Сергей ВИХОРЕВ/
директор аналитического
департамента ОАО «Элвис-плюс»/

Политика обеспечения безопасности

Эссе о лингвистике, политике и безопасности информации

Часть первая, лингвистическая, в защиту русского языка

Но панталоны, фрак, жилет,
Всех этих слов на русском нет…
А. С. Пушкин. Евгений Онегин, гл. 1
Беда, коль пироги начнет печи сапожник,
А сапоги тачать пирожник…
И. А. Крылов. Басня «Щука и кот»

Политика! Как много в этом слове… В последнее время, время современных компьютерных технологий, время, когда неизбежно возникает вопрос о защищенности информационных систем от угроз безопасности информации, время, когда необходимо принимать взвешенные решения по устранению этих угроз, многие начинают задумываться о соответствии своего бизнеса международным требованиям по информационной безопасности. И вот тут-то от аудиторов серьезных международных (да и не только международных) консалтинговых компаний нередко приходится слышать: «А у вас есть политика информационной безопасности?» И как следствие этого нетривиального вопроса, следует «накачка» CIO: «Как, у нас до сих пор нет политики?» — а потом обращение к консультантам с просьбой подготовить такой документ, как «Политика ИБ». Такой сюжет не выдумка, думаю, многие компании, занимающиеся консалтингом в области ИБ, могут подтвердить, что к ним обращались с такими просьбами. Но прежде чем определить, насколько эта задача реализуема, попытаемся для начала, с лингвистической точки зрения, разобраться, что же такое политика вообще и политика ИБ в частности.

Разные словари дают немного разные, практически схожие определения слова «политика». Наиболее полным из них является определение Словаря русского языка С. И. Ожегова: «Политика, -и, ж. 1. Деятельность органов государственной власти и государственного управления, отражающая общественный строй и экономическую структуру страны, а также деятельность общественных классов, партий и других классовых организаций, общественных группировок, определяемая их интересами и целями. 2. Вопросы и события общественной, государственной жизни. 3. Об-

Конечно же, это эссе посвящено безопасности информации, точнее, проблеме организации обеспечения безопасности информации, но прежде все-таки хотелось бы немного поговорить о лингвистике. Надо сразу оговориться — автор не лингвист и не претендует на это звание, но высказывает свою точку зрения.

раз действий, направленных на достижение чего-нибудь, определяющих отношения с людьми (разг.)»*. Из этих определений можно сделать несколько очень важных выводов.

Во-первых, «политика», судя даже по корню слова**, это то, что относится к компетенции государства. Поэтому применимость такого термина в масштабах одной, даже очень крупной организации выглядит немного натянуто (если, конечно не использовать его разговорного значения).

Во-вторых, «политика» — это некая деятельность (или образ действий), направленная на достижение каких-либо целей. Вот и получается, что политику можно претворять в жизнь, реализовывать, но политику нельзя написать! Более того, никакой, в том числе самый совершенный автомат (или компьютер) не сможет реализовать даже самую лучшую политику, он может только выполнить те установки и настройки, которые ему заложит человек, то есть компьютер может только поддерживать правила безопасности, которые соответствуют определенному образу действий, то есть политике.

Таким образом, политика по своей сути является целенаправленной деятельностью людей в соответствии с правилами, установленными для достижения какого-то результата. И для того чтобы эту политику реализовывать, надо четко представлять пути достижения поставленной цели и договориться о правилах, по которым необходимо действовать. К этому мы еще вернемся далее.

А теперь немного о другом. Откуда вообще появился в русском языке термин «политика ИБ»? Точно не знаю, но рискну предположить, что это результат «горя от ума». Информационными технологиями, как правило, занимаются грамотные специалисты, знакомые с иностранными языками, в том числе и с английским, но, при всем моем уважении к ним, они, к сожалению, не филологи и не лингвисты, а все-таки «технари», склонные довольно вольно обращаться с иностранными словами и использовать весьма специфический жаргон. Поэтому и проявляются у нас в литературе и разговорах «юзеры» вместо пользователей, «апгрейд» вместо модернизации, «хабы» вместо коммутаторов и пр. Иногда это оправдано и без таких заимствований не обойтись (вспомните, к примеру, «компьютер», «сервер»), но мера нужна во всем, а то получится этакая «смесь французского с нижегородским...».

Надо сказать, что англоязычное понятие «security policy» не новое и вообще-то широко используется в международной практике (например в международном стандарте ISO 17799, посвященном проблемам аудита управления информационной безопасностью). Не правда ли, оно очень созвучно с «политикой»? Вот и появляется соблазн перевести это слово именно так. Но английский язык все-таки достаточно полисемантичен, например, словарь Мюллера*** дает шесть (!) вариантов значения слова «policy». Среди них наряду с такими, как «линия поведения, установка, курс», «благоразумие, политичность; хитрость, ловкость» есть и «парк (вокруг

усадьбы)», «род азартной игры». Подобрать правильный и адекватный перевод иностранному слову, да еще и в такой достаточно новой предметной области, как информационная безопасность, сложно — каждый может трактовать понятие по-своему (к примеру, в состав рабочей группы по подготовке перевода стандарта ISO 15408 «Общие критерии» наряду с техническими специалистами входили как русские, так и английские лингвисты, и споры между ними были нередки. Кстати, в этой рабочей группе лингвисты все-таки пришли к единому мнению: «security policy» — a set of rules that regulate how assets are managed, protected and distributed within a target of evaluation, то есть: совокупность правил, регулирующих управление, защиту и распределение активов внутри объекта оценки).

Вот и получается, что в контексте проблемы информационной безопасности «policy» все-таки лучше переводить как «правила» (например, у Мюллера это слово переводится и как «страховой полис» — документ, который содержит условия страхования, читай правила страхования). Автор не

* Ожегов С. И. Словарь русского языка. Под ред. Н. Ю. Шведовой. 22-е изд. — М.: Рус. яз., 1990.
** Греч. politika — государственные или общественные дела, от polis — государство. (Энциклопедический словарь. Под ред. А. М. Прохорова. — М.: Советская энциклопедия, 1988.)
*** Мюллер В. К. Англо-русский словарь. — М.: Советская энциклопедия, 1969.

знает, кто первый ввел в оборот перевод «security policy» как «политика ИБ» и как он его трактовал (скорее всего, правильно), но сейчас в этот термин каждый вкладывает то, что считает нужным или выгодным.

Поэтому и назрела необходимость четко определить, что понимать под уже устоявшимся термином «политика» применительно к области обеспечения безопасности информации.

Англоязычное понятие «security policy» не новое и вообще-то широко используется в международной практике (например в международном стандарте ISO 17799, посвященном проблемам аудита управления информационной безопасностью). Не правда ли, оно очень созвучно с «политикой»?

Часть вторая, терминологическая, о сути политики безопасности информации

В начале было Слово, и Слово было у Бога, и Слово было Бог…
Все чрез Него начало быть…
Евангелие от Иоанна, гл. 1
А если я сказал к маме, значит — к маме…
Современная телереклама

Мировой и отечественный опыт свидетельствует о том, что современная система обеспечения безопасности информации строится как целостная система. Она становится эффективной тогда, когда увязывает разнообразные организационные и технические меры защиты, использует современные методы прогнозирования, анализа и моделирования постоянно меняющейся политической, социальной и экономической ситуации, учитывает лавинообразное развитие средств телекоммуникации, необходимость постоянного своего совершенствования и наращивания возможностей по защиты информации.

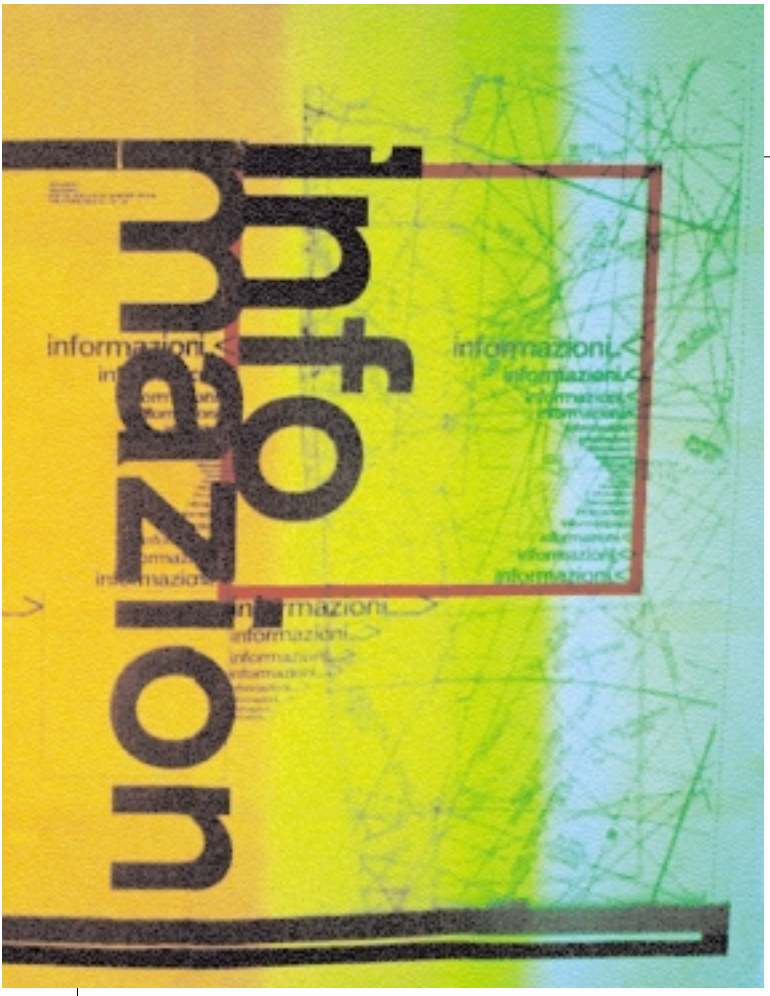
Создание такой системы требует усилий многих: от топ-менеджеров, принимающих стратегические решения, до системного администратора, осуществляющего техническую поддержку информационной системы и настройку ее отдельных элементов. Иными словами, необходимо уяснить, для чего нужно обеспечение безопасности информации, поставить перед собой и своим коллективом четкую цель, выработать систему взглядов на достижение поставленных целей и определить, как необходимо действовать каждому для достижения этих целей. И каждому надо объяснить, как и что надо делать, то есть сформулировать для них их обязанности по защите информации. Естественно, что такие правила должны быть понятными каждой категории, должны определять разные аспекты для тех, кто принимает решения, и тех, кто их исполняет, при этом они должны быть объединены одной стратегической линией, едиными долгосрочными подходами к комплексному решению задач обеспечения безопасности информации.

По всей вероятности, сформировать такие универсальные правила, которые были бы понятны всем, которые можно было бы использовать и при формировании бюджета на обеспечение безопасности информации, и при настройке межсетевого экрана — задача невыполнимая. Следовательно, сами эти правила превращаются в достаточно сложную иерархическую систему инструкций и регламентов, предназначенных для исполнения различными категориями лиц, задействованных в процессе обеспечения безопасности информации. Но когда эти самые правила будут неукоснительно исполняться всеми, когда их исполнение действительно станет повседневным образом действий каждого сотрудника независимо от его служебного положения, вот тогда можно будет говорить о том, что в организации сформирована и успешно реализуется «Политика обеспечения безопасности информации».

Таким образом получается, что термин «Политика обеспечения безопасности информации» (дальше для простоты будем говорить «политика безопасности информации») — собирательное понятие, представляющее собой совокупность взаимоувязанных нормативных документов, определяющих порядок обеспечения безопасности информации в конкретной организации, а также выдвигающих требования по поддержанию подобного порядка.

Особо хочется подчеркнуть, что интересы обеспечения безопасности информации всегда будут противоречить интересам сотрудников, так как они всегда со-

■ Рисунок. Структура и уровни политики обеспечения безопасности информации.



держат те или иные ограничения. И ожидать, что все сразу побегут выполнять предписанные им правила безопасности, вряд ли приходится. Процесс внедрения этих правил в умы сотрудников — кропотлив и требует определенной «силовой» или, вернее, «административной» поддержки. Поэтому все документы, разрабатываемые при формировании Политики безопасности информации, обязательно должны иметь официальный юридический статус (например, приняты в форме приказа по организации или утверждены главой организации). Это необходимо для того, чтобы они имели статус обязательных для исполнения всеми сотрудниками организации и позволяли, при необходимости, задействовать еще и репрессивные механизмы.

Итак, «отжав» все лирические и лингвистические отступления, можно считать, что Политика обеспечения безопасности информации представляет собой согласованный по целям защиты информации пакет нормативных, организационно-распорядительных и эксплуатационных документов, устанавливающих требования и порядок обеспечения безопасности информации, регламентирующих все вопросы организации, управления и контроля безопасности, а также эксплуатации средств защиты информации.

В принципе, говоря о политике безопасности информации, надо помнить, что здесь содержание превалирует над формой и по этой причине жесткой формы документов, входящих в пакет, — нет. Главное, чтобы «костюмчик сидел», то есть форма отражения тех или иных важных вопросов может быть любая, но, естественно, лучше, если эти вопросы как-то структурированы. В этом случае вероятность забыть и не сделать что-то важное будет меньше. Вот и попробуем провести такую структуризацию.

Часть третья, структурная, о том, какова же политика безопасности информации

…А молясь, не говорите лишнего, как язычники, ибо они думают, что в многословии своем будут услышаны…
Евангелие от Матфея, гл. 6

Структура пакета документов, способствующего формированию и реализации Политики безопасности информации, представляется в виде трех иерархических уровней. Каждый из таких уровней сам содержит совокупность нескольких документов, которые либо устанавливают некоторые принципы обеспечения безопасности, либо определяют, как эти принципы реализовать.

Первый уровень Политики безопасности информации состоит из двух основных документов. Первый — Стратегический замысел (или просто Стратегия) — документ самого высокого уровня. Как правило, такой документ не содержит сложных специфических технических терминов, незначителен по объему (всего 3–5 страниц), но очень важен по существу: он, с одной стороны, констатирует осознание руководителями важности проблемы безопасности информации, определяет общий замысел обеспечения безопасности и декларирует необходимость осуществления таких мероприятий. Как говорится, правильно поставленная задача — уже половина успеха. С другой стороны, он выступает своеобразным интерфейсом, устанавливающим взаимопонимание между «генералами от бизнеса», мыслящими категориями бизнеса, и «техническими исполнителями», непосредственно обеспечивающими безопасность информации. В этом же документе должны быть определены высшие руководители компании, ответственные за организацию безопасности информации, а также порядок финансирования работ по достижению и поддержанию требуемого уровня доверия к защите информации. Это главный, но не головной документ в решении нашей проблемы.

Головной же документ этого уровня — Концепция обеспечения безопасности информации (или просто Концепция) — важнейший, базовый, фактически системообразующий документ в общем пакете требований, определяющий стратегические, долгосрочные решения по организации информационной безопасности, интегрирующий все другие документы по поставленным целям и задачам. Приобретая, после утверждения руководством организации, юридическую силу, Концепция позволяет правильно организовать взаимодействие подразделений организации в вопросах обеспечения безопасности информации и распределить ответственность должностных лиц в решении этих вопросов.

Концепция — это достаточно емкий (до 50–60 страниц) документ, который формирует систему взглядов на проблему обеспечения безопасности информации в конкретной организации, определяет цели и задачи защиты информации в информационных системах, устанавливает корпоративные требования и практические правила управления безопасностью информации. Он устанавливает режим защиты информации, обязательный к исполнению не только внутри самой организации, но и всеми организациями и предприятиями, независимо от их подчиненности, так или иначе сталкивающимися, обрабатывающими, передающими или пользующимися информацией, собственником которой является организация. Все дальнейшие частные технические решения по развитию общей информационной и телекоммуникационной структуры организации и обеспечению ее безопасности должны опираться на выводы Концепции.

Разработке Концепции предшествует серьезный анализ общей стратегии развития бизнеса и перспектив развития, условий сложившегося информационного взаимодействия, современного состояния безопасности информации, возможных источников и видов угроз, динамики их развития, выбор класса защищенности, определение оптимального соотношения комплекса организационных, технических и программно-аппаратных методов защиты, изложение способов и практических рекомендаций по предотвращению несанкционированного доступа к информации, по защите информации от утечки по техническим каналам, планирование материальных затрат для обеспечения требуемого уровня доверия, адекватного стоимости информационных ресурсов, формирование облика системы обеспечения безопасности информации (СОБИ) и определение основных требований к ее подсистемам.

Таким образом, на первом уровне Политики безопасности формулируются цели обеспечения безопасности информации, которые в дальнейшем определяют правила и требования по всем вопросам безопасности информации и становятся обязательными для всех структурных подразделений организации.

Второй уровень Политики безопасности информации, как правило, содержит два документа — Регламент обеспечения без-

Для справки

ПОЛИТИКА *(греч. politika — государственные или общественные дела — от polis — государство)*, сфера деятельности, связанная с отношениями между социальными группами, сутью которой является определение форм, задач, содержания деятельности государства. Различают внешнюю и внутреннюю политику. Внутренняя политика охватывает основные направления деятельности государства, партий (экономическая, социальная, культурная, и др.). Внешняя политика охватывает сферу отношений между государствами.
Большой энциклопедический словарь

Policy I noun 1) политика; peace policy — политика мира, мирная политика; for reasons of policy — по политическим соображениям; tough policy — твердая политика 2) политика, линия поведения, установка, курс 3) благоразумие, политичность; хитрость, ловкость 4) scot. парк (вокруг усадьбы) Syn: see stand II noun 1) страховой полис 2) amer. род азартной игры.
Англо-русский словарь

> В Великобритании каждый час посылается более 1 млн. текстовых сообщений, поэтому издатели краткого словаря английского языка (Concise Oxford Dictionary) решили включить наиболее употребимые выражения, используемые в сообщениях, в новое издание, вышедшее в четверг.

> SMS, или краткие сообщения, помещены в специальный раздел. В разделе приводятся десятки примеров различных аббревиатур, которые стали частью языка среди молодых людей. Примеры включают BBLR (be back later) — буду позже, HAND (have a nice day) — хорошего дня. Также в словарь вошли смайлики — мимические обозначения эмоций, такие, как :) и :(. Среди новых слов — такие, как minger — неприятный человек, chowhand — жадина, tweenies — дети, пытающиеся выглядеть старше своих лет.

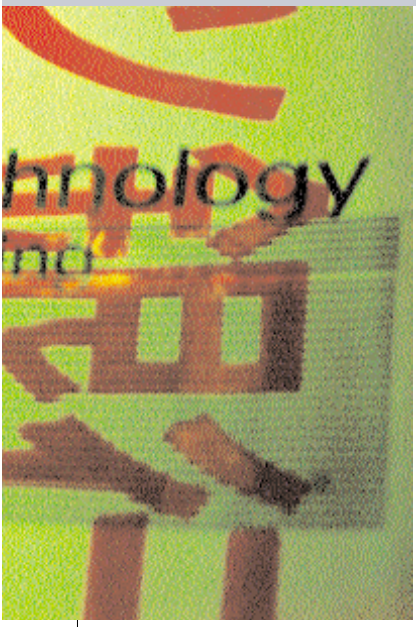
> Оксфордский словарь английского языка был пополнен. В него было внесено 125 новых слов, а толкования более тысячи слов были пересмотрены.

> Политика безопасности ОО (TOE Security Policy) — совокупность правил, регулирующих управление, защиту и распределение активов внутри ОО (A set of rules that regulate how assets are managed, protected and distributed within a TOE).

> ОО (TOE) — объект оценки (Target of Evaluation).

Разработка проекта Российского стандарта «Общие критерии оценки безопасности информационных технологий». Русский перевод основных англоязычных терминов и их определений из «Общих критериев». <

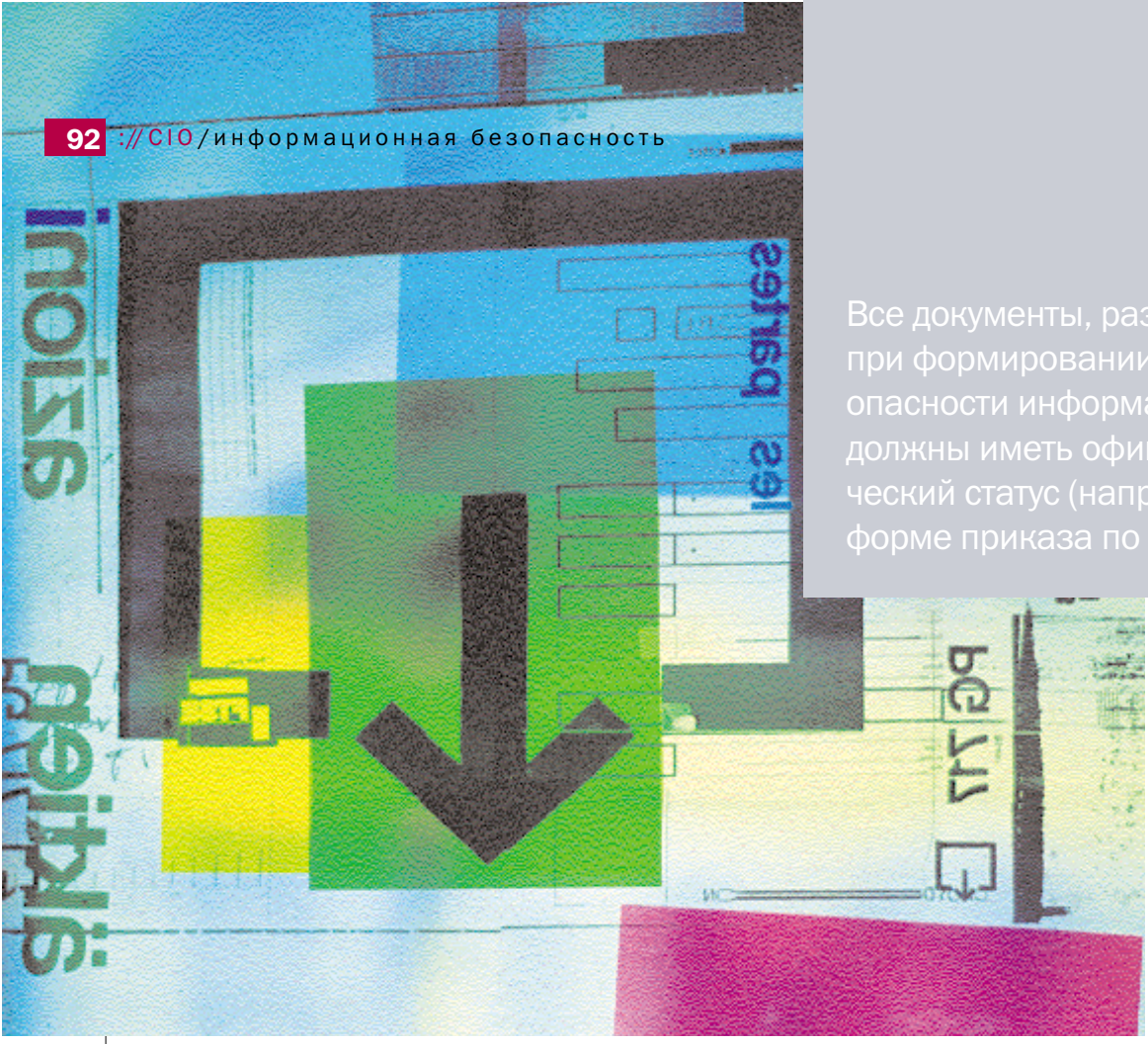
Концепция — важнейший, базовый, фактически системообразующий документ в общем пакете требований.



опасности информации (или просто Регламент) и Общие технические требования по обеспечению безопасности информации (ОТТ), которые по своей сути являются организационно-распорядительными документами, то есть регламентируют все вопросы организации и проведения работ по защите информации, положений об инфраструктурных элементах СОБИ, разрешительной системе допуска исполнителей к документам и сведениям, регламентам выполнения защищенных информационных процессов, должностных инструкций и пр., а также содержат технические требования к составляющим элементам системы защиты информации (СиЗИ), как одной из составляющих СОБИ.

Регламент – это документ, в основном отражающий организационную составляющую процесса обеспечения безопасности информации. Он разрабатывается на основании Концепции и в директивной форме излагает порядок обращения с защищаемой информацией, основные правила действий сотрудников и их ответственность в обеспечении безопасности информации в любых ситуациях и на всех стадиях жизненного цикла обработки информации.

Как правило, Регламент, основываясь на описании информационных ресурсов, имеющихся в организации, и необходимого уровня их защиты, определяет обязанности и ответственность персонала за обеспечение безопасности информации (прежде всего это руководители организации, сотрудники служб защиты информации, безопасности, эксплуатации объектов, администраторы и пользователи информационной системы), порядок взаимодействия с другими организациями (обмен информацией и ее предоставление в государственные организации или следственные и надзорные органы, взаимодействие со СМИ), общие правила разграничения доступа к информации, порядок регистрации пользователей и назначения им прав доступа. Кроме того, Регламент частично охватывает и технические требования, вернее, правила обеспечения режима защиты при использовании компьютеров и программного обеспечения (порядок использования приложений, баз данных, систем электронного документооборота, защиты от вирусов, резервного копирования, бесперебойного питания, использования переносных компьютеров, средств связи и телекоммуникаций), правила работы пользователей в сети Интернет, правила учета, хранения и обращения со съемными носителями информации и твердыми копиями, проведения регламентного обслуживания оборудования и ПО. Наверное, такой доку-



Все документы, разрабатываемые при формировании Политики безопасности информации, обязательно должны иметь официальный юридический статус (например, приняты в форме приказа по организации).

мент, как Регламент, будет неполным, если в нем не найдут отражения вопросы, раскрывающие порядок и процедуры аттестации объектов, внутреннего контроля режима защиты информации и аудита безопасности информации внешними организациями. Необходимо также, чтобы он устанавливал порядок реагирования на нарушения режима безопасности (разбор инцидентов) и ликвидации последствий при возникновении нештатных ситуаций.

Второй документ этого уровня, ОТТ, является своеобразным корпоративным стандартом и содержит технические требования к программно-аппаратным средствам защиты, в том числе и встроенным в общесистемное программное обеспечение. По своей сути, такие требования аналогичны Профилю защиты (или Заданию по безопасности), разработанному в соответствии с методологией стандарта ГОСТ ИСО/МЭК 15408 для конкретной информационной системы, и поэтому успешно могут быть им заменены.

ОТТ являются официальным нормативным техническим документом организации, устанавливающим требования к функциям безопасности, реализуемым элементами информационной системы, для обеспечения требуемого уровня безопасности информации. Этот документ является также обязательным и для подрядных организаций (разработчиков), отвечающих за создание или модернизацию информационных систем. Вместе с тем, ОТТ служат и методическим подспорьем при формулировании требований по обеспечению безопасности информации в технических заданиях на информационные системы. Правда, здесь необходимо помнить, что общие требования, изложенные в ОТТ, могут уточняться по результатам обследования и моделирования возможных угроз безопасности информации применительно к конкретному объекту организации.

На третьем уровне Политики безопасности информации разрабатывается исполнительная документация, включающая в себя различные должностные положения и инструкции. Кроме того, данный уровень содержит эксплуатационные документы средств защиты информации, обеспечивающих разграничение доступа к защищаемым ресурсам, систему мониторинга и контроля. Третий уровень политики безопасности опирается на эксплуатационную документацию используемых программно-технических средств защиты, общесистемного и прикладного программного обеспечения, а также на стратегию и тактику защиты, обеспечиваемую техническими и программными средствами СиЗИ.

Дать точный перечень документов этого уровня достаточно сложно. Он определяется сложившейся в организации деловой практикой и традициями. Но, как пример, можно сказать, что к документам этого уровня можно отнести:

- положение о категорировании информационных ресурсов;
- положение о подразделении ОБИ и Требования к специалистам службы ОБИ;
- положение об администраторе безопасности информации;
- инструкцию о порядке приема (увольнения) сотрудников (в части задач ОБИ);
- инструкцию по организации парольной защиты;
- инструкцию о порядке предоставления доступа к ресурсам ИС;
- инструкцию по организации антивирусной защиты в ИС;
- регламент получения и отзыва сертификатов ключей шифрования;
- регламент и инструкцию администратору по настройке узлового оборудования ИС;
- регламент установки, модификации и технического обслуживания оборудования и ПО ИС;
- инструкцию по ведению делопроизводства конфиденциальной документации;
- инструкцию о порядке учета, хранения и обращения со съемными носителями информации;
- инструкцию (план) по ликвидации последствий нештатных ситуаций;
- порядок аттестации объектов информатизации по требованиям безопасности;
- и еще целый ряд аналогичных инструкций.

Документов на этом уровне может быть столько, сколько надо, но главное в этом процессе не увлекаться — чем их больше, тем сложнее в них ориентироваться, тем больше вероятность, что про них забудут, тем с большей уверенностью можно сказать, что вся работа по формированию Политики безопасности информации пошла насмарку. Лучше всего, если документы второго уровня и, в частности, РЕГЛАМЕНТ, описывая тот или иной вопрос, содержал бы упоминание (и давал бы соответствующую отсылку) о соответствующем документе третьего уровня. В этом случае можно с уверенностью сказать, что, во-первых, не будет лишних документов на третьем уровне Политики безопасности информации, и, во-вторых, по крайней мере сотрудники будут знать, что такие документы есть и где их взять. Ну а дальше — все зависит от той самой ПОЛИТИКИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, которая будет сформирована в вашей организации... <