельность в области ОИБ;
- принятие руководством организации решений о реализации и эксплуатации СОИБ;
- разработка и организация реализации программ по обучению и повышению осведомленности в области ИБ;
- организация обнаружения и реагирования на инциденты ИБ;
- организация ОНБ и его восстановления после прерываний;
- проверка и оценка ИБ организаций путем выполнения следующих процессов: мониторинг и контроль защитных мер, проведение аудита и самооценки ИБ, анализ функционирования СОИБ (в том числе со стороны руководства организации);
- принятие решений по стратегическим и тактическим улучшениям СОИБ.

2.3.2. СТО БР ИББС-1.1 – АУДИТ ИБ

СТО БР ИББС-1.1 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности» распространяется на организации БС РФ, а также на организации, проводящие аудит ИБ организации БС РФ, и устанавливает требования к проведению внешнего аудита ИБ организаций БС РФ [73].

Одним из условий реализации целей деятельности организаций БС РФ является обеспечение необходимого и достаточного уровня их ИБ. Уровень ИБ считается высоким, если процессы СОИБ проводятся осознанно на основе прогноза, мониторинга и анализа внутренней и внеш-

ней среды, развития и изменения целей бизнеса (деятельности) организации. Основным из видов проверки уровня ИБ является аудит ИБ – систематический, независимый и документируемый процесс получения свидетельств аудита деятельности организации по ОИБ и установления степени выполнения в организации установленных критериев аудита ИБ, проводимый внешней по отношению к проверяемой независимой проверяющей организацией. Оценка соответствия ИБ критериям аудита ИБ проводится на основе документов по ОИБ и фактов, свидетельствующих о выполнении, частичном выполнении или невыполнении установленных требований по ОИБ.

Основными целями аудита ИБ как важнейшего процесса в непрерывном цикле процессов менеджмента ИБ организации являются:

- повышение доверия к этим организациям;
- оценка соответствия ИБ организаций критериям аудита ИБ, установленным согласно требованиям СТО БР ИББС-1.0.

Данный стандарт провозглашает основные принципы проведения аудита ИБ организаций БС РФ, такие как независимость аудита ИБ, полнота аудита ИБ, оценка на основе свидетельств аудита ИБ, достоверность свидетельств аудита ИБ, компетентность и этичность поведения. Однако данные принципы применимы при проведении аудита ИБ любых других организаций.

В СТО БР ИББС-1.1–2007 рассматривается целый ряд требований:

- к менеджменту программами аудита ИБ;
- к взаимоотношениям представителей аудиторской организации с представителями проверяемой организации, включая их обязанности и ответственность;
- к этапам проведения аудита ИБ организаций БС РФ: подготовке к проведению аудита ИБ; анализу документов; проведению аудита ИБ на месте; подготовке, утверждению и рассылке отчета по аудиту ИБ; завершению аудита ИБ.

Программа аудита ИБ включает деятельность, необходимую для планирования и организации определенного количества аудитов ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения аудитов ИБ в заданные сроки. Последовательность процессов менеджмента программы аудита ИБ (после распределение полномочий) соответствует циклической модели PDCA и включает в себя следующие процессы:

- разработка программы аудита ИБ;
- внедрение программы аудита ИБ и деятельность по проведению аудита ИБ;
- контроль и анализ программы аудита ИБ;
- совершенствование программы аудита ИБ.

Согласно стандарту хорошей практикой проверки уровня ИБ и подготовки к аудиту ИБ организации БС РФ является самооценка ИБ, которая проводится на основе принятых в организации документов и методик.

Как было отмечено выше, СТО БР ИББС-1.1 устанавливает требования к проведению внешнего аудита ИБ организаций БС РФ. Однако почти все приведенные положения и требования стандарта могут быть применены в организациях, работающих в других отраслях, с минимальными изменениями.

2.3.3. СТО БР ИББС-1.2 – МЕТОДИКА ОЦЕНКИ СООТВЕТСТВИЯ ИБ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ ТРЕБОВАНИЯМ СТО БР ИББС-1.0

Стандартом СТО БР ИББС-1.0 с целью проверки уровня ИБ как самого Банка России, так и организаций БС РФ определено требование проведения регулярной внешней и внутренней оценки ИБ, а также самооценки ИБ. Стандарт СТО БР ИББС-1.2–2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций БС РФ требованиям СТО БР ИББС-1.0» устанавливает способы определения степени выполнения и итогового уровня соответствия ИБ указанным требованиям при проведении внутренней и/или внешней оценки и самооценки ИБ [74].

Целью данной методики является стандартизация подходов и способов оценки, используемых для определения уровня соответствия ИБ организации БС РФ требованиям СТО БР ИББС-1.0 по трем направлениям оценки:

1) текущий уровень ИБ организации;
2) менеджмент ИБ организации;
3) уровень осознания ИБ организации.

Для этого определяется состав показателей ИБ и способы их оценивания.

Используются групповые и частные показатели ИБ. Групповые показатели ИБ образуют структуру направлений оценки, детализируя оценки по ним. Оценки групповых показателей используются для получения оценки по направлениям. Частные показатели ИБ входят в состав групповых показателей и представлены в виде вопросов, ответы на которые дают возможность определить оценки, которые затем формируют оценки групповых показателей.

Частные показатели разделены на две категории: выполнение которых обязательно и рекомендовано в организации. Также установлены критерии выставления оценок частных показателей ИБ, в которых оценивается степень документированности и/или выполнения требований по ОИБ.

В методике представлены формы, предназначенные для заполнения при проведении оценки. Каждая из форм содержит групповой показатель ИБ, входящие в него частные показатели ИБ, обязательность их выполнения, метрику (шкалу) для оценивания частных показателей и коэффициенты значимости частных показателей ИБ, используемые при вычислении показателя ИБ.

Оценка частного показателя ИБ должна основываться на свидетельствах аудита, в качестве основных источников которых рекомендуется использовать:

- внутренние нормативные документы проверяемой организации и при необходимости документы третьих лиц, относящиеся к ОИБ организации БС РФ;
- устные высказывания сотрудников проверяемой организации в процессе проводимых опросов;
- результаты наблюдений членов аудиторской группы за деятельностью сотрудников проверяемой организации в области ИБ.

Оценка группового показателя (за исключением группового показателя М9 «Общие требования по обработке персональных данных в организации БС РФ») вычисляется из оценок входящих в него частных показателей с учетом некоторых коэффициентов значимости, определяющих важность частного показателя для оценивания группового показателя.

В СТО БР ИББС-1.2 также представлен вид наглядного отображения получившихся результатов оценивания (оценок) в виде круговой диаграммы с уровнями соответствия требованиям СТО БО ИББС-1.0 с 0-го по 5-й по трем направлениям оценки.

Выводы

В данной главе были рассмотрены основные существующие стандарты в области управления ИБ. Их можно условно разделить на два типа – стандарты, регламентирующие процессы построения, внедрения, эксплуатации, мониторинга, анализа, постоянного улучшения СУИБ в целом, а также стандарты, регламентирующие отдельные процессы управления ИБ.

Все рассмотренные стандарты являются рекомендательными, и, следовательно, выполнение их требований не обязательно, если перед организацией не стоит задача сертификации своей СУИБ.

Поскольку большая часть рассмотренных стандартов является международной, можно сделать вывод о том, что их готовили группы международных специалистов, обладающих опытом и компетенцией в различных аспектах ИБ. Все это делает стандарты привлекательными для использования в качестве «лучших практик» по управлению ИБ.

Вопросы для самоконтроля

1. Какой стандарт (серия стандартов) стал основоположником стандартизации систем управления ИБ?
2. Для организаций какой сферы применимы стандарты серии ISO/IEC 27000?
3. Каковы отличительные черты серии стандартов ISO/IEC 27000?
4. Какой из стандартов серии ISO/IEC 27000 содержит требования к созданию, внедрению, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ?
5. В чем состоят основные различия и сходства стандартов ISO/IEC 27001 и ITU-T X.1051?
6. Какой из стандартов серии ISO/IEC 27000 признан каталогом «лучших» практик по ИБ?
7. В каком стандарте серии ISO/IEC 27000 содержится руководство по внедрению СУИБ?
8. На основании чего может проводиться оценка эффективности СУИБ?
9. Можно ли проводить аудит (или сертификацию) на соответствие стандарту ISO/IEC 27002 (бывший ISO/IEC 17799)?
10. Каковы основные идеи руководства по аудиту СУИБ и средств управления ИБ, реализованных в СУИБ?
11. Почему подход к проведению аудитов систем менеджмента качества и окружающей среды, изложенный в стандарте ISO/IEC 19011, может быть применен для проведения внутренних аудитов СУИБ?
12. В каком стандарте серии ISO/IEC 27000 описана инфраструктура руководства ИБ?
13. Какой стандарт серии ISO/IEC 27000 рассматривает вопросы управления безопасностью сетей?
14. В чем состоят преимущества использования (учета) требований российских и международных стандартов по управлению ИБ при построении СУИБ или отдельных процессов управления ИБ?
15. Каковы преимущества одновременного учета требований стандартов, предъявляемых как к СУИБ в целом, так и стандартов, предъявляющих требования к отдельным процессам, разрабатываемым в рамках СУИБ?
16. В чем состоят основные сходства и различия между стандартами на СУИБ и на отдельные процессы управления ИБ?
17. Какие методы и средства ОИБ для ИТ рассматриваются в стандартах ISO/IEC 13335 и идентичных им ГОСТ Р ИСО/МЭК 13335?
18. Как оценивается ИБ ИТ согласно стандартам ISO/IEC 15408 и 18045 и идентичных им ГОСТ Р ИСО/МЭК?
19. Какие из рассмотренных стандартов затрагивают аспекты анализа рисков ИБ?
20. Каковы основные цели построения системы УНБ, соответствующей требованиям стандартов BS 25999 и 25777?
21. В чем может заключаться различие между требованиями к системам управления непрерывностью бизнеса и к процессу управления непрерывностью бизнеса?
22. Каковы основные цели следования модели PDCA при построении процесса управления инцидентами ИБ в соответствии с требованиями ГОСТ Р ИСО/МЭК ТО 18044?

23. Какие тенденции характерны для развития стандартизации управления ИБ в Российской Федерации?
24. В чем состоят преимущества использования «отраслевых» стандартов на СУИБ по сравнению, например, со стандартом ISO/IEC 27001, требования которого применимы к любой организации независимо от отрасли или сферы деятельности?
25. Каково значение стандартов серии СТО БР ИББС в рамках развития стандартизации управления ИБ в России?
26. Какие аспекты регламентируют стандарты серии СТО БР ИББС, если говорить об управлении ИБ?
27. Каковы основные цели и задачи стандартизации по ОИБ организаций БС РФ?
28. Каковы основные цели проведения аудита ИБ организаций БС РФ?
29. На основе какой методики рекомендуется проводить оценку соответствия уровня ИБ организации БС РФ требованиям стандарта СТО БР ИББС-1.0?