Министерство науки и высшего образования Российской Федерации
Министерство внутренних дел Российской Федерации

Московский университет Министерства внутренних дел
Российской Федерации имени В.Я. Кикотя

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Учебное пособие

Москва

Московский университет
МВД России имени В.Я. Кикотя

2022

УДК 004.056
ББК 16.8
У67

Рецензенты:
начальник кафедры информационной безопасности Краснодарского университета МВД России доктор технических наук, профессор **А. В. Еськов**; профессор кафедры информационного и технического обеспечения ОВД Дальневосточного юридического института МВД России кандидат технических наук, доцент **К. М. Бондарь**; профессор кафедры уголовного права и криминологии доктор юридических наук, доцент **И. В. Никитенко**

Коллектив авторов:
В. А. Минаев, Е. С. Поликарпов, В. Т. Еременко, М. Ю. Рытов

У67 **Управление информационной безопасностью** : учебное пособие / [В. А. Минаев и др.]. – М. : Московский университет МВД России имени В.Я. Кикотя, 2022. – 310 с.
ISBN 978-5-9694-1145-6

В учебном пособии изложена базовая терминология в сфере управления информационной безопасностью. Рассмотрены вопросы стандартизации систем и процессов управления информационной безопасностью. Описана методика разработки и реализации политики информационной безопасности в подразделениях МВД России. Показаны основные свойства и особенности современной системы управления информационной безопасностью.

Пособие предназначено обучающимся по направлению подготовки «Информационная безопасность» при изучении дисциплины «Управление информационной безопасностью» и смежных с ней.

УДК 004.056
ББК 16.8

ISBN 978-5-9694-1145-6

© Московский университет
МВД России имени В.Я. Кикотя, 2022

СОДЕРЖАНИЕ

ПРИНЯТЫЕ СОКРАЩЕНИЯ

АБС – автоматизированная банковская система.
АО – аппаратное обеспечение.
АС – автоматизированная система.
БД – база данных.
ВЧС – виртуальная частная сеть.
ИБ – информационная безопасность.
ИС – информационная система.
ИСО – Международная организация по стандартизации.
ИТ – информационные технологии.
ИТТ – информационные и телекоммуникационные технологии.
МСЭ – межсетевой экран.
МЭК – Международная электротехническая комиссия.
НСД – несанкционированный доступ.
ОИБ – обеспечение информационной безопасности.
ОНБ – обеспечение национальной безопасности.
ОС – операционная система.
ПО – программное обеспечение.
ПолИБ – политика информационной безопасности.
СЗИ – средства защиты информации.
СИБ – система информационной безопасности.
СМИБ – система менеджмента информационной безопасности.
СОВ – система обнаружения вторжений.
СОИБ – система обеспечения информационной безопасности.
СУБД – система управления базой данных.
СУИБ – система управления информационной безопасностью.
СУНБ – система управления непрерывностью бизнеса.
ТКЭ – технико-криминалистическая экспертиза.
УНБ – управление непрерывностью бизнеса.
ЭЦП – электронная цифровая подпись.

ВВЕДЕНИЕ

К сегодняшнему дню информация представляет собой один из самых главных активов любой организации, имеющий ценность для нее, находящийся в ее распоряжении, обеспечивающий ее эффективное функционирование и вследствие этого нуждающийся в защите. Система МВД России не является исключением.

Между тем вовремя не нейтрализованные и доступные злоумышленникам уязвимости в обеспечении безопасности информационных активов организации могут привести к катастрофическим потерям финансового и репутационного характера, нанести непоправимый ущерб бизнес-процессам, а применительно к деятельности органов внутренних дел (ОВД) – оперативно-служебным процессам. Поэтому вопрос разработки адекватной потребностям той или иной структуры эффективной СУИБ, ее квалифицированного внедрения и использования сегодня, как никогда прежде, актуален. Это вопрос из ряда «быть или не быть» для любой организации.

Осуществление операций с применением инфокоммуникационных технологий (ИКТ) в современной организации выходит далеко за рамки ограничений, присущих защищенным центрам обработки данных со строго определенными физическими и логическими периметрами. Это связано с тем, что в процессе эволюции усложнились программные и аппаратные средства. Многочисленные операции теперь выполняют серверы, рабочие станции, ноутбуки, мобильные телефоны, умные часы и другие устройства, которые сотрудники организации, смежные с ними структуры могут использовать в любое время.

Доступ к ресурсам ИС получает значительное число пользователей различных категорий, подключающихся к корпоративным сетям через Интернет как по выделенным линиям, так

и по коммутируемым каналам и радиоканалам.

Обработка информационных потоков в системе МВД России требует высоких темпов и точности. Сбор и хранение крупных информационных баз на защищенных электронных носителях, объединение в общий массив сложных территориально-динамических данных, увеличение стоимости информационных ресурсов, большая зависимость от конфиденциальности, целостности, доступности и других значимых свойств информационных активов – это только часть важных проблем, требующих четкой организации управления ИБ.

Российские организации осознали необходимость эффективного управления своей информационной безопасностью, приобретающей все большее значение по мере их роста и продвижения в своей деятельности. Клиентам важно знать, что соблюдается конфиденциальность их персональных данных. Инвесторам необходима уверенность в том, что активы организации защищены. Смежные структуры ожидают, что организация будет функционировать без сбоев, вызванных ошибками в работе ИС на всех стадиях их жизненного цикла, умышленными или неумышленными действиями персонала, вредоносным ПО и другими деструктивными факторами.

В начале 80-х гг. прошедшего века защита информации могла быть эффективно обеспечена при помощи специально разработанных организационных мер и различных программно-аппаратных средств. С развитием локальных и глобальных сетей, каналов спутниковой связи вопрос об ИБ встал острее.

Несистемная реализация защитных мер не может обеспечить требуемый уровень ИБ. Чтобы надежно защитить свою информацию, необходимо интегрировать решение вопросов защиты в единый для всей организации процесс управления ИБ, связанный со снижением рисков для ее деятельности.

Управление ИБ не может рассматриваться только с технической и технологической точек зрения, поскольку это – комплексный, непрерывно реализуемый процесс, обязательно имеющий правовую, организационную, документальную и другие составляющие.

В современных условиях достаточно много сделано для обеспечения ИБ организаций, но явно недостаточно предложено по управлению теми защитными мерами, которые внедрены в них. Ведь зачастую специалисты в организациях полностью не осознают, какие их активы являются наиболее критичными, какие риски ИБ связаны с этими активами, какие защитные меры необходимо запланировать в этой связи. Все указанные проблемы решаются за счет построения СУИБ.

Разработка централизованной СУИБ на уровне организации зависит от множества внутренних и внешних факторов, которые часто противоречат друг другу, иными словами – конфликтуют. Что хорошо для одной организации, совсем не подходит для других. В этой связи им требуются различные комбинации структур, процессов и механизмов, обеспечивающих защищенное состояние существующей информационной инфраструктуры наилучшим образом в каждом регионе и конкретной временной точке, эффективно проводя принятую организацией политику.

В учебном пособии рассмотрены основополагающие аспекты, связанные со сложным процессом управления ИБ, состоящим из многих направлений и охватывающим всю организацию независимо от ее масштаба и области деятельности, а также созданием, планированием, реализацией, контролем и совершенствованием осуществляющей этот процесс СУИБ.

Глава 1. БАЗОВАЯ ТЕРМИНОЛОГИЯ В СФЕРЕ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

1.1. Система

Система (греч. *systema* – целое, составленное из частей) – это единство взаимосвязанных и взаимодействующих элемен тов, характеризующихся общей целью [1; 2].

Если говорить более детально, система – это состоящее из двух или более элементов множество, которое удовлетворяет следующим трем условиям [3]:

1. Поведение каждого элемента воздействует на поведение целого (например, организм человека). Каждая его часть, сердце, легкие, желудок и другие влияют на функционирование организма в целом.

2. Воздействие на целое взаимозависимо, что означает – поведение каждого элемента и его влияние на целое зависит от того, как ведет себя, по крайней мере, еще какой-то элемент. При этом ни один элемент самостоятельно не воздействует на систему в целом.

3. Элементы системы связаны таким образом, что образование ими независимых подгрупп невозможно.

Уточняя определение, систему можно определить как множество элементов любой природы, взаимодействующих между собой для достижения общей цели, обладающее системным свойством/свойствами, и этого свойства не имеет ни один из элементов и ни одно из их подмножеств.

Свойствами системы являются [4]:

1) целостность – первичность целого по отношению к элементам;

2) неаддитивность – несводимость свойств системы к сумме свойств составляющих ее элементов;

3) синергетичность – целенаправленность действий совокупности элементов системы, усиливающая эффективность ее функционирования;

4) эмерджентность – наличие новых свойств у множества элементов системы, которых не было до их объединения. Элемент обладает свойствами, которые он теряет в случае отделения от системы;

5) мультипликативность – эффекты умножения, а не сложения свойств функционирования элементов в системе;

6) взаимодействие и взаимозависимость системы и внешней среды;

7) структурность – возможность декомпозиция системы на части и установление связей между частями;

8) иерархичность – каждая часть системы может быть рассмотрена как подсистема общей системы;

9) непрерывность функционирования;

10) целенаправленность – система всегда рассматривается относительно некоторой цели/целей;

11) адаптивность – стремление системы к состоянию устойчивого равновесия, предполагающее постоянную адаптацию ее параметров к изменению характеристик внешней среды;

12) альтернативность развития – существование нескольких альтернативных путей достижения конкретной цели;

13) наследственность – передача наиболее сильных признаков эволюции системы от ее старой версии к новой;

14) приоритетность – преобладание целей системы более глобального уровня перед целями ее частей или подсистем.

1.2. Системный подход

Системный подход – методология исследования объекта как системы в разных аспектах, комплексно, учитывая всю совокупность связей между ее элементами [1].

Системный подход ориентирован на раскрытие целостности объекта, на выявление многообразных типов связей и отношений как внутри исследуемого объекта, так и в его взаимоотношениях с внешней средой.

Установлением структурных связей между элементами системы, базируясь на комплексе общенаучных, естественнонаучных, статистических, математических методов, занимается *системный анализ*, представляющий совокупность методов и средств изучения сложных объектов. Системный анализ используется как эффективный инструмент решения сложных, не всегда четко сформулированных проблем, к числу которых относится управление различными объектами. Системный анализ позволяет структурировать проблемы, разложить их в серию решаемых с помощью различных методов задач, найти критерии их решения, детализировать цели.

При системном подходе в рамках моделирования систем необходимо, прежде всего, четко определить его цель. Реализации этой цели способствуют корректный отбор элементов системы, описание структуры и связей между ними, выбор критериев оценки адекватности модели.

Основными целями при системном подходе являются обеспечение:

– повышения синергетичности;

– снижения эмерджентности;

– мультипликативности в организации;

– устойчивости функционирования организации;

– адаптивности работы организации;

– совместимости работы различных подсистем организации;

– эффективной работы обратных связей в организации.

Системный подход предполагает этапность решения проблемы, включающую:

– изучение предметной области (качественный анализ);

– выявление и формулирование проблемы;

– математическю (количественню) постановку проблемы;

– натурное и/или математическое моделирование исследуемых объектов и процессов.

1.3. Процесс

Термин «процесс» (лат. *processus* – продвижение) может быть рассмотрен в нескольких аспектах:

– последовательная смена явлений, состояний в развитии конкретной системы;

– цепь логически связанных, повторяющихся действий, в результате которых используются ресурсы организации с целью достижения определенных измеримых результатов [5];

– поиск и оценка альтернативных решений, обработка результатов исследования, формулирование выводов по решению проблемы.

Обобщая различные определения, можно определить процесс как совокупность взаимосвязанных видов деятельности, преобразующей характеристики входов в характеристики выходов, потребляющей для этого различные ресурсы и обеспечивающей управляющие воздействия (управления) (рис. 1.1). Входами в процесс, как правило, выступают выходы других процессов [5].

Рис. 1.1. Иллюстрация понятия «процесс»

Входами могут быть, например, множество активов организации, используемых при осуществлении некоторой деятельности. На выходе получается непосредственный результат процесса.

Входы и выходы процесса управления информационной безопасностью могут быть осязаемыми (используемое оборудование для защиты, характеристики информационных атак, защищаемая информация на различных носителях и т. п.) и неосязаемыми (характеристики «спящих» угроз, планируемые требования и услуги по защите информации и т. п.).

Любой процесс управления информационной безопасностью имеет заинтересованные стороны, например, потребителя защиты информации, внутреннего или внешнего относительно организации, и действует в соответствии с установленными целями.

Процессы, происходящие в организации и требующие для своего осуществления управления их информационной безопасностью, можно разделить на четыре группы [4]:

1. Основные (процессы жизненного цикла), обеспечивающие базовый результат деятельности организации. Назначение таких процессов – создание ключевых продуктов; результат – конечный продукт.

2. Обеспечивающие, предназначенные для нормального функционирования основных и других процессов необходимыми ресурсами; они обеспечивают сервисное обслуживание оборудования, энергоресурсное снабжение, обеспечение средой производства, информацией, финансовой, требуемые параметры окружающей среды, PR-деятельность и связь с общественностью и т. д. Результат указанных процессов – ресурсы, сервисы, услуги для основных процессов. Очевидно, что в этом смысле ОИБ относится к вспомогательной деятельности.

3. Процессы управления (менеджмента), относящиеся к постановке целей, стратегическому планированию, установлению политик, созданию инфокоммуникаций и т. п. Назначение процесса – управление деятельностью организации; результат – деятельность организации с той или иной эффективностью. По своей природе управленческие задачи являются информационными.

4. Процессы измерения, анализа и совершенствования направлены на усовершенствование всей деятельности организации. Чем более совершенна эта деятельность, тем лучше отлажены процессы указанной группы.

Их эффективность отражает способность достижения желаемых результатов, оцениваемых посредством внутренних и внешних процессов контроля.

1.4. Процессный подход

Процессный подход – это идентификация и управление применяемых организацией процессов и особенно их взаимодействия [5]. В основе подхода – взгляд на организацию как на совокупность ключевых процессов, а не функциональных подразделений. Главное внимание при этом уделяется процессам, объединяющим отдельные функции в общие потоки, и в целом направлены на достижение конечного результата всей организации, а не отдельного подразделения.

Таким образом, основное преимущество процессного подхода заключается в управлении и контроле взаимодействия между различными процессами и связующими звеньями в контексте функциональной иерархии (организационно-штатной структуры) организации.

В ГОСТ Р ИСО 9000–2001 «Системы менеджмента качества. Основные положения и словарь» [5] содержится ряд требований

к реализации процессного подхода в организации, главными из которых являются следующие:

– определение процессов, необходимых для реализации;

– выявление входов и выходов каждого процесса для установления их последовательности и взаимодействия;

– планирование и обеспечение ресурсами (включая информацию), необходимыми для реализации процессов и управления ими;

– установление необходимой степени и документирование процессов;

– планирование процессов;

– наличие критериев и методов оценки управления процессами;

– осуществление мониторинга, оценки и анализа процессов;

– проведение корректирующих и превентивных действий по результатам анализа процессов, включая совершенствование процессов;

– определение методов и осуществление управления процессами, результаты которых нельзя проверить посредством измерения.

1.5. Управление

Управление – вид человеческой деятельности, появившийся с возникновением совместной активности людей и регулирующий их отношения в этом процессе. Оно представляет целенаправленную деятельность человека, с помощью которой он упорядочивает и подчиняет своим интересам элементы среды существования общества [6].

Это процесс, состоящий из серии непрерывных взаимосвязанных действий (как отражение управленческих функций). Управление суммирует все управленческие функции, состав

которых впервые предложен Анри Файолем: «Управлять – это значит предвидеть, организовывать, распоряжаться, координировать и контролировать» [7].

С позиции системного подхода управление представляет собой совокупность непрерывных взаимосвязанных возможных воздействий на объект (управляемую систему) для достижения заданной цели. Оно направлено либо на сохранение ее основного качества (совокупности свойств, утеря которых приводит к разрушению системы), либо на выполнение некоторой программы, обеспечивающей устойчивость функционирования и достижение определенной цели.

Системой управления (СУ) называют систему, реализующую функции управления. Главные вопросы, стоящие перед СУ, – чем и как управлять.

Основной элемент управляющей системы (УС) – *субъект управления*. Это лицо, группа лиц или специально созданный орган, являющийся источником управленческого воздействия на объект – *управляемую систему*, осуществляющие деятельность, направленную на обеспечение его нормального функционирования и успешное достижение заданной цели.

Объект управления – это система (организация, коллектив, конкретное лицо), на которую направлены управленческие воздействия с целью ее совершенствования, повышения качества реализации функций и решения задач, успешного достижения запланированной цели (целей).

Управление всегда связано с решением проблем, возникших в процессе функционирования объекта управления. При этом субъект управления, применяя системный подход, выявляет всю совокупность условий, причин и факторов, приведших к возникновению проблем, и определяет возможные пути и средства их разрешения.

Субъект управления реализует задачи целеполагания, достижения оптимального выполнения программы, обеспечивая удержание выходных характеристик системы в требуемых пределах при изменении характеристик внешней среды.

Метод управления – это совокупность последовательно применяемых способов воздействия субъекта управления на объект управления для достижения поставленной цели.

Программное управление – это выполнение последовательности действий (операций) в строгом соответствии с предписанной программой (правилами, распоряжениями, законами и т. п.).

Управление учитывает обратные связи, отражающие отклонения от намеченного пути, предполагает понимание объектом управления своего состояния в каждый момент времени на траектории следования к намеченной цели. При отклонении текущих параметров от требуемых включается программа коррекции траектории, что позволяет компенсировать ошибки и учесть внешние возмущения.

В теории управления существует три основных подхода: системный, процессный и ситуационный. О первых двух сказано выше. Ситуационный подход предполагает их сочетание в зависимости от конкретной ситуации функционирования организации для достижения ее своих целей, в частности, связанной с обеспечением информационной безопасности.

Для полноты раскрытия термина «управление» необходимо отметить, что в английском языке имеется несколько слов, которые переводятся на русский как «управление»:

1) *control* – исторически первый из применяемых в ИТ терминов, отражающий самые простейшие операции в области управления, в большей степени с точки зрения технического аспекта деятельности;

2) *management* – термин, который первоначально употреблялся в отношении управления человеческими ресурсами. В настоящее время встречается в сочетании с множеством понятий из области ИТ и имеет смысл организации и регулирования какой-либо деятельности, т. е. ее администрирования;

3) *governance* – термин, который стал активно использоваться применительно к ИТ только в последнем десятилетии; под ним обычно понимается руководство по организации и контролю за какой-либо деятельностью. Переводится на русский как «власть, руководство, управление».

Организация IT Governance Institute (ITGI, http://www.itgi.org) определяет руководство ИТ как структуру взаимоотношений и процессов в организации по управлению и контролю для достижения ею поставленных целей посредством увеличения ее стоимости в процессе снижения рисков и повышения дохода от использования ИТ и связанных с ними процессов. Просто управление ИТ ориентировано на ИТ-сервисы и продукты и управление ИТ-операциями. Руководство ИТ значительно шире и концентрируется на том, что ИТ должны делать для удовлетворения нынешних и будущих потребностей бизнеса и клиентов организации.

В основе такого руководства лежит концепция, согласно которой управление организацией должно быть хорошо организованной деятельностью, осуществляемой специалистами, осознающими полную ответственность и подотчетность своих действий. Руководство является формальным средством исполнения своих обязанностей представителями исполнительной власти в государственных, коммерческих, образовательных и иных организациях. Руководство обусловлено необходимостью управления рисками и защитой самой организации и по своей сути связано с двумя функциями: производством продукции и снижением рисков.

В организации должна быть создана система руководства, применяемая ко всем видам деятельности и процессам: планированию, проектированию, закупкам, разработке, внедрению и мониторингу. Система руководства включает в себя управление окружающей средой и различными областями деятельности и строится на определенных принципах:

– понятные ожидания (понятные показатели, четкие политики и стандарты, сильные связи, ясная стратегия);

– понятное выполнение операций с установленной ответственностью (компетентные организационные структуры, четко определенные роли и обязанности, упорядоченные процессы и процедуры, эффективное использование технологий, ответственное управление активами);

– проактивное управление изменениями;

– своевременное и точное обнаружение;

– независимый анализ и постоянное совершенствование.

Руководство осуществляется в следующих условиях и обстоятельствах:

– федеральные и государственные законы, директивы и руководящие указания;

– промышленное регулирование практики управления;

– миссия и стратегия организации;

– допустимые для организации риски;

– этика, культура и ценности организации;

– расположение организации и подход к управлению (централизованный или децентрализованный);

– политики, стандарты, процессы и процедуры, принятые в организации;

– роли и ответственность в организации;

– планы и отчетность организации;

– проверка организации на различные виды соответствия.

Возможные области руководства:

1) стратегическое планирование и регулирование – прогноз и возможности, необходимые для поставки продуктов организации;

2) поставка продукции – создание прибыли во время и в рамках бюджета;

3) управление рисками ИБ – непрерывный процесс, начинающийся с идентификации рисков ИБ (угроз ИБ и уязвимостей) и оценки их воздействия на активы, снижение рисков ИБ посредством контрмер и формальное принятие руководством остаточных рисков ИБ;

4) управление ресурсами – правильное использование возможностей (люди, оборудование, ПО и т. д.) для удовлетворения потребностей организации;

5) измерение производительности обеспечивает обратную связь с потребностями организации, чтобы она оставалась дееспособной или вовремя принимались корректирующие меры.

В начале XX в. начала развиваться наука управления, которую стали называть менеджмент (англ. *manage* – управлять, руководить).

В современной литературе имеются разные определения менеджмента, раскрывающие это понятие с различных точек зрения:

– способ (манера) обращения с людьми, власть и искусство управления, особого рода административные навыки, орган управления (Оксфордский словарь английского языка);

– совокупность принципов, форм, методов, приемов и средств управления производством и производственным персоналом с использованием достижений науки управления;

– искусство управления интеллектуальными, финансовыми, материальными ресурсами [2];

– эффективное и результативное достижение целей организации посредством планирования, организации, лидерства (руководства) и контроля над организационными ресурсами [3];

– скоординированная деятельность по руководству и управлению организацией [5] (поэтому иногда делают вывод, что понятие менеджмента шире, чем просто управление).

В других источниках менеджмент определяется:

– как особый вид профессионально осуществляемой (осуществляемой профессионалами, профессиональными управляющими) деятельности, направленной на достижение определенных целей путем рационального использования материальных и трудовых ресурсов с применением определенных научных подходов, принципов, функций и методов;

– объединение управленческой деятельности с кадровой политикой;

– состояние всей управленческой инфраструктуры в различных масштабах;

– процесс оптимизации человеческих, материальных и финансовых ресурсов для достижения организационных целей;

– теория и практика научного и хозяйственного управления организацией в условиях рынка;

– система научных знаний, составляющих теоретическую базу практического опыта в области управления и имеющих междисциплинарный характер;

– совокупность лиц, идентифицируемых с менеджерами, а также с органами или аппаратом управления и т. п.

Менеджмент включает основные функции управления (прогнозирование, целеполагание, планирование, организация деятельности, мотивирование персонала, лидерство, контроль, учет и анализ, корректировка деятельности и т. д.) и определяет эффективное достижение целей организации при оптимальном

использовании ресурсов. Ограниченность ресурсов при выполнении функций управления требует их эффективного распределения и использования с учетом взаимозависимости, и взаимосвязанности этих функций. Менеджмент применяет и реализует специальные технологии и инструменты управления: организацию и организационные отношения (формальные и неформальные), организационную культуру, мотивирование, стимулирование и др. Таким образом, менеджмент является наиболее эффективным способом управления.

Часто слова «менеджмент» и «управление» используются как синонимы, хотя их научная трактовка, что видно из приведенных выше объяснений, совпадает не полностью.

1.6. Циклическая модель управления процессом

Для структурирования всех процессов управления и для обеспечения учета всех значимых элементов процессного подхода применяется циклическая модель, или цикл, PDCA (англ. PlanDoCheckAct – планируй, выполняй, проверяй, действуй), предложенная и развитая двумя американскими учеными и специалистами в теории управления качеством.

В. Шухарт впервые описал цикл PDCA в 1939 г. в своей книге «Статистические методы с точки зрения управления качеством». В. Деминг пропагандировал использование цикла PDCA в качестве основного способа достижения непрерывного улучшения процессов, и поэтому в современном мире эта формула больше известна как «цикл Деминга». Он также ввел модификацию цикла PDCA – цикл PDSA (англ. *study* – изучай):

1. *«Планируй» (Plan)* – определение целей и задач, а также способов достижения целей. На данном этапе обеспечивается единое направление деятельности организации по достижению ее целей в соответствии с существующими требованиями в обо-

значенный отрезок времени. Для этого определяются и описываются текущее и желаемое состояния процессов за счет выявленных несоответствий и причин их появления. Планирование не является отдельным разовым событием, если организация стремится функционировать как можно дольше. Поэтому она пересматривает свои цели, если полное достижение первоначальных практически завершено или их выполнение невозможно в силу ряда причин. Вторая причина, по которой планирование должно осуществляться непрерывно, – это неопределенность будущего. Изменения в окружающей среде, ошибки в оценках и другие факторы приводят к тому, что события разворачиваются не так, как это предвиделось при выработке первоначальных планов. Поэтому, чтобы планы согласовывались с реальностью, их необходимо регулярно пересматривать.

2. *«Осуществляй» (Do)* – реализация процесса: обучение и подготовка кадров, выполнение работ. На данном этапе, в первую очередь, происходит создание некоторой структуры, которая должна выполнять намеченные планы и тем самым достигать цели организации. Следует помнить о том, что стандарты всегда несовершенны, поэтому также необходимо полагаться на опыт и знания квалифицированных работников. Однако на всех этапах цикла Деминга возникает проблема таких работников. Поэтому необходимо реализовать программы обучения и целенаправленной подготовки кадров.

3. *«Проверяй» (Check)* – проверка результатов выполнения работ, проведенных на предыдущем этапе. При проверке необходимо проводить мониторинг достижения целей и требований к результатам деятельности организации за определенный период. Если все идет в соответствии с поставленными задачами и согласно требованиям стандартов, то никакой корректировки не требуется. Однако при обнаружении отклонения вмешатель-

ство для установления причин неэффективной деятельности и планирования мер по ее улучшению становится необходимым.

4. *«Воздействуй» (Act)* – осуществление управляющих воздействий по улучшению показателей процессов. На данном этапе предпринимаются действия по коррекции отклонений от первоначальных планов и улучшению функционирования процессов. Если вносимые изменения не решают поставленную задачу, цикл следует повторить. При этом одно из возможных действий – пересмотр целей для того, чтобы они стали более реалистичными.

Применение цикла PDCA позволяет эффективно управлять деятельностью организации на системной основе [7]. Данный цикл может быть применен внутри каждого процесса организации как на высоком уровне управления, так и применительно к простым производственным процессам.

Системный подход рассматривает управленческую деятельность как совокупность элементов, взаимодействующих между собой в пространстве и во времени, функционирование которых направлено на достижение общей цели.

Системный подход к управлению организацией – это организация взаимосвязанных процессов с целью достижения заданной стратегической цели [1]. При таком понимании организация представляется в виде иерархической системы взаимосвязанных моделей, позволяющих изучать ее целостные свойства и структуру. Он позволяет:

– определить систему путем выявления или разработки процессов, влияющих на достижение заданной стратегической цели;

– структурировать систему так, чтобы достичь заданной стратегической цели наиболее эффективным способом;

– обеспечить взаимосвязи между процессами системы;

– обосновать зависимость организации от факторов внешней и внутренней среды, оказывающих прямое и косвенное воздействие на ее функционирование;

– проводить непрерывное совершенствование системы;

– лучше понимать распределения ролей и ответственности при достижении стратегических целей, уменьшая тем самым межфункциональные барьеры и улучшая коллективную работу.

Признаки системного подхода к управлению:

1. Исходным моментом в организации управления и конечным результатом его осуществления является человек с его потребностями, мотивами, ценностями. При этом создаются организационные, экономические и социально-психологические условия заинтересованности человека в результатах труда, удовлетворении его потребностей.

2. Принципы и методы системного подхода позволяют управлять как внутренними процессами деятельности людей, так и процессами поведения организации в социально-экономической среде.

3. Профессионализм управления, выступающий как одно из главных требований к персоналу.

4. Гибкая организация управления, способная оперативно перестаиваться в соответствии с меняющимися условиями, факторами внешней и внутренней среды.

Процессный подход к управлению, или процессное управление, – подход к управлению, который рассматривает управление как реализацию непрерывной серии взаимосвязанных управленческих функций.

Процессное управление представляет собой планомерную деятельность по формированию целенаправленного поведения организации посредством описания и менеджмента системы взаимосвязанных и взаимодополняющих процессов организации

и их ресурсного обеспечения. Руководство организацией возможно осуществлять, только управляя ее процессами [1]. Поэтому процессное управление – это инструмент, обеспечивающий реализацию стратегии организации.

Система управления, основанная на процессном подходе, – это система, в которой основным объектом управления выступает производственный процесс. Применение процессного подхода требует описания, оптимизации и автоматизации указанных процессов.

При использовании процессного подхода структура управления организацией включает два уровня:

– управление в рамках каждого процесса;

– управление группой процессов на уровне всей организации.

Основой управления отдельным процессом и группой процессов являются показатели эффективности, среди которых выделяют:

– затраты и время на его осуществление;

– показатели качества процесса;

– информационная безопасность.

Поскольку сегодня цифровая обработка информации является частью почти всех сфер жизни, считается, что термин «информационная безопасность» (а не «безопасность ИТ») более всеобъемлющ.

В России в основном используются три термина: «безопасность информации», «защита информации» и «информационная безопасность».

Согласно Руководящему документу Гостехкомиссии России от 30 марта 1992 г. «Защита от несанкционированного доступа к информации. Термины и определения», безопасность информации – это состояние защищенности информации, обрабатыва-

емой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз [8].

Согласно Рекомендациям по стандартизации Р 50.1.053–2005 «Информационные технологии. Основные термины и определения в области технической защиты информации» и ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения», безопасность информации (данных) – это состояние защищенности информации, при котором обеспечиваются ее (их) конфиденциальность, доступность и целостность [9; 10].

Согласно Р 50.1.053–2005, безопасность информации (при применении информационных технологий – это состояние защищенности ИТ, обеспечивающее безопасность информации, для обработки которой она применяется, и ИБ автоматизированной ИС, в которой она реализована.

В ГОСТ Р 50922–2006 под защитой информации понимается деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Понятие «информационная безопасность» в различных контекстах имеет разный смысл. Например, в Доктрине информационной безопасности Российской Федерации этот термин определяется как состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В Стандарте Банка России СТО БР ИББС 1.0 ИБ – это безопасность, связанная с угрозами в информационной сфере. При этом защищенность достигается обеспечением совокупности свойств ИБ: доступности, целостности, конфиденциальности информационных активов, а информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распростра-

нение, хранение и использование информации, а также системы регулирования возникающих при этом отношений [11].

Обобщая, можно сказать, что под ИБ понимается:

– защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры [12];

– механизм защиты, обеспечивающий конфиденциальность, целостность и доступность информации [13];

– свойство информации сохранять конфиденциальность, целостность и доступность [14].

Согласно ГОСТ Р 53113.1–2008 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения», *информационная безопасность* – это аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и надежности информации, или средства ее обработки [15].

Кроме того, данное понятие в современных условиях включает в себя еще четыре свойства:

– аутентичность или подлинность (свойство, гарантирующее правдивость) применяется к пользователям, процессам, системам, информации;

– учет (однозначное отслеживание всех действий, влияющих на ИБ);

– неоспоримость (причастность к совершению операций с информацией);

– надежность (соответствие запланированному поведению и результатам).

Итак, ИБ можно определить как состояние защищенности информации, которое достигается обеспечением совокупности свойств доступности, целостности, конфиденциальности, аутентичности, учета, неоспоримости и надежности.

Под ИБ организации понимается состояние защищенности интересов (целей) организации в условиях угроз ИБ (угроз доступности, целостности, конфиденциальности, аутентичности, учета, неоспоримости и надежности) в информационной сфере.

ИБ должна стать неотъемлемой частью производственной и деловой культуры организации. Для достижения целей ИБ организации перечисленные свойства информации поддерживаются комплексом мероприятий по управлению ИБ, осуществляемых на основе соответствующих нормативных актов, ПолИБ и организационных структур, за счет реализации установленных мер, методов, процедур и программно-аппаратных СЗИ, которыми необходимо постоянно управлять [13].

Итак, ИБ представляет, главным образом, проблему управления (хотя в условиях сильной зависимости от использования ИТ и техническая сторона не должна оставаться без внимания), а ОИБ – это процесс поддержания состояния защищенности активов организации, который должен осуществляться постоянно, и поэтому им необходимо управлять. Этапы этого процесса составляют основу комплексной СОИБ организации, поскольку ОИБ требует комплексного подхода, включающего организационную (подготовленный персонал и нормативные документы), техническую (СЗИ) и другие составляющие (рис. 1.2).

Рис 1.2. Этапы процесса обеспечения информационной безопасности организации

Вопросы для самоконтроля

1. Как определяется понятие системы?
2. Каковы основные свойства системы?
3. В чем заключается системный подход к исследованию объектов информационной безопасности?
4. Каковы особенности рассмотрения системного подхода применительно к управлению информационной безопасностью?
5. Какие виды деятельности в организации можно назвать процессом?
6. Какую роль играют процессы в организации?

7. Какие элементы процесса могут быть исключены из определения: входные данные процесса, выходные данные процесса, управляющее воздействие, ресурсы?

8. Что понимается под ресурсами в рамках определения понятия процесса?

9. Кто в организации может и должен определять цели процессов?

10. Что понимается под управляющим воздействием в рамках определения понятия процесса?

11. В чем заключается процессный подход?

12. Дайте определение понятия «управление» с позиций системного подхода.

13. Дайте определение понятия «менеджмент».

14. В чем различия понятий «управление» и «менеджмент»?

15. Каковы основные функции управления?

16. Что такое метод управления?

17. Дайте определение системы управления.

18. Что представляет собой система управления, основанная на процессном подходе?

19. Каковы особенности рассмотрения процессного подхода применительно к управлению?

20. К каким процессам организации может быть применена циклическая модель PDCA?

21. В чем состоят основные преимущества использования циклической модели PDCA?

22. Чем различаются термины «защита информации» и «информационная безопасность»?

23. Какие свойства ИБ в современных условиях должны приниматься во внимание и что понимается под каждым из ее свойств?

Глава 2. СТАНДАРТИЗАЦИЯ СИСТЕМ И ПРОЦЕССОВ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Если говорить с позиции производства, управление информационной безопасностью является частью более широкого процесса управления рисками. Если организация после анализа и оценки всех своих бизнес-рисков делает вывод об актуальности рисков ИБ, то в игру вступает уже непосредственно защита информации как способ минимизации некоторых рисков. Управление рисками позволяет эффективно и рационально выстраивать процессы ИБ и распределять ресурсы для защиты существенных и актуальных активов компании, а оценка рисков позволяет применять целесообразные меры по их минимизации. Для этого логично применять более дорогостоящие решения, чем для противодействия незначительным или труднореализуемым угрозам.

Кроме этого, выстроенный процесс управления рисками ИБ позволит разработать и в случае необходимости применить четкие планы обеспечения непрерывности деятельности и восстановления работоспособности: глубокая проработка различных рисков поможет заранее учесть, например, внезапно возникшую потребность в удаленном доступе для большого количества сотрудников, как это может произойти в случае эпидемий или коллапса транспортной системы.

2.1. Общая концепция управления рисками

Под *риском информационной безопасности*, или киберриском, понимают потенциальную возможность использования уязвимостей конкретной угрозой активов для причинения ущерба организации. Под *величиной риска* понимают произведение

вероятности негативного события и размера ущерба. Условно это можно выразить следующей формулой:

*Величина риска = Вероятность события * Размер ущерба.*

Существует классификация рисков: по источнику риска (например, атаки хакеров или инсайдеров, финансовые ошибки, воздействие государственных регуляторов, юридические претензии контрагентов, негативное информационное воздействие конкурентов); по цели (информационные активы, физические активы, репутация, бизнес-процессы); по продолжительности влияния (операционные, тактические, стратегические).

Этапы и цели анализа рисков ИБ:

1. Идентифицировать активы и оценить их ценность.

2. Идентифицировать угрозы активам и уязвимости в системе защиты.

3. Просчитать вероятность реализации угроз и их влияние на производство.

4. Соблюсти баланс между стоимостью возможных негативных последствий и стоимостью мер защиты, дать рекомендации руководству по обработке выявленных рисков.

Этапы с 1-го по 3-й являются процедурами оценки риска (англ. *risk assessment*) и представляют собой сбор имеющейся информации и частично – ее обработку.

Этап 4-й – это полноценный анализ рисков (англ. *risk analysis*), т. е. изучение собранных данных и выдача результатов/указаний для дальнейших действий. При этом важно понимать уровень уверенности в корректности проведенной оценки.

На 4-м этапе также предлагаются методы обработки для каждого из актуальных рисков: передача (например, путем страхования), избегание (например, отказ от внедрения той или иной технологии или сервиса), принятие (сознательная готовность понести ущерб в случае реализации риска), минимизация (при-

менение мер для снижения вероятности негативного события, приводящего к реализации риска).

После завершения всех этапов анализа рисков следует выбрать приемлемый для компании уровень рисков (англ. *acceptable risk level*), установить минимально возможный уровень безопасности (англ. *baselines of performance*), затем внедрить контрмеры и в дальнейшем оценивать их с точки зрения достижимости установленного минимально возможного уровня безопасности. Ущерб от реализации атаки может быть прямым или непрямым.

Прямой ущерб – это непосредственные очевидные и легко прогнозируемые потери компании, такие как утеря прав интеллектуальной собственности, разглашение секретов производства, снижение стоимости активов или их частичное, или полное разрушение, судебные издержки и выплаты штрафов и компенсаций и т. д.

Непрямой ущерб может означать качественные или косвенные потери.

Качественными потерями могут являться приостановка или снижение эффективности деятельности компании, потеря клиентов, снижение качества производимых товаров или оказываемых услуг.

Косвенные потери – это, например, недополученная прибыль, потеря деловой репутации, дополнительно понесенные расходы. Кроме этого, в зарубежной литературе встречаются такие понятия, как *тотальный риск* (англ. *total risk*), который присутствует, если вообще никакие меры защиты не внедряются, а также *остаточный риск* (англ. *residual risk*), который присутствует, если угрозы реализовались, несмотря на внедренные меры защиты.

Анализ рисков может быть как *количественным*, так и *качественным*.

Рассмотрим один из способов *количественного анализа* рисков. Основными показателями будем считать следующие величины:

ALE – annual loss expectancy, ожидаемые годовые потери, т. е. «стоимость» всех инцидентов за год.

SLE – single loss expectancy, ожидаемые разовые потери, т. е. «стоимость» одного инцидента.

EF – exposure factor, фактор открытости перед угрозой, отражающий, какой процент актива разрушится при успешной реализации угрозы.

ARO – annualized rate of occurrence, среднее количество инцидентов в год в соответствии со статистическими данными.

Значение SLE вычисляется как произведение расчетной стоимости актива и значения EF, т. е. $SLE = AssetValue * EF$. При этом в стоимость актива следует включать и штрафные санкции за его недостаточную защиту.

Значение ALE вычисляется как произведение SLE и ARO, т. е. $ALE = SLE * ARO$. Значение ALE позволяет проранжировать риски – риск с самым высоким ALE будет самым критичным. Далее рассчитанное значение ALE можно использовать для определения максимальной стоимости реализуемых мер защиты, учитывая общепринятый подход, что стоимость защитных мер не должна превышать стоимость актива или величину прогнозируемого ущерба, а расчетные затраты на атаку для злоумышленника должны быть меньше, чем ожидаемая им прибыль от реализации этой атаки. Ценность мер защиты также можно определить, вычтя из расчетного значения ALE до внедрения мер защиты значение расчетного значения ALE после внедрения мер защиты, а также вычтя ежегодные затраты на реализацию этих мер. Условно записать это выражение можно следующим образом:

Ценность мер защиты = ALE до внедрения мер защиты – ALE после внедрения мер защиты – Ежегодные затраты на реализацию мер защиты.

Примерами *качественного анализа* рисков могут быть, например, метод Дельфи, в котором проводится анонимный опрос экспертов в несколько итераций до достижения консенсуса, а также мозговой штурм и прочие примеры оценки («экспертный метод»).

Далее приведем краткий и неисчерпывающий список различных методологий риск-менеджмента, а самые распространенные рассмотрим подробно:

1. Фреймворк «NIST Risk Management Framework» на базе американских документов NIST (National Institute of Standards and Technology – Национального института стандартов и технологий, США) включает в себя набор взаимосвязанных так называемых специальных публикаций (англ. *Special Publication – SP*, для простоты изложения будем называть их стандартами):

1.1. Стандарт NIST SP 800-39 «Managing Information Security Risk» («Управление рисками информационной безопасности») предлагает трехуровневый подход к управлению рисками: организация, бизнес-процессы, информационные системы. Данный стандарт описывает методологию процесса управления рисками: определение, оценка, реагирование и мониторинг рисков.

1.2. Стандарт NIST SP 800-37 «Risk Management Framework for Information Systems and Organizations» («Фреймворк управления рисками для информационных систем и организаций») предлагает для обеспечения безопасности и конфиденциальности использовать подход управления жизненным циклом систем.

1.3. Стандарт NIST SP 800-30 «Guide for Conducting Risk Assessments» («Руководство по проведению оценки рисков»)

сфокусирован на ИТ, ИБ и операционных рисках. Он описывает подход к процессам подготовки и проведения оценки рисков, коммуницирования результатов оценки, а также дальнейшей поддержки процесса оценки.

1.4. Стандарт NIST SP 800-137 «Information Security Continuous Monitoring» («Непрерывный мониторинг информационной безопасности») описывает подход к процессу мониторинга информационных систем и ИТ-сред в целях контроля примененных мер обработки рисков ИБ и необходимости их пересмотра.

2. Стандарты Международной организации по стандартизации ISO (International Organization for Standardization):

2.1. Стандарт ISO/IEC 27005:2018 «Information technology – Security techniques – Information security risk management» («Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности») входит в серию стандартов ISO 27000 и является логически взаимосвязанным с другими стандартами по ИБ из этой серии. Данный стандарт отличается фокусировкой на ИБ при рассмотрении процессов управления рисками.

2.2. Стандарт ISO/IEC 27102:2019 «Information security management – Guidelines for cyber-insurance» («Управление информационной безопасностью. Руководство по киберстрахованию») предлагает подходы к оценке киберстраховки как меры обработки рисков, а также к оценке и взаимодействию со страховщиком.

2.3. Серия стандартов ISO/IEC 31000:2018 описывает подход к риск-менеджменту без привязки к ИТ/ИБ. В этой серии стоит отметить стандарт ISO/IEC 31010:2019 «Risk management – Risk assessment techniques», а также данный стандарт в его отечественном варианте ГОСТ Р ИСО/МЭК 31010–2011 «Менеджмент риска. Методы оценки риска».

3. Методология FRAP (Facilitated Risk Analysis Process) является относительно упрощенным способом оценки рисков, с фокусом только на самых критических активах. Качественный анализ при этом проводится с помощью экспертной оценки.

4. Методология OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) сфокусирована на самостоятельной работе членов производственных подразделений. Она используется для масштабной оценки всех информационных систем и производственных процессов организации.

5. Стандарт AS/NZS ISO 31000-2009 является австралийским и новозеландским стандартом с фокусом не только на ИТ-системах, но и на производственной успешности организации, т. е. предлагает более широкий подход к управлению рисками.

6. Методология FMEA (Failure Modes and Effect Analysis) предлагает проведение оценки системы с точки зрения ее слабых мест для поиска ненадежных элементов.

7. Методология CRAMM (Central Computing and Telecommunications Agency Risk Analysis and Management Method) предлагает использование автоматизированных средств для управления рисками.

8. Методология FAIR (Factor Analysis of Information Risk) – фреймворк для проведения количественного анализа рисков, предлагающий модель построения системы управления рисками на основе экономически эффективного подхода, принятия информированных решений, сравнения мер управления рисками, финансовых показателей и точных риск-моделей.

9. Концепция COSO ERM (Enterprise Risk Management) описывает пути интеграции риск-менеджмента со стратегией и финансовой эффективностью деятельности организации и акцентирует внимание на важности их взаимосвязи. В документе

описаны такие компоненты управления рисками, как стратегия и постановка целей, экономическая эффективность деятельности организации, анализ и пересмотр рисков, корпоративное управление и культура, а также информация, коммуникация и отчетность.

NIST Risk Management Framework

Рассмотрим набор документов.

Программная платформа – фреймворк управления рисками (Risk Management Framework) американского национального института стандартов и технологий (NIST). Данный институт выпускает документы по ИБ в рамках серии стандартов FIPS (Federal Information Processing Standards, Федеральные стандарты обработки информации) и рекомендаций SP (Special Publications, Специальные публикации) 800 Series.

Данная серия публикаций отличается логической взаимосвязанностью, детальностью, единой терминологической базой. Среди документов, касающихся управления рисками ИБ, следует отметить публикации NIST SP 800-39, 800-37, 800-30, 800-137 и 800-53/53a.

Создание данного набора документов явилось следствием принятия Федерального закона США об управлении информационной безопасностью (FISMA, Federal Information Security Management Act, 2002 г.) и Федерального закона США о модернизации информационной безопасности (FISMA, Federal Information Security Modernization Act, 2014 г.). Несмотря на декларируемую «привязку» стандартов и публикаций NIST к законодательству США и обязательность их исполнения для американских государственных органов, эти документы вполне можно рассматривать и как подходящие для любой организации, стремящейся улучшить управление ИБ, вне зависимости от юрисдикции и формы собственности.

NIST SP 800-39

Документ NIST SP 800-39 «Managing Information Security Risk: Organization, Mission, and Information System View» («Управление риском информационной безопасности: уровень организации, миссии, информационной системы») предлагает независимый от компании-поставщика, структурированный, гибкий подход к управлению рисками ИБ в контексте деятельности организации, ее активов и контрагентов. При этом риск-менеджмент должен быть целостным процессом, затрагивающим всю организацию, в которой практикуется риск-ориентированное принятие решений на всех уровнях. Управление риском определяется в данном документе как процесс, включающий в себя этапы определения (frame), оценки (assess), обработки (respond) и мониторинга (monitor) рисков. Рассмотрим указанные этапы подробнее.

1. На этапе определения рисков организации следует выявить:

– предположения о рисках, т. е. идентифицировать актуальные угрозы, уязвимости, последствия, вероятность возникновения рисков;

– ограничения рисков, возможности осуществления оценки, реагирования и мониторинга;

– риск-толерантность, т. е. терпимость к рискам – приемлемые типы и уровни рисков, а также допустимый уровень неопределенности в вопросах управления рисками;

– приоритеты и возможные компромиссы, т. е. нужно изучить компромиссы, на которые может пойти организация при обработке рисков, а также ограничения и факторы неопределенности, сопровождающие этот процесс.

2. На этапе оценки рисков организации следует выявить:

– угрозы ИБ, т. е. конкретные действия, лиц или сущности, которые могут являться угрозами для самой организации или могут быть направлены на другие организации;

– внутренние и внешние уязвимости, включая организационные уязвимости в производственных процессах управления организацией, архитектуре ИТ-систем и т. д.;

– ущерб организации с учетом вероятности реализации угроз;

– вероятность возникновения ущерба.

В итоге организация начинает понимать детерминанты риска, т. е. уровень ущерба и вероятность его возникновения для каждого риска. Для обеспечения процесса оценки рисков организация предварительно определяет:

– инструменты, техники и методологии, используемые для оценки риска;

– допущения и ограничения, которые могут повлиять на оценки рисков;

– роли и ответственность;

– способы проведения оценки рисков в организации;

– способы сбора, обработки и передачи информации об оценке рисков в пределах организации;

– частоту проведения оценки рисков;

– способы получения информации об угрозах (источники и методы).

3. На этапе реагирования на риск организация выполняет:

– разработку планов реагирования на риск;

– оценку планов реагирования на риск;

– определение планов реагирования на риск, допустимых с точки зрения риск-толерантности организации;

– реализацию принятых планов реагирования на риск.

Для обеспечения реагирования на риски организация определяет типы возможной обработки рисков (принятие, избегание, минимизация, разделение или передача риска), а также инструменты, технологии и методологии для разработки планов реаги-

рования, способы оценки планов реагирования и методы оповещения о предпринятых мерах реагирования в рамках организации и/или сторонних агентов.

На этапе мониторинга рисков решаются задачи:

– проверки реализации планов реагирования на риск и выполнения нормативных требований ИБ;

– определения эффективности мер реагирования на риски;

– оценки значимых для риск-менеджмента изменений в ИТ-системах и средах, включая спектр угроз, уязвимости, производственные функции и процессы, ИТ-инфраструктуру, взаимоотношения с другими организациями, риск-толерантность организации и т. д.

Организации описывают методы оценки нормативного соответствия и эффективности мер реагирования на риски, а также контроль изменений, способных повлиять на эффективность реагирования на риски.

Управление рисками ведется на уровнях организации, производственных процессов и информационных систем, при этом следует обеспечивать взаимосвязь и обмен информацией между указанными уровнями в целях непрерывного повышения эффективности осуществляемых действий.

На верхнем уровне организации осуществляется принятие решений по определению рисков, что напрямую влияет на процессы нижних уровней (производственных процессов и информационных систем), а также на финансирование этих процессов.

На уровне организации осуществляются выработка и внедрение функций управления, согласующихся с целями организации и с нормативными требованиями: создание функции риск-менеджмента, назначение ответственных, внедрение стратегии управления рисками и определение риск-толерантности, разработка и реализация инвестиционных стратегий в ИТ и ИБ.

На уровне производственных процессов происходят определение и создание риск-ориентированных производственных процессов и организационной архитектуры. Кроме того, на данном уровне осуществляется разработка архитектуры ИБ, которая обеспечит эффективное выполнение требований ИБ и внедрение всех необходимых мер и средств защиты.

На уровне информационных систем обеспечивается выполнение решений, принятых на более высоких уровнях, применительно к управлению рисками ИБ на всех этапах жизненного цикла систем: инициализация, разработка, внедрение, использование и вывод из эксплуатации.

Отметим, что в описании каждого из способов обработки рисков нужно указать, что в организации должна существовать как общая стратегия выбора способа обработки риска в той или иной ситуации, так и отдельные стратегии для каждого из способов обработки рисков.

Основные принципы обработки рисков:

1) принятие (*acceptance*) риска не должно противоречить стратегии риск-толерантности организации и ее возможности отвечать за возможные последствия этого;

2) избегание (*avoidance*) риска – зачастую самый надежный способ обработки рисков, но он может идти вразрез с необходимостью широкого применения нужных организациям ИТ-систем и технологий;

3) разделение (*share*) и передача (*transfer*) рисков – это соответственно частичное или полное разделение ответственности за последствия реализованного риска с внешними партнерами в соответствии с принятой стратегией, конечная цель которой – успешность функционирования организации;

4) смягчение (*mitigation*) рисков подразумевает применение стратегии минимизации рисков ИБ на всех трех уровнях.

Организации следует выстраивать производственные процессы в соответствии с принципами защиты информации, архитектурные решения, политики, процессы и средства ИБ должны быть достаточно универсальными и гибкими для применения их в динамичной и разнородной среде организации, с учетом непрерывно меняющегося спектра угроз ИБ.

NIST SP 800-37

«Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy» («Фреймворк управления рисками для информационных систем и организаций: жизненный цикл систем для обеспечения безопасности и конфиденциальности») обновлен в 2018 г., чтобы учесть современный спектр угроз и акцентировать внимание на важности управления рисками на уровне руководителей организации, подчеркнуть связь между программой управления рисками (Risk Management Framework, RMF) и программой кибербезопасности (Cybersecurity Framework, CSF), указать на важность интеграции процессов управления конфиденциальностью и управления рисками поставок (англ. *supply chain risk management, SCRM*), а также логически увязать список предлагаемых мер защиты с документом NIST SP 800-53. Выполнение положений NIST SP 800-37 можно использовать при проведении взаимной оценки процедур риск-менеджмента организаций в случаях, когда им требуется обмен данными или ресурсами. По аналогии с NIST SP 800-39 рассматривается управление рисками на уровнях организации, производственных процессов, информационных систем.

В NIST SP 800-37 указывается на важность разработки и внедрения возможностей по обеспечению безопасности и конфиденциальности в ИТ-системах на протяжении всего жизненного цикла (англ. *system development life cycle*, *SDLC*), непрерывной поддержки ситуационной осведомленности о со-

стоянии защиты ИТ-систем с применением процессов непрерывного мониторинга (*continuous monitoring*, *CM*) и предоставления информации руководству для принятия взвешенных риск-ориентированных решений. В RMF выделены следующие типы рисков: программный риск, риск несоответствия законодательству, финансовый риск, юридический риск, бизнес-риск, политический риск, риск безопасности и конфиденциальности, проектный риск, репутационный риск, риск безопасности жизнедеятельности, риск стратегического планирования.

Кроме этого, RMF:

– предоставляет повторяемый процесс для риск-ориентированной защиты информации и информационных систем;

– подчеркивает важность подготовительных мероприятий для управления безопасностью и конфиденциальностью;

– обеспечивает категоризацию информации и информационных систем, а также выбора, внедрения, оценки и мониторинга средств защиты;

– предлагает использовать средства автоматизации для управления рисками и мерами защиты в режиме реального времени, а также актуальные метрики для предоставления информации руководству для принятия решений;

– связывает процессы риск-менеджмента на различных уровнях и указывает на важность выбора ответственных за принятие защитных мер.

В документе указаны семь этапов применения RMF:

1. Определение целей и их приоритезация с точки зрения организации и ИТ-систем.

2. Категоризация систем и информации на основе анализа возможного негативного влияния в результате ее потери. NIST SP 800-30 также указывает три фактора при проведении оценки риска (угроза, уязвимость, вероятность события).

3. Выбор базовых мер защиты и их уточнение для снижения риска до приемлемого уровня.

4. Внедрение мер защиты и описание процедур их применения.

5. Оценка внедренных мер защиты для определения их корректности, работоспособности и результативности, удовлетворяющих требованиям безопасности и конфиденциальности.

6. Авторизация систем или мер защиты на основе заключения о приемлемости рисков.

7. Непрерывный мониторинг систем и примененных мер защиты для оценки их эффективности, изменений, проведения оценки рисков и анализа негативного их влияния, создания отчетов по состоянию безопасности и конфиденциальности.

В NIST SP 800-37 рассматриваются задачи, решаемые на каждом из этапов применения RMF. Для каждой из задач указывается ее название, перечисляются входные и выходные данные процесса, приводится перечень ответственных и вспомогательных ролей, даются ссылки на связанные документы NIST.

Задачи этапа **«Подготовка»** на уровне *организации*:

– определение ролей для управления рисками;

– создание стратегии управления рисками, с учетом риск-толерантности организации;

– проведение оценки рисков;

– выбор целевых значений мер защиты из Cybersecurity Framework;

– приоритезация ИТ-систем;

– определение для ИТ-систем общих мер защиты, которые могут быть унаследованы с более высоких уровней (например, с уровня организации или производственных процессов);

– разработка и внедрение непрерывного мониторинга эффективности мер защиты.

Задачи этапа **«Подготовка»** на *уровне ИТ-систем* в себя:

– определение производственных функций и процессов, которые поддерживает каждая ИТ-система;

– идентификация лиц, заинтересованных в создании, внедрении, оценке, функционировании, поддержке, выводе из эксплуатации систем;

– определение активов, требующих защиты;

– определение границы авторизации для системы;

– выявление типов информации, обрабатываемых/передаваемых/хранимых в системе;

– идентификация и анализ жизненного цикла всех типов информации, обрабатываемых/передаваемых/хранимых в системе;

– проведение оценки рисков на уровне ИТ-систем и обновление результатов оценки;

– определение требований по безопасности и конфиденциальности для систем и сред функционирования;

– определение местоположения систем в общей архитектуре организации;

– формальная регистрация ИТ-систем в соответствующих департаментах и документах.

Задачи этапа **«Категоризация»**:

– документирование характеристик системы;

– категоризация системы и документирование результатов категоризации по требованиям безопасности;

– пересмотр и согласование результатов и решений по категоризации по требованиям безопасности.

Задачи этапа **«Выбор набора мер защиты»**:

– выбор мер защиты для системы и среды ее функционирования;

– уточнение (адаптация) выбранных мер защиты для системы и среды ее функционирования;

– распределение точек применения мер обеспечения безопасности и конфиденциальности к системе и среде ее функционирования;

– документирование мер обеспечения безопасности и конфиденциальности системы и среды ее функционирования в соответствующих планах;

– создание и внедрение мониторинга эффективности применяемых мер защиты, которая логически связана с общей организационной стратегией мониторинга и дополняет ее;

– пересмотр и согласование планов обеспечения безопасности и конфиденциальности системы и среды ее функционирования.

Задачи этапа **«Внедрение мер защиты»**:

– внедрение мер защиты в соответствии с планами обеспечения безопасности и конфиденциальности;

– документирование изменений в запланированные меры защиты на основании реальных результатов.

Задачи этапа **«Оценка внедренных мер защиты»**:

– выбор команды, соответствующей типу проводимой оценки;

– разработка, пересмотр и согласование планов по оценке мер защиты;

– проведение оценки мер защиты в соответствии с процедурами, описанными в планах;

– подготовка отчетности, содержащей найденные недостатки и рекомендации по их устранению;

– выполнение корректирующих действий по мерам защиты и переоценку скорректированных мер;

– подготовка плана действий на основании найденных недостатков и рекомендации из отчетов.

Задачи этапа **«Авторизация»**:

– сбор пакета документов и отправку его на авторизацию;

– анализ и определение риска использования системы или применения мер защиты;

– определение и внедрение плана действий при реагировании на выявленный риск;

– определение приемлемости риска использования системы и применения мер защиты;

– сообщение о результатах авторизации и о недостатках мер защиты, представляющим значительный риск для безопасности или конфиденциальности.

Задачи этапа **«Непрерывный мониторинг»**:

– мониторинг информационной системы и среды ее функционирования на наличие изменений, которые влияют на состояние безопасности и конфиденциальности системы;

– оценка мер защиты в соответствии со стратегией непрерывного мониторинга;

– реагирование на риск на основе результатов непрерывного мониторинга, оценок риска, плана действий;

– обновление планов, отчетов по оценке, планов действий на основании результатов непрерывного мониторинга;

– сообщение о состоянии безопасности и конфиденциальности системы соответствующему должностному лицу в соответствии со стратегией непрерывного мониторинга;

– пересмотр состояния безопасности и конфиденциальности системы для определения приемлемости риска;

– разработка стратегии вывода системы из эксплуатации и выполнение соответствующих действий при окончании срока ее службы.

NIST SP 800-30

«Guide for Conducting Risk Assessments» («Руководство по проведению оценок риска») посвящен процедуре оценки риска, которая является важнейшим компонентом процесса управ-

ления в организации в соответствии с NIST SP 800-39, наряду с определением, обработкой и мониторингом.

Процедуры оценки рисков используются для идентификации, оценки и приоритезации рисков, порождаемых использованием информационных систем, для операционной деятельности организации, ее активов и работников.

Целями оценки рисков являются информирование лиц, принимающих решения, и поддержка процесса реагирования на риск путем идентификации:

– актуальных угроз как самой организации, так и опосредованно другим организациям;

– внутренних и внешних уязвимостей;

– потенциального ущерба организации с учетом возможностей использования уязвимостей угрозами;

– вероятности возникновения ущерба.

Конечным результатом является вычисление значения риска от его вероятности и размера ущерба. Оценка производится на всех трех уровнях управления рисками (организации, производственных процессов, информационных систем) по аналогии с подходом, применяемым в NIST SP 800-39 и NIST SP 800-37.

Оценка рисков – это непрерывный процесс, затрагивающий все уровни управления рисками в организации, проводимый с частотой, соответствующей целям и объему оценки.

Процесс оценки рисков включает:

– подготовку к оценке;

– проведение оценки;

– передачу информации об оценке внутри организации;

– поддержание и развитие достигнутых результатов.

В указанном документе говорится о важности формирования методологии оценки рисков. Указано, что организация может

выбрать одну или несколько методологий оценки в зависимости от имеющихся ресурсов, сложности и зрелости производственных процессов, критичности/важности обрабатываемой информации. Создание корректной методологии повышает качество и воспроизводимость реализуемых оценок риска. Методология оценки риска включает:

– описание процесса оценки;

– модель, описывающую оцениваемые факторы риска и взаимосвязи между ними;

– способ оценки (например, качественный или количественный), описывающий значения, которые могут принимать факторы риска;

– способ анализа, описывающий, как учитываются комбинации факторов риска.

Модель рисков описывает оцениваемые факторы риска и взаимосвязи между ними.

Факторы риска – это характеристики, используемые в моделях риска в качестве входных данных для определения уровней рисков при проведении их оценки. Кроме этого, факторы риска используются для выделения тех из них, которые ощутимо влияют на уровни рисков в определенных ситуациях и контекстах.

При этом некоторые факторы риска могут быть декомпозированы до более детальных характеристик, например, угрозы можно декомпозировать до источников угроз (англ. *threat sources*) и событий угроз (англ. *threat events*).

Угроза – это любое обстоятельство или событие, имеющее потенциал негативного влияния на производственные процессы или активы организации, сотрудников, другие организации путем осуществления несанкционированного доступа, разрушения, разглашения или модификации информации и/или отказа в обслуживании.

Источником угроз может быть намеренное действие, направленное на использование уязвимости, или ненамеренное действие, в результате которого уязвимость проэксплуатирована случайно.

Среди источников можно назвать:

– враждебные кибератаки или физические атаки;

– человеческие ошибки;

– структурные ошибки в активах, подконтрольных организации;

– природные, антропогенные и техногенные аварии или катастрофы.

Детальность определения событий угроз зависит от глубины построения модели рисков. В случае детального рассмотрения модели рисков можно строить сценарии угроз, которые являются набором из нескольких событий, приводящих к негативным эффектам, привязанных к определенному источнику (источникам) угроз и упорядоченных по времени; при этом рассматривается потенциальная вероятность последовательной эксплуатации нескольких уязвимостей, приводящей к успешной реализации атаки. События угроз в кибер- или физических атаках характеризуются набором тактик, техник и процедур (англ. *tactics, techniques, and procedures, TTPs*), о которых говорилось ранее.

Рассматриваемый документ также говорит о таком понятии, как *«смещение угрозы»* (англ. *threat shifting*), под которым понимается изменение атакующими своих TTPs в зависимости от мер защиты, предпринятых организацией и выявленных атакующими. Смещение угрозы может быть осуществлено во временном смысле (например, попытки атаковать в другое время или растянуть атаку во времени), в целевом отношении (например, выбор менее защищенной цели), ресурсном плане (например, использование атакующими дополнительных ресурсов для взлома цели), методах планирования или атаки (например, использова-

ние другого хакерского инструментария или попытки атаковать иными методами).

Кроме этого, нужно учитывать, что атакующие зачастую для достижения своих целей предпочитают путь наименьшего сопротивления, т. е. выбирают самое слабое звено в цепи защиты.

Уязвимость – это слабость в информационной системе, процедурах обеспечения безопасности, внутренних способах защиты или в особенностях конкретной реализации/внедрения той или иной технологии или системы.

Уязвимость характеризуется опасностью в контексте возможности ее исправления; при этом опасность может быть определена в зависимости от ожидаемого негативного эффекта от эксплуатации этой уязвимости.

Большинство уязвимостей в информационных системах организации возникают или из-за не примененных (случайно или нарочно) мер ИБ, или некорректно примененных. Важно помнить и об эволюции угроз и самих защищаемых систем – и в тех, и в других со временем происходят изменения, которые следует учитывать при проведении переоценки рисков. Кроме уязвимостей технического характера в ИТ-системах, следует учитывать и ошибки в управлении организацией и в архитектуре систем.

Предварительное условие (англ. *predisposing condition*) в контексте оценки рисков – это условие, существующее в бизнес-процессе, архитектуре или ИТ-системе, из-за угрозы влияющее (снижающее или увеличивающее) на вероятность причинения ущерба.

Логическими синонимами являются термины «подверженность» (англ. *susceptibility*) или «открытость» (англ. *exposure*) риску, означающие, что уязвимость может быть использована для нанесения ущерба. Например, SQL-сервер потенциально подвержен уязвимости SQL-инъекции.

Кроме технических предварительных условий, следует учитывать и организационные: так, местоположение офиса в низине увеличивает риск подтопления, а отсутствие коммуникации между сотрудниками при разработке ИТ-системы увеличивает риск ее взлома.

Вероятность возникновения угрозы (англ. *likelihood of occurrence*) – показатель того, что определенная уязвимость (или группа уязвимостей) может быть использована причинения реального ущерба.

Для намеренных угроз оценка вероятности возникновения обычно оценивается на основании намерений, возможностей и целей злоумышленника. Для ненамеренных угроз оценка вероятности возникновения, как правило, зависит от эмпирических и исторических данных.

При этом вероятность возникновения оценивается на определенную временную перспективу – например, на следующий год или на отчетный период.

При оценке вероятности возникновения угрозы следует учитывать состояние управления и бизнес-процессов организации, предварительные условия, наличие и эффективность имеющихся мер защиты. Вероятность негативного влияния означает возможность того, что при реализации угрозы будет нанесен какой-либо ущерб. При определении общей вероятности возникновения угроз используют три этапа:

1. Оценка вероятности того, что угроза будет кем-либо инициирована (в случае намеренной угрозы) или случится само (в случае ненамеренной).

2. Оценка вероятности того, что возникшая угроза приведет к ущербу или нанесет вред организации, активам, сотрудникам.

3. Общая вероятность рассчитывается как комбинация первых двух полученных оценок.

В документе дается рекомендация не искать абсолютно все взаимосвязанные угрозы и уязвимости, а сконцентрироваться на тех из них, которые действительно могут быть использованы в атаках, а также на бизнес-процессах и функциях с недостаточными мерами защиты.

Уровень негативного влияния (англ. *impact*) события угрозы – это величина ущерба, который ожидается от несанкционированного разглашения, доступа, изменения, утери информации или недоступности информационных систем. Организации явным образом определяют:

1. Процесс, используемый для определения негативного влияния.

2. Предположения и обоснования, используемые для определения негативного влияния.

3. Источники и методы получения информации о негативном влиянии.

Кроме этого, при расчете негативного влияния организации должны учитывать ценность активов и информации: можно использовать принятую в компании систему категорирования информации по уровням значимости или результаты оценок негативного влияния на конфиденциальность.

При оценке рисков важным фактором является *степень неопределенности* (англ. *uncertainty*), которая возникает из-за естественных ограничений:

– невозможность точно спрогнозировать будущие события; недостаточность сведений об угрозах;

– неизвестные уязвимости;

– нераспознанные взаимозависимости.

С учетом вышесказанного, **модель риска** можно описать как следующую логическую структуру: *источник угрозы* (с определенными характеристиками) с определенной *вероятностью*

инициирует *угрозу*, которая использует *уязвимость* (несущую определенную опасность, с учетом предварительных условий и успешного обхода защитных мер), вследствие чего создается *негативное влияние* (зависящее от размера и вероятности возникновения ущерба), которое порождает *риск*.

Документ дает рекомендации по использованию процесса *агрегирования рисков* (англ. *risk aggregation*) в целях объединения нескольких разобщенных или низкоуровневых рисков в один более общий: например, риски отдельных ИТ-систем могут быть агрегированы в общий риск для всей поддерживаемой ими бизнес-системы.

При таком объединении следует учитывать то, что некоторые риски могут реализовываться одновременно или чаще, чем это прогнозировалось. Также следует учитывать взаимосвязи между разобщенными рисками их надо либо объединять либо разъединять.

В NIST SP 800-30 также описаны основные *способы оценки рисков*:

– количественный (англ. *quantitative*);

– качественный (англ. *qualitative*);

– полуколичественный (англ. *semi-quantitative*).

Количественный анализ оперирует конкретными цифрами (стоимостью, временем простоя, затратами и т. д.) и лучше всего подходит для проведения анализа выгод и затрат (англ. *cost-benefit analysis*), однако является достаточно ресурсоемким.

Качественный анализ применяет описательные характеристики (например, высокий, средний, низкий), что может привести к некорректным выводам ввиду субъективности выставления оценок.

Полуколичественный способ является промежуточным вариантом, предлагающим использовать больший диапазон возможных оценок (например, по шкале от 1 до 10) для более точной

оценки и анализа результатов сравнения. Применение конкретного способа оценки рисков зависит как от сферы деятельности организации (например, в банковской сфере может применяться более строгий количественный анализ), так и от стадии жизненного цикла системы (например, на начальных этапах цикла может проводиться только качественная оценка рисков, а на более зрелых – уже количественная).

Наконец, в документе описаны три основных *способа анализа* факторов рисков:

– угрозоцентричный (англ. *threat-oriented*);

– ориентированный на активы (англ. *asset/impact-oriented*);

– уязвимости (англ. *vulnerability-oriented*).

Угрозоцентричный способ сфокусирован на создании сценариев угроз и начинается с определения источников угроз и событий угроз; далее, уязвимости идентифицируются в контексте угроз, а негативное влияние связывается с намерениями злоумышленника.

Способ, *ориентированный на активы*, подразумевает выявление событий угроз и источников угроз, способных оказать негативное влияние на активы; во главу угла ставится потенциальный ущерб активам.

Применение способа, *ориентированного на уязвимости*, начинается с анализа предварительных условий и недостатков/слабостей, которые могут быть использованы; далее определяются возможные события угроз и последствия использования найденных уязвимостей.

Документ содержит рекомендации по комбинированию описанных способов анализа для получения более объективной картины угроз при оценке рисков.

Итак, по NIST SP 800-30 процесс оценки рисков разбивается на четыре шага:

– подготовка к оценке рисков;

– проведение оценки рисков;

– коммуницирование результатов оценки и передача информации внутри организации;

– поддержание достигнутых результатов.

Рассмотрим подробнее задачи, выполняемые на каждом из этапов:

1. **Подготовка к оценке рисков**:

1.1. Идентификация цели оценки рисков: какая информация ожидается в результате оценки, какие решения будут продиктованы результатом оценки.

1.2. Идентификация области оценки рисков в контексте применимости к конкретной организации, временному промежутку, архитектуре и используемых технологиях.

1.3. Идентификация ограничений, с учетом которых проводится оценка рисков. В рамках этой подзадачи определяются ограничения в таких элементах, как источники угроз, события угроз, уязвимости, предварительные условия, вероятность возникновения, негативное влияние, риск-толерантность и уровень неопределенности, а также выбранный способ анализа.

1.4. Идентификация источников предварительной информации, источников угроз и уязвимостей, а также информации о негативном влиянии, которая используется в оценке рисков. В этом процессе источники информации могут быть как внутренними (такими, как отчеты по инцидентам и аудитам, журналы безопасности и результаты мониторинга), так и внешними (например, отчеты CERT, результаты исследований и прочая релевантная общедоступная информация).

1.5. Идентификация модели рисков, способа оценки рисков и подхода к анализу, которые используются в оценке рисков.

2. **Проведение оценки рисков**:

2.1. Идентификация и описание актуальных источников угроз, включая возможности, намерения и цели намеренных угроз, а также возможные эффекты от ненамеренных угроз.

2.2. Идентификация потенциальных событий угроз, релевантности этих событий, а также источников угроз, которые могут инициировать события угроз.

2.3. Идентификация уязвимостей и предварительных условий, которые влияют на вероятность того, что актуальные события угроз приведут к негативному влиянию. Ее целью является определение того, насколько рассматриваемые бизнес-процессы и информационные системы уязвимы перед идентифицированными ранее источниками угроз и насколько идентифицированные события угроз действительно могут быть инициированы этими источниками угроз.

2.4. Определение вероятности того, что события угроз приведут к негативному влиянию с учетом характеристик источников угроз, уязвимостей и предварительных условий, а также подверженности организации этим угрозам, принимая во внимание внедренные меры защиты.

2.5. Определение негативного влияния, порожденного реализацией угроз, с учетом характеристик их источников, уязвимостей и предварительных условий, а также подверженности организации этим угрозам, принимая во внимание внедренные меры защиты.

2.6. Определение риска при реализации угроз, принимая во внимание уровень негативного влияния и вероятность наступления событий. В Приложении к данному стандарту приведена таблица для расчета уровня риска в зависимости от вероятности и негативного влияния.

3. **Коммуницирование результатов оценки рисков и передача информации**:

3.1. Коммуницирование результатов оценки рисков лицам, принимающим решения, для реагирования на риски.

3.2. Передача заинтересованным лицам информации, касающейся рисков, выявленных в результате оценки.

4. **Поддержание достигнутых результатов**:

4.1. Проведение непрерывного мониторинга факторов риска, которые влияют на риски в операционной деятельности организации, на ее активы, сотрудников, другие организации. Данной подзадаче посвящен стандарт NIST SP 800-137.

4.2. Актуализация оценки рисков с использованием результатов непрерывного мониторинга факторов риска.

Документ NIST SP 800-30 предлагает достаточно детальный подход к моделированию угроз и расчету рисков. Ценными являются приложения к данному стандарту, содержащие примеры расчетов по каждой из подзадач оценки рисков, а также перечни возможных источников угроз, событий угроз, уязвимостей и предварительных условий.

NIST SP 800-137

Документ NIST SP 800-137 «Information Security Continuous Monitoring for Federal information Systems and Organizations» («Непрерывный мониторинг информационной безопасности для федеральных информационных систем и организаций»).

Задачей непрерывного мониторинга информационной безопасности является оценка эффективности мер защиты и статуса безопасности систем с целью реагирования на постоянно меняющиеся вызовы и задачи в сфере информационной безопасности.

Система непрерывного мониторинга ИБ помогает предоставлять ситуационную осведомленность о состоянии безопас-

ности информационных систем на основании информации, собранной из различных ресурсов (активы, процессы, технологии, сотрудники), а также об имеющихся возможностях по реагированию на изменения ситуации. Данная система является одной из тактик в общей стратегии управления рисками.

В данной публикации приведен рекомендуемый процессный подход к выстраиванию системы мониторинга ИБ, состоящий:

– из определения стратегии непрерывного мониторинга ИБ (включает в себя выстраивание стратегии на уровне организации, бизнес-процессов и информационных систем; назначение ролей и ответственных; выбор тестового набора систем для сбора данных);

– разработки программы непрерывного мониторинга ИБ (включает определение метрик для оценки и контроля; выбор частоты проведения мониторинга и оценки; разработку архитектуры системы мониторинга);

– внедрения программы непрерывного мониторинга ИБ;

– анализа найденных недостатков и отчета о них (включает анализ данных; отчетность по оценке мер защиты; отчетность по мониторингу статуса защиты);

– реагирования на выявленные недостатки;

– модернизации стратегии и программы непрерывного мониторинга ИБ.

В документе даются следующие рекомендации по выбору инструментов обеспечения непрерывного мониторинга ИБ:

– поддержка ими большого количества источников данных;

– использование открытых и общедоступных спецификаций (например, SCAP – Security Content Automation Protocol);

– интеграция с другим ПО, таким как системы Help Desk, системы управления инвентаризацией и конфигурациями, системами реагирования на инциденты;

– поддержка процесса анализа соответствия законодательным нормам;

– гибкий процесс создания отчетов, возможность усиливать глубину рассматриваемых данных;

– поддержка систем Security Information and Event Management (SIEM) и систем визуализации данных.

Международная организация по стандартизации ISO (ИСО) и Международная электротехническая комиссия IEC (МЭК) формируют специализированную систему всемирной стандартизации. На текущий момент можно утверждать, что мировое сообщество проделало существенную работу в направлении стандартизации СУИБ и отдельных процессов управления ИБ и по-прежнему весьма активно продолжает эту работу. В соответствии с разработанными 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 текущего состояния, использование методик (с 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 принята 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 действия и т. д.

2.2. 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 77991:1999) 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 77992:1999 «Information Security Management. Specification for ISMS» для СУИБ (Information Security Management System). В 2002 г. стандарт усовершенствован, и выпущена его новая редакция BS 77992:2002. На ее основе в 2005 г. 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/1EC 27001:2005, они представляют руководства по управлению ИБ для различных сфер деятельности, включая финансовый и страховой сектор, здравоохранение, телекоммуникации и т. д.

С 2012 г. существуют международные стандарты серии 27000 (табл. 2.1).

Что касается собственно российских стандартов по управлению ИБ, то сначала приняты стандарт ГОСТ Р ИСО/МЭК 17799–2005, идентичный ISO/IEC 17799:2000 и актуализированный 1 января 2008 г., и стандарт ГОСТ Р ИСО/МЭК 27001–2006, идентичный ISO/IEC 27001:2005. После некоторого перерыва приняты национальные стандарты, идентичные 27006, 27005, 27004 и 270331. В настоящее время российская стандартизация в области управления ИБ проходит промежуточную стадию формирования и является еще недостаточно совершенной.

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 1SO/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

Продолжение табл. 2.1

27008:2011	Руководство по аудиту средств управления ИБ, реализованных в СУИБ
27010	Управление ИБ при коммуникации между секторами (в нескольких частях, представляющих 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)
27011:2008	Руководство по управлению ИБ для телекоммуникационных компаний на основе ISO/IEC 27002
27013	Руководство по интегрированному внедрению ISO 20000 и ISO 27001
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
27033-1:2009	Безопасность сетей. Часть 1. Общие положения и концепции
27033-2	Руководство по проектированию и внедрению системы обеспечения безопасности сетей
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 JP-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

Окончание табл. 2.1

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
27034-6	Руководство по обеспечению безопасности конкретных приложений
27035:2011	Управление инцидентами безопасности (заменит ISO/IEC TR 18044)
27036	Руководство по аутсорсингу безопасности
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

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

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 JT-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 представляет более дидактический подход для организаций, внедряющих у себя СУИБ.

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

Агентство разработало и регулярно обновляет четыре стандарта в области ОИБ [16; 19]:

– BSI-Standard 100-1 «Information Security Management Systems», который содержит общие требования к СУИБ;

– BSI-Standard 100-2 «IT-Grundschutz Methodology», освещающий вопросы поэтапного построения СУИБ и ее дальнейшего использования на практике и содержащий 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 политики ИБ и выбору защитных мер, а также рассматриваются сопровождение и усовершенствование деятельности по ОИБ в повседневной практике организации;

– BSI-Standard 100-3 «Risk Analysis based on IT-Grundschutz», посвященный анализу рисков ИБ на основе методики IT-Grundschutz;

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

Кроме того, BSI составило сборник IT-Grundschutz Catalogues (Каталог 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.

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]. Главная 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. 2.1); 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.

В ISO/IEC 27000:2009 СУИБ определяется как часть общей системы управления, основанная на использовании методов

оценки производственных рисков для разработки, внедрения, функционирования, мониторинга, анализа, сопровождения (поддержания) и совершенствования ИБ.

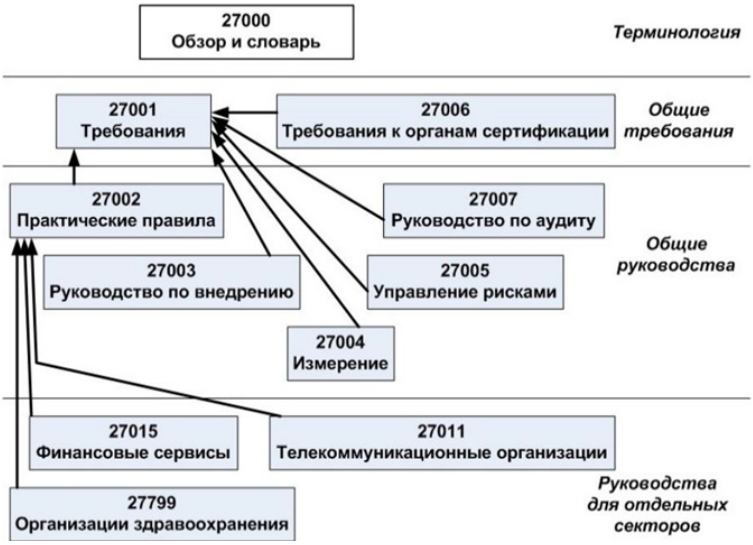

Рис. 2.1. Логическая взаимосвязь стандартов серии 27000

Далее уточняется, что СУИБ определяет модель защиты информационных активов организации для достижения ее производственных 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 производственных 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 учтены основные положения следующих документов: ISO/IEC Guide2:1996 «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.

ISO/IEC 27001:2005 и ГОСТ Р ИСО/МЭК 27001–2006. Требования к СУИБ

Международный стандарт ISO/IEC 27001:2005 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. 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). Применение этого стандарта позволяет на основе процессного подхода управлять конфиденциальностью, целостностью и доступностью важного актива

компании. Стандарт может с одинаковым успехом использоваться 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 организации и, что немаловажно, информацию, принадлежащую ее партнерам/клиентам, все, что является значимым информационным активом, и все, 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 производственные цели, используемые производственные процессы, а также ее структура и размер, что, в свою очередь, ведет к выработке конкретных требований по обеспечению безопасности в широком смысле ее понимания. СУИБ объединяет людей, процессы и ИТ-системы, а также обеспечивает согласованную работу службы безопасности, ИТ-отдела и руководства организации.

При использовании СУИБ реализуется системный подход к управлению «чувствительной» для организации информацией с целью обеспечения ее конфиденциальности, целостности

и доступности. В связи с этим особую значимость приобретают факторы:

– понимания требований по ОИБ организации и необходимости установления политики и целей ИБ;

– внедрения и использования мер для управления рисками ИБ наряду с общими производственными рисками организации;

– мониторинг и проверка производительности и эффективности СУИБ;

– непрерывное улучшение СУИБ, основанное на результатах объективных измерений.

В период с 2005 по 2011 г. более семи тысяч организаций во всем мире успешно прошли официальные процедуры сертификации СУИБ по требованиям ISO/IEC 27001:2005 и сотни тысяч организаций активно внедряют международные стандарты серии 27000 без прохождения официальных процедур сертификации. Сертифицируя СУИБ на соответствие стандарту ISO/IEC 27001:2005, организация демонстрирует применение проверенного международными компаниями методологического подхода к ОИБ, показывает 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.

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 [22]

разработан на базе первой части британского стандарта 7799, который предназначен для управления ИБ организации вне зависимости от сферы ее деятельности.

В России стандарт 1SO/IEC 17799 начал активно применяться в области управления ИБ, начиная с 20 января 2004 г. В 2005 г. принят ГОСТ Р ИСО/МЭК 17799–2005, идентичный 17799:2000, содержащий десять основных разделов (ПолИБ; организационные вопросы безопасности; классификация и управление процессами безопасности, связанные с персоналом; физическая защита от воздействий окружающей среды; управление передачей данных и операционной деятельностью; контроль доступа; управление непрерывностью производства). После введения в действие этот стандарт актуализирован и переиздан в 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 таких требований к информации, как конфиденциальность, целостность, доступность, аутентичность.

В последней редакции стандарта 17799 определяются следующие направления управления ИБ:

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

– ПолИБ (определяются требования к поддержке заданной ИБ; описываются некоторые новые стандарты, руководящие принципы и процедуры в области ОИБ);

– организация защиты (управление ИБ при взаимодействии с объектами);

– управление активами (обеспечение защиты активов организации);

– безопасность персонала (снижение риска человеческих ошибок и преднамеренных нарушений, а также средства управления ПолИБ со стороны пользователей, их обучение вопросам ИБ);

– физическая защита и защита от воздействия окружающей среды (предотвращение несанкционированного доступа, изменения, кражи и повреждения средств защиты и информации при физическом доступе; также рассматриваются системы вентиляции, пожаротушения, водоснабжения и электропитания);

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

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

– приобретение, развитие и сопровождение ИС (обеспечение выполнения функций защиты информации в операционных системах и приложениях на всех стадиях их жизненного цикла);

– управление инцидентами ИБ (включая планирование, идентификацию, реагирование и сохранение собранной информации, устранение последствий);

– управление непрерывностью производства организации (обеспечение защиты критически важных производственных

процессов от сбоев и нарушений на основе повышения их устойчивости и восстановления после сбоев и аварий);

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

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

ISO/IEC 27003:2010. Руководство по внедрению СУИБ

Стандарт ISO/IEC 27003:2010 «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 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.

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 план внедрения проекта СУИБ в организации.

Данный стандарт описывает процесс разработки спецификации и проектирования СУИБ, 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, в том числе:

– по проектированию СУИБ;

– проектированию организации ОИБ;

– проектированию защиты ИТ и физической безопасности;

– учету других аспектов использования СУИБ;

– разработке 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.

ISO/IEC 27004:2009

Стандарт «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 представления единого руководства по применению механизмов оценки в результате измерений. На основе полученных показателей, их анализа и принятия соответствующих решений по устранению выявленных проблем организациям удастся повысить результативность функционирования СУИБ. Эта информация крайне важна для обоснования решений, связанных с СУИБ, в том числе для ее дальнейшего совершенствования.

С начала 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 по 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 и усовершенствования процессов или средств управления СУИБ.

ГОСТ Р ИСО/МЭК 27004–2011содержит разделы:

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

– обязанности руководства;

– разработка процедуры измерений (процессов отбора показателей и сбора информации);

– процесс измерений;

– анализ данных и отчет по результатам измерений;

– оценивание и совершенствование 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 процедур 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). Для проведения данных мероприятий необходима разработка программы измерений, связанных с ИБ. Полученные результаты

позволят выявить прогресс (или отсутствие такового) в достижении целей ОИБ за некоторый период времени как одного из элементов совершенствования СУИБ организации.

Стандарт содержит достаточно детальное описание процессов измерения, использования операции агрегирования результатов измерений, применения аналитических методов и методов принятия решений для выявления «индикаторов» совершенствования СУИБ. В стандарте не указывается, какие основные и производные измерения 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 определенных методов, аналитических моделей и критериев принятия решений.

Механизмы, описанные в стандарте, применимы к различным организациям с разными СУИБ. Подход организации к выполнению требований относительно измерений, определенных в ISO/IEC 27001, зависит от целого ряда факторов, включая риски ИБ, величину организации, имеющиеся ресурсы и применимые правовые, нормативные и договорные требования. В идеальном случае деятельность, связанная с постоянными измерениями, должна быть интегрирована в обычную деятельность организации с привлечением минимальных ресурсов.

Для организаций небольшого размера измерений может быть немного, и для них необходимо разработать одну программу измерений, в то время как для крупных организаций таких программ может быть 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.

ISO/IEC 27005:2011 и ГОСТ Р ИСО/МЭК 27005–2010. Управление рисками ИБ

Стандарт ISO/IEC 27005:2011 «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 производственным 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 уже завершивших свое действие стандартах ISO/IEC 133353:1998 [27] и 133351:2000 [28], связанных с управлением безопасностью ИТТ.

Вторая редакция этого стандарта гармонизирована с ISO/IEC 27000:2009 [20]. Считается, что ISO/IEC 27005:2011 разработан на основе британского стандарта BS 77993:2006 «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 77993:2006 носит концептуальный характер, что позволяет экспертам по ИБ реализовать любые методы, средства и технологии оценки, обработки и управления рисками ИБ. Стандарт не содержит рекомендаций по выбору какого-либо аппарата оценки риска ИБ, а также по разработке мер, средств и сервисов защиты, используемых для минимизации рисков ИБ. BS 77993:2006 допускает использование как количественных, так и качественных методов оценки рисков ИБ, но, к сожалению,

в документе нет рекомендаций по выбору конкретного математического и методического аппарата оценки рисков ИБ.

Стандарт BS 77993:2006 придерживается самого общего понятия риска ИБ, под которым понимается комбинация вероятности события и стоимости компрометируемого ресурса. Управление риском ИБ сформулировано как скоординированные непрерывные действия по управлению рисками и их контроля в организации. Процесс управления делится на четыре фазы:

1) оценка рисков ИБ, включающая анализ и вычисление рисков;

2) обработка рисков ИБ – выбор и реализация мер и средств защиты;

3) контроль рисков ИБ путем мониторинга, тестирования, анализа механизмов безопасности и аудита ИБ системы;

4) 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 выбор законодательных и нормативных требований безопасности, отмечает необходимость использования принципа осведомленности о процессах оценки, контроля и оптимизации рисков ИБ в организации и многое другое. На каждом этапе 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 77993:2006 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 и рисков, декларации применимости, списки проверок, протоколы процедур и тестов, журналы безопасности, аудиторские отчеты, планы коммуникаций, инструкции, регламенты и т. п.

С 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 1SO/IEC 27005:2008 и заменяющий ГОСТ Р ИСО/МЭК ТО 133353–2007 «Методы менеджмента безопасности информационных технологий» и ГОСТ Р ИСО/МЭК ТО 133354–2007 «Выбор защитных мер».

В целом ГОСТ Р ИСО/МЭК 27005–2010 носит описательный характер и не содержит 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 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 разделов:

– обзор процесса управления рисками ИБ как непрерывного процесса;

– установление контекста управления рисками ИБ;

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

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

– принятие рисков ИБ;

– коммуникация рисков ИБ;

– 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 ни одному из них не отдается предпочтение. Однако 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 и обработка рисков ИБ, остаточные риски ИБ.

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

ISO/IEC 27006:2011 и ГОСТ Р ИСО/МЭК 27006–2008. Требования к органам, осуществляющим аудит и сертификацию СУИБ

Стандарт ISO/IEC 27006:2011 «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 руководство по процессам сертификации аккредитованными для этого органами и в первую очередь предназначен для поддержки аккредитации органов сертификации СУИБ. Стандарт ISO 17026, упомянутый как нормативная ссылка в ISO/IEC 27006:2011, недавно обновлен, поэтому требуется 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» идентичен более ранней редакции международного стандарта ISO/IEC 27006:2007, введен в действие в России с 2009 г. [33].

Цель ГОСТ Р ИСО/МЭК 27006–2008 – установить общие требования к сертификации или регистрации СУИБ организаций, чтобы быть признанными надежными для выполнения за-

явленных 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 170211 «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, 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 разделы:

– принципы;

– общие требования (правовые и договорные вопросы, обязательства и финансирование);

– требования к структуре;

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

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

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

– требования системы управления к органам сертификации.

В приложениях приведены анализ сложности сертифицируемых организаций и их областей деятельности, примеры компетенций аудиторов, продолжительность аудитов, руководство по анализу реализованных мер управления на основе ISO/IEC 27001:2005.

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 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по аудиту систем менеджмента ИБ» [34] содержит руководство для аккредитованных органов сертификации, внутренних аудиторов, внешних аудиторов 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 соответствие 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 пересмотренном к настоящему времени стандарте ISO 19011:2002, содержащем руководящие указания по аудиту систем менеджмента качества и систем менеджмента окружающей среды, и стандарте ISO 170212 «Оценка соответствия. Требования к сертификационному аудиту систем управления, проводимому 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 использован соответствующий подход оценки рисков ИБ;

– исследование результатов оценки рисков ИБ;

– проверка того, что 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.

В ISO/IEC 27007:2011 рассматриваются принципы аудита, управление программой аудита (включая постановку задач, определение ответственности, необходимых ресурсов и процедур, реализацию, документы, мониторинг и анализ), деятельность в рамках проводимого аудита (начиная с инициализации процесса, проведения анализа представленных документов, подготовки к аудиту на месте и заканчивая подготовкой отчета по результатам аудита, завершению аудита и последующих действий), компетентность и оценка аудиторов.

ISO/IEC 27007:2011 ориентирован на аудит всей СУИБ в целом.

Стандарт ISO/IEC 27008:2011 «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.

Стандарт ISO/IEC 27008:2011 не предназначен для аудита систем управления в целом, поскольку он ориентирован на процесс управления рисками ИБ в рамках СУИБ. Он представляет

собой руководящие указания по анализу реализации и функционирования средств управления ИБ, включая техническую проверку их соответствия вышеперечисленным стандартам и установленным в организации стандартам ИБ.

Результаты проведенного в соответствии с ISO/IEC 27008:2011 аудита могут быть использованы для усовершенствования СУИБ за счет оптимизации взаимодействия между ее отдельными процессами. В качестве примера таких мероприятий можно привести реализацию механизмов снижения вреда, причиненного сбоями в защите информации, за счет чего возможно появление некорректных финансовых отчетов и документов, а также негативное воздействие на нематериальные ценности, такие как репутация и имидж организации, частная жизнь, навыки и опыт людей.

ISO/IEC 27011:2008. Руководство по управлению ИБ для телекоммуникационных компаний на основе ISO/IEC 27002

Стандарт ISO/IEC 27011:2008 «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 ITUT.

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 других свойств ИБ. Целевая аудитория стандарта не ограничивается только ТК. Он рассчитан на тех, кто отвечает за ОИБ вендоров, провайдеров и т. п.

Конфиденциальность в ISO/IEC 27011:2008 означает неразглашение данных о коммуникациях в терминах существования, содержания, источника, места назначения, даты и времени передачи информации. Лица, привлеченные ТК, должны сохранять

конфиденциальность любой информации обо всем, что, возможно, стало им известно во время выполнения ими своих трудовых обязанностей.

Целостность понимается в смысле того, что использование телекоммуникационных средств должно обеспечивать подлинность, точность и полноту информации, переданной или полученной по проводам, радиоканалам или любыми другими методами.

Доступность означает обеспечение только авторизированного доступа к информации, передаваемой с помощью телекоммуникаций, 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.

Архитектура и реализация СУИБ продиктованы потребностями производства, требованиями по ОИБ, используемыми процедурами, а также размером и структурой ТК. Предполагается, что со временем эти характеристики и поддерживающие их системы изменяются. Поэтому реализация СУИБ будет масштабироваться в соответствии с изменяющимися потребностями организации.

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

Поскольку ТК предоставляют телекоммуникационные сервисы, используя средства связи и сервисы совместно с другими организациями, то к передаваемой информации имеют доступ не только их сотрудники, но и другие пользователи вне этих организаций. Поэтому управление ИБ для ТК охватывает все обла-

сти сетевой инфраструктуры, сервисные приложения и многое другое.

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

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

– ПолИБ;

– организация ИБ;

– управление активами;

– безопасность персонала;

– физическая и экологическая безопасность;

– управление средствами связи и их функционированием;

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

– приобретение, развитие и сопровождение ИС (требования по ОИБ для ИС, корректная работа с приложениями, защита файловых систем, безопасность процессов разработки и поддержки, устранение технических уязвимостей);

– управление инцидентами ИБ (подготовка отчетов о событиях ИБ и уязвимостях, процесс управления инцидентами ИБ);

– управление непрерывностью производства с учетом ИБ;

– соответствие стандартам ИБ.

ISO/IEC 27013. Руководство по интегрированному внедрению стандартов ISO/IEC 20000 и 27001

Стандарт ISO/IEC 27013 «Информационная технология. Методы и средства обеспечения безопасности» представляет собой руководство по системам интегрированного управления ИБ и ИТ-сервисами, как взаимодополняющим и поддерживающим

друг друга. Стандарт помогает 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.

Стандарт ISO/IEC 20000 посвящен управлению и обслуживанию ИТ-сервисов, учитывающим лучшие существующие практики, и состоит из двух частей.

Первая часть ISO/IEC 200001:2005 «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].

Вторая часть 1SO/IEC 200002:2005 «Менеджмент ИТ-сервисов. Практические правила управления сервисом» дает практические рекомендации по процессам, требования к которым сформулированы в ISO/IEC 200001, и является руководством для аудиторов и компаний, намеренных пройти сертификацию [40].

Стандарт ISO/IEC 27013 создает основу для приоритезации деятельности в таких направлениях:

– координация задач усовершенствования и управления для ИБ и сервисов;

– координация междисциплинарной деятельности при реализации интегрированного подхода (например, при управлении инцидентами);

– создание общей системы процессов и их документирования (включая политики, процедуры и др.);

– выработка единой терминологии;

– объединение преимуществ для клиентов и сервис-провайдеров, и извлечение дополнительной выгоды, появляющейся при интеграции систем управления ИБ и ИТ-сервисами;

– совместный аудит систем управления ИБ и ИТ-сервисами и сокращение затрат на его проведение.

ISO/IEC 27014. Инфраструктура руководства ИБ

Стандарт ISO/IEC 27014 «Информационная технология. Методы и средства обеспечения безопасности. Инфраструктура руководства ИБ» станет руководством, помогающим организациям руководить 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 учесть важные факторы:

– производственной стратегии, политики и задачи организации в отношении ИБ, рисков и средств управления ИБ;

– соответствия надлежащим нормативным документам и законам в области ИБ;

– соблюдения соответствия контрактным и другим обязательствам в области ИБ;

– требований к аудиту и сертификации.

Стандарт рассматривает 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, внутренних аудитов, составления отчетов по СУИБ для руководства организации и т. п.;

– взаимосвязь руководств ИБ, ИТ и всеми информационными активами организации;

– ответственность за ОИБ, владение информационными активами внутри организации.

ISO/IEC 27015. Руководство по управлению ИБ для финансовых сервисов

Стандарт ISO/IEC 27015 «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.

ISO/IEC 27015 направлен на поддержку специфической деятельности финансовых организаций, особенно заинтересованных в ОИБ, для которых таким образом создается международно признанная и одобренная основа для реализации производства, отвечающая всем правовым требованиям и требованиям регуляторов. В стандарте 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 факторы: производственная стратегия организации и возможности сегмента рынка, специфические сервисы и производимая продукция организации, правовые ограничения и ограничения регуляторов.

ISO/IEC 27015 не претендует на определение обязательных требований. Скорее, он служит руководством по обеспечению наглядности деятельности по управлению ИБ в организации и доказательством следования лучшим практикам в области управления и обеспечения ИБ.

ISO/IEC 27031:2011

Стандарт ISO/IEC 27031:2011 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности ИТТ к непрерывности бизнеса» содержит концепции и принципы, возлагаемые на ИТТ как на неотъемлемую часть критической инфраструктуры любой организации по обеспечению непрерывности производства [42]. Этот стандарт официально заменяет британский стандарт BS 25777:2008 [43], который, в свою очередь, разработан на базе существующих стандартов обеспечения непрерывности бизнеса 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, но не представляющей собой пошаговую инструкцию по внедрению процессов управления непрерывностью ИТ-сервисов. Управление непрерывностью ИТТ обеспечивает необходимую жизнеспособность ИТТ и сервисов и возможность их восстановления до определенного уровня в необходимые сроки, согласованные с руководством организации. Эффективное управление непрерывностью ИТТ гарантирует, что организация способна достичь своих целей, особенно в моменты аварий и бедствий.

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

– управления программой непрерывности ИТТ;

– внедрения принципов управления непрерывностью ИТТ в культуру организации;

– документирования системы управления непрерывностью ИТТ;

– определения требований к непрерывности ИТТ;

– разработки и реализации стратегии обеспечения непрерывности ИТТ;

– разработки и тестирования планов обеспечения непрерывности ИТТ;

– обучения в области восстановления сервисов ИТТ;

– анализа и совершенствования 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 в рамках СУИБ организации для обеспечения непрерывности ее производства, измерять непрерывность, безопасность и готовность к преодолению аварий и бедствий.

Область действия 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.

Во многих современных организациях ИТТ превалируют над другими технологиями и являются основными компонентами поддержания критически важных бизнес-процессов и про-

цессов управления. Планирование непрерывности бизнеса без надлежащей защиты, доступности и непрерывности функционирования ИТТ невозможно.

Готовность ИТТ снижает для организации негативное воздействие (масштаб, продолжительность и/или последствия) инцидентов ИБ и включает:

– подготовку в организации ИТТ (инфраструктура, функционирование и приложения для ИТТ) и взаимосвязанных процессов и персонала к противодействию обстоятельствам, которые могут изменить риски и повлиять на непрерывность функционирования самих ИТТ и производства организации;

– перераспределение и оптимизацию использования ресурсов, восстановлением после аварий/бедствий, реакцией на нештатные ситуации и инциденты, нарушающие безопасность ИТТ.

Стандарт ISO/IEC 27031:2011 базируется на цикле PDCA, расширяя обычный процесс планирования непрерывности производства 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 события, влекущие за собой серьезные инциденты.

Основная содержательная часть ISO/IEC 27031:2011 представлена такими разделами:

– роль готовности ИТТ для непрерывности производства;

– 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 планирования готовности ИТТ, то это позволяет избежать дублирования одинаковых процессов в одной организации.

ISO/IEC 27033. Управление безопасностью сетей

Стандарт ISO/IEC 27033 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность в сетях» освещает вопросы обеспечения безопасности в сетях.

Необходимость в обеспечении безопасности сетей особенно важна в современном информационном пространстве. Сетевые соединения могут находиться в границах одной организации, осуществляться между разными организациями, а иногда – между организацией и сетями общего пользования. Поэтому производство организаций сильно зависит от всех видов связи: от классических автоматизированных систем до беспроводного доступа.

Стандарт содержит большой список определений и сокращений в области безопасности сетей. Описан процесс планирования и управления безопасностью сетей, рассмотрены основы сетевого взаимодействия, даны рекомендации по идентификации рисков ИБ для сетей, выделены области управления безопасностью сетей.

В качестве необходимых защитных мер определены: утверждение и следование ПолИБ для сетей, процедуры ОИБ и проверки ИБ, технические аспекты устранения уязвимостей, идентификация, аутентификация и авторизация, аудит и мониторинг безопасности, обнаружение и предотвращение вторжений, защита от вредоносного ПО, сервисы на основе криптографии.

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). Отдельное внимание уделено разработке и тестированию решений по ОИБ в сетях, их функционированию, мониторингу и анализу.

ISO/IEC 270332 «Руководство по проектированию и внедрению системы обеспечения безопасности сетей» определяет как

организация должна создавать архитектуру, проект и реализацию технической безопасности для сетей, которые обеспечивают эффективную, соответствующую производственным требованиям защиту, опирающуюся на базовые модели и понятную для всех сотрудников организации, вовлеченных в планирование, проектирование и внедрение технологий безопасности сетей.

ISO/IEC 270333:2010 «Базовые сетевые сценарии – угрозы, методы проектирования и средства управления» [47] устанавливает специфические риски, методики проектирования и вопросы управления сетями. Риски рассматриваются в таких областях предоставления сервисов, как доступ в Интернет, взаимодействие различных организаций между собой и с клиентами, коллективная работа, сегментация сетей, сетевое взаимодействие для работы из дома и офиса, мобильная связь, удаленные пользователи, аутсорсинг.

ISO/IEC 270334 «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.

ISO/IEC 270335 «Обеспечение безопасности виртуальных частных сетей, угрозы, методы проектирования и средства управления» приводит специфические риски, методики проектирования и средства управления для защиты соединений, устанавливаемых посредством использования виртуальных частных сетей (ВЧС) (англ. *Virtual Private Network, VPN*).

ISO/IEC 270336 «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.

ISO/IEC 270337 «Руководство по обеспечению безопасности беспроводных сетей, риски, методы проектирования и средства управления» устанавливает специфические риски, методики проектирования и средства управления для защиты беспроводных и радиосетей.

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 взаимосвязи между внедрением управления безопасностью ИТ и техническими аспектами безопасности сетей.

ISO/IEC 18028 состоит из пяти частей, рассматривающих управление безопасностью сетей, архитектуру безопасности сетей, защиту сетевых взаимодействий при помощи шлюзов безопасности, защиту удаленного доступа, защиту сетевых взаимодействий при помощи ВЧС.

Первая часть стандарта ISO/IEC 180281:2006 содержит руководство по созданию сетей и организации 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.

ISO/IEC 27035:2011. Управление инцидентами ИБ

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 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 – это действия и превентивные, и корректирующие одновременно.

Стандарт ISO/IEC 27035:2011 «Информационная технология. Методы и средства обеспечения безопасности. Управление инцидентами ИБ» [48] содержит планомерный подход:

– к обнаружению и оценке инцидентов ИБ;

– осуществлению ответной реакции и управлению инцидентами ИБ;

– обнаружению, оценке и устранению уязвимостей.

После принятия в 2011 г. стандарт заменяет ISO/IEC TR 18044:2004 «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 модель управления инцидентами ИБ и устанавливает рекомендации по менеджменту инцидентов ИБ для руководителей подразделения по ИБ, информационных систем, сервисов и сетей.

ISO/IEC 27035:2011 всесторонне рассматривает управление как уязвимостями, так и инцидентами ИБ. Приводятся шаблоны

для подготовки отчетов по событиям, инцидентам ИБ и уязвимостям.

В стандарте освещены основы управления инцидентами ИБ, его преимущества и ключевые вопросы, примеры инцидентов ИБ и причин их возникновения.

Процесс управления инцидентами ИБ включает:

– планирование и подготовку к обработке инцидентов ИБ, составление документов, поддерживающих управление инцидентами;

– обнаружение/идентификацию и подготовку отчета по инциденту ИБ;

– оценку инцидента и принятие решений по нему;

– ответную реакцию на инцидент ИБ;

– извлечение уроков из инцидента ИБ.

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 ходе разработки процесса управления инцидентами ИБ возможно связать требования ISO/IEC 27001 и представленную модель управления инцидентами ИБ, 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 эффективным образом;

– последствия инцидентов ИБ могут быть минимизированы;

– за счет анализа событий и инцидентов ИБ повышается вероятность предотвращения инцидентов в будущем, улучшаются механизмы и процессы ОИБ.

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. В российских публикациях по данной теме используется термин «технико-криминалистическая экспертиза».

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 последовательное сохранение всех доказательств, представленных в электронной форме так, чтобы они собирались и защищались с помощью технологий, признаваемых судами. Для этого требуется соблюдение или даже превышение базового уровня защиты доказательств.

Стандарт ISO/IEC 27037 представляет руководство по сбору и сохранению доказательств компьютерных преступлений, представленных в электронной форме. Его можно использовать при трансграничных преступлениях (когда жертва и атакующий находятся в различных государствах), когда собранные в одной стране доказательства должны быть признаны и приняты к рассмотрению в суде другой страны. В настоящее время юридические тонкости 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 преступления в одной стране, в другой таковыми не считаются.

Стандарт ISO/IEC 27037 разработан на основе британского стандарта BS 10008:2008 («Допустимость электронной информации в качестве доказательств и ее доказательная сила») [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.

Стандарт ISO/IEC 27037 содержит гармонизированный для разных стран процесс распознавания и идентификации, документирования преступления, сбора и сохранения, упаковки и транспортировки доказательств. Рассмотрены доказательства, порождаемые различными источниками.

2.3. Стандарты на отдельные процессы управления информационной безопасностью

Стандарт ISO/IEC 13335. Методы и средства обеспечения безопасности информационных технологий

Стандарт, первоначально появившийся в статусе технического отчета, объединил несколько руководящих документов по управлению безопасностью ИТ.

Он состоит из четырех частей:

1. ISO/IEC 13335-1:2004 «Концепции и модели менеджмента безопасности информационных и телекоммуникационных технологий», объясняющий концепции и модели управления безопасностью ИТТ. Последняя переработанная версия содержит и вторую часть стандарта ISO/IEC 13335-2, которая после этого отменена как самостоятельная часть стандарта 13335 [52].

2. ISO/IEC TR 13335-3:1998 «Методы менеджмента безопасности информационных технологий», устанавливающий методы управления ИБ ИТ. В настоящее время эта часть заменена стандартом ISO/IEC 27005.

3. ISO/IEC TR 13335-4:2000 «Методы и средства менеджмента безопасности информационных технологий», который охватывал выбор технических средств управления ИБ. В настоящее время данная часть стандарта также отменена и заменена стандартом ISO/IEC 27005.

4. ISO/IEC TR 13335-5:2001 «Руководство по менеджменту безопасно IT-сети», который представляет собой руководство по управлению безопасностью сетей – отменена и заменена стандартом ISO/IEC 180281, который, в свою очередь, стал частью стандарта ISO/IEC 27033 [53].

В России приняты четыре следующих стандарта, идентичных соответствующим частям ISO/IEC 13335.

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 принципы безопасности:

– менеджмент риска. Активы должны быть защищены путем принятия соответствующих мер, которые должны выбираться и применяться на основании методологии управления риска-

ми, учитывающей существующие ограничения, исходя из активов организации, угроз, уязвимостей и различных воздействий угроз;

– обязательства организации в области ОИБ ИТТ и в управлении рисками ИБ;

– 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 ИБ ИТТ должно быть непрерывным в течение всего их жизненного цикла.

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 обзор способов управления, цели, стратегия и политика обеспечения безопасности ИТТ, описание анализа рисков, применение защитных мер, рассмотрение работ по 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].

ГОСТ Р ИСО/МЭК ТО 13335-4-2007 «Информационная технология. Методы и средства обеспечения безопасности. Выбор защитных мер» [56] (идентичный TSO/IEC TR 133354:2000) яв-

ляется 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 учетом особенностей окружающей среды, а также устанавливаются способы достижения защиты на основе базового уровня безопасности. Приведенный в стандарте выбор 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].

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 руководство по управлению безопасностью сетей для персонала, ответственного за эту деятельность, и содержит основные положения по выявлению и анализу факторов, имеющих отношение 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 необходимо решить 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 типов рассматриваемых сетевых соединений;

– анализ характеристик объединения в сеть и связанные с этим доверительные отношения;

– определение видов рисков ИБ, включая оценки производственных операций и информацию, которую предполагается передавать через соединения, и любую другую информацию, потенциально доступную для несанкционированного получения через соединения;

– идентификация средств управления, которые могут быть использованы, на основе анализа типов 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.

ISO/IEC 15408 и ISO/IEC 18045:2008. Общие критерии и методология оценки безопасности информационных технологий

Состоящий из трех частей стандарт ISO/IEC 15408 «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 создан для взаимного признания результатов оценки безопасности ИТ в мировом масштабе. Он позволяет срав-

нить 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 (в стандарте выделено 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 моделей (профилей защиты), описывающих стандартные модули системы безопасности, например, СУБД или МСЭ. 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.

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 154081–2008 «Информационная технология. Методы и средства обеспечения безопасности. Введение и общая модель» (идентичный ISO/IEC 154081:2005) устанавливает общий подход к формированию требований к оценке безопасности, основные конструкции (профиль защиты, задание по безопасности) представления требований безопасности в интересах потребителей, разработчиков и оценщиков продуктов и систем ИТ [61].

2. ГОСТ Р ИСО/МЭК 154082–2008 «Информационная технология. Методы и средства обеспечения безопасности. Функциональные требования безопасности» (идентичный ISO/IEC 154082:2005) содержит универсальный систематизированный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определенным правилам [62].

3. ГОСТ Р ИСО/МЭК 154083–2008 «Информационная технология. Методы и средства обеспечения безопасности. Требования доверия к безопасности» (идентичный ISO/IEC 154083:2005) 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, устанавливающие 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 [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 нормативный документ, применяемый совместно с ГОСТ Р ИСО/МЭК 15408. Последний описывает минимум действий, выполняемых оценщиком и органом сертификации, подтверждающим действия оценщика, при проведении оценки безопасности ИТ по ИСО/МЭК 15408 с использованием определенных в последнем критериев и свидетельств оценки. Стандарт также предназначен для заявителей оценки, разработчиков, авторов профилей защиты и заданий по безопасности и других сторон, заинтересованных в безопасности ИТ.

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, обеспечивающим проверку результативности внедрения политики организации в области менеджмента качества и/или окружа-

ющей среды (последние системы иногда называются системами экологического менеджмента). Аудиты являются важной составляющей деятельности по оценке соответствия при сертификации/регистрации, оценке провайдеров, инспекционном контроле.

Вторая редакция стандарта ISO 19011:2011 «Руководство по аудиту систем менеджмента» [66] по сравнению с первой, применявшейся только к стандартам ISO 9001 и ISO 14001, расширила область применения 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 обеспечены все необходимые предпосылки для того, чтобы сделать аудит важнейшим инструментом достижения целей организации.

В ISO 19011:2011 добавлено понятие риска и в явной форме установлены требования к компетентности аудиторов. Признана важность применения технологий удаленного аудита, например, проведение удаленных интервью и просмотр документации. Другое важное улучшение – более четкое описание разницы между стандартами ISO 19011:2011и 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] содержит указания по принципам аудита, управлению программами аудита, проведению аудита систем менеджмента, управлению программами аудита.

Для процесса проведения аудита в стандарте отдельно описываются подпроцессы:

– инициализация аудита (назначение ведущего аудитора группы, определение целей, критериев и объема аудита, оценка осуществимости аудита, выбор аудиторской группы);

– подготовка к аудиту (предварительный анализ документации, подготовка плана аудита, распределение обязанностей в группе, подготовка рабочих документов);

– проведение аудита на месте (вступительное совещание, сопровождающие и наблюдатели, сбор и проверка информации аудита, подготовка заключений аудита, заключительное совещание);

– подготовка, утверждение и распространение отчета по аудиту.

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

В приложениях к стандарту приведены формы и указания по их заполнению: график проведения аудитов, отчет об анализе программы аудита, опросный лист, паспорт аудитора, план аудита, отчет по аудиту и другие документы.

Указания стандарта являются гибкими. Их использование может быть различным в зависимости от размера, вида деятельности, сложности проверяемых организаций, а также целей и области аудита.

BS 25999 и ГОСТ Р 53647. Управление непрерывностью бизнеса

Британские стандарты серии BS 25999 разработаны на основе передового опыта в данной области группой специалистов-практиков мирового класса, в которую вошли представители разных государств и отраслей.

В серию BS 25999 входят два стандарта:

1. BS 259991:2006 «УНБ. Практические правила» [68], который определяет процесс, принципы и терминологию в области УНБ, закладывая основы для понимания, разработки и внедрения системы УНБ в организации и поддержания ее надежности.

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.

2. BS 259992:2007 «УНБ. Спецификация» [69]. В то время как BS 259991:2006 содержит общие рекомендации по УНБ, вторая часть устанавливает и детализирует конкретные требования к СУНБ, соблюдение которых может быть объективно проверено. Используя эти требования, организации могут проводить оценку существующей СУНБ как самостоятельно, так и привлекая внешних консультантов. На основании второй части стандарта сертификационные органы выдают заключение о соответствии СУНБ требованиям стандарта BS 25999.

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 259991:2006).

2. ГОСТ Р 53647.2–2009 «Менеджмент непрерывности бизнеса. Часть 2. Требования» [71] (идентичный BS 259992:2007).

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

В перечисленых 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 функ-

ционирования организации в целом. УНБ включает управление восстановлением и продолжением деятельности в случае нарушения нормального хода производства, а также управление общей программой УНБ посредством проведения обучения и повышения осведомленности персонала, а также анализа с целью поддержания планов 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 производственных процессов в рамках области действия СУНБ.

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.

2.4. Стандарты в области управления информационной безопасностью банковской системы Российской Федерации

Для организаций банковской сферы задача ОИБ выступает одним из важных требований, поскольку, являясь объектом пристального внимания злоумышленников, банки ежедневно сталкиваются с инцидентами ИБ. Развитие и укрепление банковской системы Российской Федерации (БС РФ), включающей в себя Банк России, кредитные организации, филиалы и представительства

иностранных банков, а также обеспечение эффективного и бесперебойного функционирования платежной системы Российской Федерации являются целями деятельности Банка России.

Важнейшее условие их реализации – 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, 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 Российской Федерации, нанести ущерб интересам ее собственников и клиентов. Поэтому для организаций БС РФ угрозы ИБ информационных активов и их реализация в виде инцидентов ИБ представляют реальную опасность. Для противостояния таким угрозам и обеспечения эффективности мероприятий по ликвидации неблагоприятных 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 и рисков ИБ, принятия мер, необходимых для управления этими рисками. Для подобных целей 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;

– достижение адекватности мер по защите от реальных угроз ИБ,

– предотвращение и/или снижение ущерба от инцидентов ИБ.

Главные задачи стандартизации по ОИБ организаций БС РФ заключаются:

– в установлении единых требований по ОИБ;

– повышении эффективности мероприятий по обеспечению и поддержании ИБ организаций.

Комплекс документов по обеспечению и управлению ИБ организаций БС РФ состоит из отраслевых стандартов (СТО) и рекомендаций в области стандартизации.

Разработан ряд документов комплекса:

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

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

3. 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.

4. Рекомендации в области стандартизации Банка России РС БР ИББС-2.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методиче-

ские 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.

5. 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.

6. 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.

7. 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.

8. 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.

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. Какой из стандартов серии ISO/IEC 27000 содержит требования к созданию, внедрению, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ?

4. Какой из стандартов серии ISO/IEC 27000 признан каталогом лучших практик по ИБ?

5. В каком стандарте серии ISO/IEC 27000 содержится руководство по внедрению СУИБ?

6. Каковы основные идеи руководства по аудиту СУИБ?

7. Какой стандарт серии ISO/IEC 27000 рассматривает вопросы управления безопасностью сетей?

8. Какие из рассмотренных стандартов затрагивают аспекты анализа рисков ИБ?

9. Каковы основные цели построения системы УНБ, соответствующей требованиям стандартов BS 25999 и 25777?

10. Каковы основные цели следования модели PDCA при построении процесса управления инцидентами ИБ в соответствии с требованиями ГОСТ Р ИСО/МЭК ТО 18044?

11. Какие тенденции характерны для развития стандартизации управления ИБ в Российской Федерации?

12. В чем состоят преимущества использования отраслевых стандартов по сравнению со стандартами, требования которых применимы к любой организации независимо от отрасли или сферы деятельности?

13. Какие аспекты регламентируют стандарты серии СТО БР ИББС, если говорить об управлении ИБ?

14. Каковы цели и задачи стандартизации по ОИБ организаций БС РФ?

Глава 3. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Основные понятия

Термин «политика» (греч. *politika* – государственные или общественные дела) используется в человеческом обществе давно. Существует много трактовок этого понятия, из которых чаще всего применяются следующие:

– сфера деятельности, связанная с отношениями между социальными группами, сутью которой является определение форм, задач, содержания деятельности государства;

– направление деятельности государства или каких-либо социальных групп в той или иной области в определенный период;

– образ действий, направленных на достижение чего-либо, поведение, определяющее отношения с людьми;

– общее намерение и направление, официально выраженное руководством [22].

В англоязычной литературе при рассмотрении вопросов ОИБ, кроме политики, используются и другие термины (стандарты, базис, руководства и процедуры) [80]:

– политики обычно рассчитаны на долгий срок и содержат руководство по разработке более конкретных правил для ситуаций и систем. Они могут относиться к различным вопросам, таким как управленческие решения по настройке электронной почты организации, обеспечению режима секретности или защите факсов;

– политики поддерживаются стандартами, процедурами и руководствами, в которых должно содержаться общее направление обязательной деятельности для организации. Примеры областей, для которых необходимы политики: физическая защита, безопасность персонала и оборудования, защита сетей, управление рисками и инцидентами ИБ.

Стандарт представляет собой правило, указывающее конкретное направление действий или ответную реакцию на данную ситуацию. Он является обязательным директивным указанием (директивой), которое должно выполняться в соответствии с политиками.

Базис устанавливает, как для конкретных технологий используются средства управления. Он создается для обеспечения функции защиты таким образом, чтобы для наиболее часто используемых систем они управлялись единым образом, поддерживая нужный уровень безопасности в пределах всей организации.

Процедуры определяют конкретные действия, как политики, стандарты, базисы и руководства будут реализованы в данной ситуации. Это технологии или процессы, имеющие отношение к конкретным платформам, приложениям или процессам. С целью обеспечения конкретных технических или процедурных требований внутри организации, где они применяются, процедуры как можно точнее должны поддерживать организационные политики, стандарты, базисы и руководства. Примеры процедур: сертификация и аккредитация, оценка рисков ИБ, обнаружение вторжений, тесты на проникновение, реагирование на чрезвычайные ситуации, восстановление после аварий, резервирование, реагирование на инциденты ИБ.

Руководства содержат рекомендации по выполнению требований, которые желательно учитывать при осуществлении защиты. Они, не являясь обязательными, должны соблюдаться, если нет документированных причин не делать этого.

Для организации общий подход в области ОИБ отражается в разработанном, утвержденном и строго выполняемом всеми ее сотрудниками и партнерами документе – политике ОИБ организации (ПолИБ).

ПолИБ содержит позицию организации по отношению к деятельности в области ОИБ, ее стремление соответствовать государственным, международным требованиям и стандартам в этой области. Он определяет стратегию и тактику построения в организации системы защиты информации. В российской терминологии документ, определяющий стратегию, часто называют концепцией, а документ, определяющий тактику, – политикой. За рубежом принято создавать единый документ, включающий одновременно стратегию и тактику защиты. ПолИБ организации является основой для разработки целого ряда документов в области ОИБ: стандартов, руководств, процедур, практик, регламентов, должностных инструкций и пр.

Согласно самому первому определению, приведенному в стандарте «Оранжевая книга» (Trusted Compute System Evaluation Criteria), *ПолИБ* – это набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации [81]. Гостехкомиссия России определила такую ПолИБ как совокупность правил, регламентирующих права субъектов к объектам доступа [76]. После этого данный термин определялся как в международных, так и российских стандартах, и руководящих документах в основном как ПолИБ организации:

– совокупность требований и правил по ОИБ для объекта ИБ, выработанных в соответствии с требованиями руководящих и нормативных документов в целях противодействия множеству угроз ИБ, с учетом ценности защищаемой информационной сферы и стоимости СОИБ [82];

– документированные решения в области ОИБ [83];

– совокупность (одно или несколько) документированных правил, процедур, практических приемов в области безопасности, которыми руководствуется организация в своей деятельности [10; 61].

Взаимоувязанная совокупность документов в области стандартизации Банка России (СТО БР ИББС – 1.0) вводит понятие ПолИБ организации [11].

Различают ПолИБ организации в целом (тогда она называется корпоративной ПолИБ) и ее подразделений [83].

ПолИБ сети определяется как документ, в рамках единой информационной инфраструктуры и СОИБ организации формально устанавливающий правила доступа к ее компьютерной сети, на основе которых пользователи этой сети (сотрудники и партнеры организации) накапливают, применяют и распоряжаются ее активами.

В современной практике ОИБ термин «ПолИБ» может употребляться как в широком, так и в узком смысле [83]. В широком смысле он определяется как система документированных управленческих решений по ОИБ организации, в узком – отдельный нормативный документ, определяющий требования безопасности, систему мер и/или порядок действий, а также ответственность сотрудников организации и средства управления для определенной области ОИБ.

Также известно понятие «частная ПолИБ» [11], или ПолИБ по конкретным вопросам или проблемам, или ПолИБ по конкретным системам [84], ориентированная на отдельную область ОИБ или технологию, используемую в организации или ее подразделениях. Например, это ОИБ в части, касающейся ИБ, ОИБ телекоммуникационных систем и сервисов, антивирусная защита, доступ в Интернет, использование средств криптографической защиты и т. д. В них формулируются требования по созданию и эксплуатации СЗИ, организации информационных и бизнес-процессов организации по конкретному направлению ОИБ.

Таким образом, частные ПолИБ являются составляющими корпоративной ПолИБ организации, поскольку конкретизиру-

ют ее. *Частная ПолИБ* – это документация, детализирующая положения ПолИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности организации [11].

Поскольку основу ПолИБ составляет, как правило, конкретный способ управления каким-либо видом доступа, определяющим порядок обращения субъектов системы к ее объектам, название этого способа и определяет название частной ПолИБ. Как показывает опыт, наиболее часто разрабатываемыми в организациях частными ПолИБ являются политики для следующих областей:

– физической защиты (включая вопросы организации пропускного режима, регистрации сотрудников и посетителей, использования средств сигнализации и видеонаблюдения и т. п.);

– организации режима секретности;

– ОИБ при процессе транспортировки носителей информации;

– обращения с информацией, составляющей государственную тайну;

– опубликования материалов в открытых источниках;

– доступа сторонних пользователей (организаций) в ПС органи зации;

– оценки рисков ИБ;

– управления паролями;

– контроля доступа и защиты от несанкционированного доступа;

– назначения, распределения ролей и обеспечения доверия к персоналу;

– использования Интернета;

– разработки и лицензирования ПО;

– установки и обновления версий ПО;

– приобретения ИС и их элементов (программных и аппаратных средств);

– использования отдельных универсальных ИТ в масштабе организации:

– электронной почты;

– сетевых сервисов;

– программно-технических средств защиты;

– межсетевых экранов (МЭ);

– технологии виртуальных частных сетей (ВЧС);

– средств антивирусной защиты;

– средств криптографической защиты информации;

– электронной цифровой подписи (ЭЦП);

– инфраструктуры открытых ключей;

– модемов и других коммуникационных средств;

– мобильных аппаратных средств;

– проведения внешних и внутренних аудитов ИБ;

– резервирования информации.

В РС БР ИББС-2.0 по документации в области ОИБ отмечается, что деятельность организации по ОИБ осуществляется на основе действующих законодательных актов и нормативных документов Российской Федерции по ОИБ, нормативных актов Банка России и внутренних документов самой организации по ОИБ [75].

В состав внутренних документов рекомендуется включать следующие виды документов, организованных в виде иерархической структуры (рис. 3.1):

– документы 1-го уровня, содержащие положения корпоративной ПолИБ организации и определяющие высокоуровневые цели, содержание и основные направления деятельности по ОИБ, предназначенные для организации в целом;

– документы 2-го уровня, содержащие положения частных ПолИБ и детализирующие положения корпоративной ПолИБ

применительно к одной или нескольким областям ИБ, видам и технологиям деятельности организации;

– документы 3-го уровня, содержащие положения ИБ, применяемые к процедурам (порядку выполнения действий или операций) ОИБ, правила и параметры, устанавливающие способ выполнения конкретных действий, связанных с ИБ в рамках технологических процессов, используемых в организации, либо ограничения по выполнению отдельных действий, связанных с реализацией защитных мер в используемых технологических процессах (технические задания, регламенты работ, порядки, инструкции по эксплуатации, руководства по администрированию и т. п.);

– документы 4-го уровня, отражающие достигнутые промежуточные и окончательные результаты, относящиеся к ОИБ организации.

Рис. 3.1. Иерархия документов в области ОИБ для организации

Согласно ГОСТ Р ИСО/МЭК 17799–2005, на верхнем уровне ПолИБ должны быть оформлены следующие документы: «Концепция обеспечения ИБ» (или просто «Концепция ИБ»), «Правила допустимого использования ресурсов информационной системы»,

«План обеспечения непрерывности бизнеса» [13]. На практике можно встретить и документы с такими названиями: «Регламент управления ИБ», «Технический стандарт ИБ» и т. п. Данные документы могут выпускаться в двух редакциях: для внешнего и внутреннего использования. По аналогии с определением концепции ИБ РФ Межведомственной комиссии по ИБ Совета Безопасности Российской Федерции концепция ИБ организации – это официально принятая ее руководством система взглядов на проблему ОИБ, методы и средства защиты жизненно важных интересов организации в информационной сфере. Эта система взглядов взаимоувязывает правовые, организационные и программно-аппаратные меры защиты и основана на анализе защищенности ИС в разрезе видов угроз и динамики их развития.

Концепция ИБ отражает стратегию и тактику ОИБ организации и отвечает на три основных вопроса: что защищать, от чего защищать и как защищать. Таким образом, концепция ИБ организации во многом схожа с корпоративной ПолИБ, хотя второй документ содержит более конкретное наполнение стратегии и тактики правилами, процедурами, практическими приемами и руководящими принципами в области ОИБ, которыми руководствуется организация в своей деятельности.

ПолИБ также можно разделить на две части:

– организационную (административную), выполняемую людьми;

– техническую, реализуемую с помощью оборудования и программ.

Организационная часть ПолИБ обычно излагается в документах трех уровней. Документы верхнего уровня носят общий характер и определяют ПолИБ для организации в целом. Второй уровень выделяют при наличии структурной сложности организации – специфичные области деятельности, подразделе-

ния, технологии, подсистемы и т. п. Третий уровень относится к конкретным службам или подразделениям организации и детализирует верхние уровни ПолИБ. На данном уровне определяются конкретные цели, частные критерии и показатели ИБ, задаются права групп пользователей, формулируются условия доступа к информации, выводятся правила ОИБ.

Техническая часть ПолИБ – это совокупность правил и практических методов, регулирующих обработку чувствительной информации и использование ресурсов ПО и аппаратного обеспечения (АО) ИС. Она базируется на правилах двух видов. Первая группа связана с заданием правил разграничения доступа ко всем информационным ресурсам организации, вторая – основана на правилах анализа сетевого трафика. В основе этих правил лежит принцип доверия к пользователям, приложениям, процессам, базам данных (БД), файлам и т. п. Поэтому, определяя техническую ПолИБ, нужно установить, насколько можно доверять пользователям и информационным ресурсам, учитывая возможность атаки с подменой («маскарадом») ресурсов.

Кроме этого, ПолИБ могут создаваться для отдельных пользователей или групп пользователей, для отдельного департамента, роли/должности внутри организации или за ее пределами (для партнеров, клиентов и т. п.).

3.2. Причины выработки политики информационной безопасности

Предположим, что администратор ИБ интранета крупной организации наблюдает за системой поздно вечером и видит, что развивается атака [85]. Что ему делать? Позволить атаке и дальше продолжаться, собирая регистрируемые соответствующими системами данные для дальнейшего расследования или отклю-

чить интранет от экстранета (от сетей партнеров данной организации и каналов Интернет)? Если так, отключить ли основное средство фильтрации трафика МЭ между интранетом и экстранетом? Или отключить соединение с Интернетом, например, препятствуя доступу пользователей на веб-сервер организации? Имеет ли он полномочия это сделать? Руководству организации до наступления такого события необходимо четко расставить приоритеты и определить все необходимые действия.

Рассмотрим сценарий, когда администратор ИБ думает, что интранет действительно атакуют, поэтому и отключает соединение с экстранетом. Пользователи начинают выражать недовольство из-за невозможности выполнять привычные операции в интранете. Потом оказывается, что администратор ИБ ошибся и, например, принял работу только что поступившего в организацию нового сотрудника за злоумышленника.

В этом случае кража данных является абстрактной возможностью, а недовольные пользователи реальны уже сегодня. Таким образом, необходима политика, которая определяет важность защитных мер и четко устанавливает процедуры, требуемые для выполнения, когда кажется, что имеет место атака. Как только точно определены приоритеты, нужно понять технологию реализации установленной политики.

Наиболее эффективный способ добиться минимизации рисков нарушения ИБ организации – это разработать ПолИБ и в соответствии с ней реализовать, развивать и совершенствовать СОИБ организации [11].

Укажем основные аргументы в пользу того, что ПолИБ должна быть выработана для организации любого масштаба и вида деятельности.

Во-первых, ПолИБ составляет общую основу для защиты всех активов организации, в которой определяются правила раз-

граничения доступа к ним. Правила определяют, какое поведение по отношению к активам разрешено, т. е. санкционировано, а какое запрещено, выступая в качестве незаконного.

Во-вторых, ПолИБ определяет «правила игры» для всех сотрудников организации и третьих лиц, что позволяет достичь согласия по вопросам ОИБ как внутри самой организации, так и вовне.

В-третьих, ПолИБ помогает сделать правильный выбор платформы для работы с активами, учитывая, какие инструментальные средства и процедуры будут использованы.

Первостепенной целью разработки ПолИБ организации является обеспечение решения вопросов ОИБ в пределах организации и вовлечение ее высшего руководства в данный процесс. Для этого в первую очередь определяется верный с точки зрения организации способ использования ее активов, а также процедуры, предотвращающие нарушения ИБ.

В основе любой политики лежат модели доверия – трастовые модели. Понятие «доверие» возникает тогда, когда один субъект предполагает, что второй субъект будет вести так, как ожидает от него первый, на основе их взаимодействия [86; 87]. Таким образом, доверие имеет дело с предположениями, ожиданиями и поведением. Существует риск, связанный с доверием.

Выделяют три основные трастовые модели:

1) *либеральная* – доверять всем и всегда. Самая простая модель, но непрактичная, поскольку любые пользователи имеют доступ к любым ресурсам независимо от их конфиденциальности. Один проникший в систему злоумышленник, внешний или внутренний, может получить несанкционированный доступ к информации, которая определяет успешность деятельности всей организации;

2) *запретительная* – не доверять никому и никогда. Модель также малоприменима на практике, поскольку существенно огра-

ничивает или даже затрудняет выполнение основных функций практически всех служащих организации, и тогда просто невозможно найти тех, которые согласятся работать в таких условиях;

3) *компромиссная* – доверять иногда некоторым людям и степень доверия периодически пересматривать. Определяет доступ ко всем ресурсам по мере необходимости, например, по запросам от пользователей или руководства организации. Данная модель, как и все предыдущие, предполагает, что в начале работы в системе пользователи уведомляются об их правах доступа, а примеры нарушения прав становятся известны всем сотрудникам организации.

Выбор конкретной модели доверия, с учетом которой разрабатывается ПолИБ, определяется руководством организации.

Среди других причин, побуждающих организацию разрабатывать ПолИБ, выделяют следующие [83]:

1. Требование руководства, обнаружившего недостаток внимания к проблемам ИБ, которые привели к снижению эффективности деятельности организации. Появление таких требований существенно стимулируют серьезные инциденты, повлекшие за собой остановку или замедление работы организации в результате различных локальных и удаленных атак, разглашение конфиденциальной информации или кража компьютеров.

2. Требования законодательства и отраслевых стандартов. ПолИБ позволяет определить правила, в соответствии с которыми часть информации организации будет отнесена к категории коммерческой или служебной тайны, что позволит ее защитить в правовом аспекте (ст. 139 ГК РФ [88]). В зависимости от сферы деятельности организация должна выполнять требования существующего законодательства по соответствующей отрасли. Например, в соответствии со ст. 857 ГК РФ банки должны гарантировать тайну банковского счета и банковского вклада, операций

по счету и сведений о клиенте. Страховщики должны защищать тайну страхования (ст. 946 ГК РФ) и т. п. В соответствии с Указом Президента Российской Федерации от 6 марта 1997 г. № 188 (с изм. от 23.09.2005) «Об утверждении перечня сведений конфиденциального характера» организации должны обеспечивать защиту персо нальных данных сотрудников.

3. Требования клиентов и партнеров о подтверждении необходимого уровня ОИБ для гарантии они могут потребовать юридического подтверждения того, что их конфиденциальная информация защищена надлежащим образом. Именно в ПолИБ есть четкое доказательство намерений организации относительно ИБ.

4. Необходимость сертификации по стандартам (например, ISO/IEC 9001 [89; 90], 27002, 15408 и т. п.), подтверждающей уровень ОИБ для защиты информации и производственных процессов.

5. Устранение замечаний аудиторов и выполнение их рекомендаций. Любая внешняя аудиторская проверка обращает внимание на необходимость формализации производственных процессов, в том числе особое внимание уделяется наличию ПолИБ, на соответствие которой проводится аудит.

6. Обеспечение конкурентоспособности за счет оптимизации производственных процессов и увеличения их эффективности. Правильно реализованная ПолИБ позволяет уменьшить время недоступности сервисов, вызванной инцидентами ИБ, таким образом увеличивая показатель живучести организации.

7. Демонстрация заинтересованности руководства в ОИБ, что значительно увеличивает приоритет безопасности в глазах сотрудников организации.

8. Создание корпоративной культуры ИБ и широкое вовлечение сотрудников в процесс ОИБ. Это достигается путем вве-

дения процедуры обязательного ознакомления с требованиями ПолИБ и подписания соответствующего документа о том, что сотруднику понятны все требования политики, и он обязуется их выполнять. ПолИБ позволяет ввести требования по поддержанию необходимого уровня ИБ в обязанности каждого сотрудника. Важным условием успеха в области ОИБ становится создание в организации атмосферы, благоприятной для поддержания высокого приоритета ИБ.

9. Уменьшение стоимости страхования – важной составляющей управления информационными рисками, основанной на выдаче страховыми обществами субъектам информационных отношений гарантий по восполнению материального ущерба в случае реализации угроз ИБ. Наличие ПолИБ является необходимым и обязательным условием страхования. В России есть компании, предлагающие страховать информационные риски (например, РОСНО, Ингосстрах и др.).

10. Экономическая целесообразность. ПолИБ является самым недорогим и одновременно самым эффективным средством ОИБ за счет его последовательного воплощения и дальнейшего соблюдения в жизни организации.

11. Хорошая практика. Сегодня наличие ПолИБ – правило хорошего тона. Еще в 2002 г. в опросе, проведенном компанией PriceWater HouseCoopers в Великобритании, 67 % компаний выделили именно эту причину создания ПолИБ.

После принятия и утверждения ПолИБ касается каждого сотрудника организации. Определенная часть сотрудников вполне может сопротивляться соответствующим мерам, которые, по их мнению, будут сказываться на результативности их работы. К ним относятся многочисленные процедуры идентификации перед доступом к БД, увеличивающие время работы за компьютером.

Часть пользователей может не признавать запретов, ограничивающих свободу их действий, и рассматривать ПолИБ лишь как меру контроля их поведения (такой контроль в зарубежных научных публикациях характеризуется термином «синдром старшего брата»).

Каждый пользователь имеет представления относительно своей потребности в контроле над безопасностью. Они не всегда совпадают с теми, которые приняты в организации, куда он пришел работать. Если потенциальный сотрудник не разделяет ПолИБ организации, стоит принципиально рассмотреть вопрос о его приеме на работу.

Доступ к активам организации может предоставляться ее сотрудникам, а также в определенных разрезах клиентам, подрядчикам, партнерам и некоторым другим лицам.

Так кто же должен быть заинтересован в ПолИБ? В первую очередь, это сами пользователи, которых ПолИБ касается в наибольшей степени, поскольку регламентирует их каждодневную работу. Далее это вспомогательный персонал систем (системный администратор, администратор ИБ, технический персонал и т. д.), который должен реализовывать на практике и следить за выполнением ПолИБ. И наконец, это руководство организации. Именно оно ответственно перед сотрудниками, клиентами и заказчиками за репутацию организации, ее эффективность.

3.3. Основные требования и принципы разработки и внедрения политики информационной безопасности

ПолИБ как основополагающий документ определяет систему приоритетов, принципов и методов достижения целей защиты активов организации в условиях угроз ИБ. Она содержит основные методологические подходы, позволяющие специалистам

в области ИБ определить наиболее важные объекты, подготовить необходимые меры, принципы и направления защиты.

Поэтому формулировать ПолИБ путем выработки четкой позиции в решении вопросов ИБ должно высшее руководство: президент, председатель, директор, совет директоров или иной уполномоченный. Цель ОИБ не может быть достигнута, пока на высоком уровне не определено, чего следует добиваться, и не выделены ресурсы, позволяющие должным образом защитить информационную инфраструктуру организации и обеспечить управление ею.

ПолИБ организации разрабатывается на основе накопленного в организации опыта в области ОИБ, результатов идентификации активов, подлежащих защите, оценки рисков ИБ, учетом особенностей производственного процесса бизнеса и технологий, требований законодательства Российской Федерации, отраслевых нормативных актов, а также интересов и целей конкретной организации [11].

ПолИБ должна быть [13; 14; 21; 22]:

– утверждена высшим руководством организации и издана;

– реализуема (содержать только те положения, которые могут быть выполнены), а ее реализация контролируема;

– краткой (объемом не более 10 страниц), простой для понимания и не допускать двойного толкования ее положений;

– обеспечивающей защиту и при этом не снижать эффективность работы сотрудников;

– определяющей ответственность руководства и излагать подход организации к управлению ИБ;

– аналитичной, включающей оценивание возможностей для улучшения ПолИБ и подход к управлению ИБ в ответ на изменения в организационном окружении, деловых обстоятельствах, юридических условиях или в технической среде;

– пересматриваться и модифицироваться согласно разработанной заранее процедуре при возникновении значительных изменений в развитии организации. Пересмотр должен включать проверку соответствия ПолИБ актуальной законодательной базе, оценку ее эффективности, исходя из характера, числа и последствий зарегистрированных инцидентов ИБ, определение стоимости мероприятий по управлению ИБ и их влияние на деятельность организации;

– возглавлена ответственным должностным лицом, которое отвечает за ее реализацию и пересмотр в соответствии с установленной процедурой;

– доведена до сведения всех сотрудников организации в доступной и понятной форме, с которой они должны ознакомиться под расписку;

– согласованной с основами теории ИБ, существующими нормативными правовыми документами, соблюдение которых требуется от организации, а также директивами, приказами и общими задачами самой организации.

Выполняя перечисленные требования, можно разработать действительно эффективную ПолИБ, которая будет:

– определять необходимый и достаточный набор требований по ОИБ, позволяющих уменьшить риски ИБ до приемлемой величины;

– основывать на проведенном анализе рисков ИБ, оптимальном уровне риска для организации на основе заданного критерия;

– оказывать минимальное влияние на производительность труда;

– учитывать особенности производственных процессов организации;

– поддерживаться руководством;

– позитивно восприниматься и исполняться сотрудниками.

Разрабатываемая ПолИБ должна обязательно отражать следующие принципы, которыми целесообразно руководствоваться при поддержании ИБ в организации на требуемом уровне [80; 85; 91]:

1. Законность, т. е. осуществление защитных мер в соответствии с действующим законодательством в области ИБ, другими правовыми актами по ОИБ, утвержденными органами государственной власти.

2. Определенность сформулированных целей.

3. Системность, позволяющая учесть все взаимосвязанные и изменяющиеся во времени элементы, условия и факторы, значимые для поддержания ИБ в организации, включая все объекты защиты и направления нарушений ИБ, уязвимости используемых систем, высокую квалификацию злоумышленника и т. п.

4. Комплексный (мультидисциплинарный) подход к разработке ПолИБ, позволяющий учитывать правовые, технические, административные, организационные, учебные, коммерческие и функциональные вопросы.

5. Научная обоснованность и техническая реализуемость защитных мер.

6. Эшелонированность и разнообразие защитных средств (нельзя полагаться на один защитный рубеж, каким бы надежным он ни казался: в интранете за средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией – управление доступом, и как последний рубеж – протоколирование и аудит).

7. Способность защитных мер к интеграции для наиболее эффективного выполнения требования ПолИБ и согласованность применения различных защитных мер при построении системы защиты организации, отсутствие слабых мест при стыковке различных защитных мер, покрытие ими всех объектов защиты.

8. Эффективность и непрерывность защиты, предполагающая целенаправленный непрерывный процесс принятия соответствующих мер на всех этапах жизненного цикла организации.

9. Разумная достаточность, позволяющая выбрать золотую середину между стойкостью защиты и ее стоимостью, потреблением вычислительных ресурсов, удобством работы пользователей и другими характеристиками.

10. Своевременность, адекватность и пропорциональность защитных мер реальным угрозам и рискам ИБ.

11. Гибкость управления и применения защитных мер, позволяющая варьировать уровень защищенности в зависимости от текущей ситуации и потребности организации в ИБ в определенный период времени.

12. Невозможность миновать защитные средства. Применительно к интранету это означает, что все информационные потоки должны проходить через средство фильтрации МЭ; не должно быть «тайных» модемных входов или тестовых линий, идущих в обход него.

13. Усиление самого слабого звена, выявляемого при регулярном обследовании защищаемых активов организации. Ведь злоумышленник предпочитает легкую победу; часто самым слабым звеном оказывается не компьютер или ПО, а человек; тогда проблема ОИБ приобретает не технический характер.

14. Простота защитных средств (защитные средства должны быть интуитивно понятны и просты в использовании).

15. Невозможность перехода защитных средств в небезопасное состояние, т. е. при любых обстоятельствах (включая нештатные), они либо полностью выполняют свои функции, либо полностью блокируют доступ к особо важным активам организации.

16. Наблюдаемость и контролируемость защитных мер (любые защитные меры должны быть такими, чтобы результат их применения был явно наблюдаем (прозрачен) и мог быть оценен подразделением организации, имеющим соответствующие полномочия).

17. Обязательность контроля (мониторинг и аудит) защитных мер и соблюдения ПолИБ, позволяющая своевременно выявлять и пресекать попытки ее нарушения на основе используемых защитных мер при совершенствовании критериев и методов оценки их эффективности.

18. Распределение ролей и ответственности, при котором ни один человек не имеет полномочий, позволяющих ему единолично осуществлять выполнение критичных операций и нарушать критически важный для организации процесс или создавать уязвимости в защите по заказу злоумышленников (важно для предотвращения злонамеренных или неквалифицированных действий системного администратора, сговора между сотрудниками).

19. Минимизация полномочий и привилегий, предписывающая предоставлять пользователям и администраторам систем ИБ только те права доступа, которые необходимы для выполнения служебных обязанностей (цель – уменьшить ущерб от случайных или некорректных действий).

20. Рассмотрение как персональной (для каждого сотрудника в пределах его полномочий), так и групповой ответственности при инцидентах ИБ, чтобы в случае любого нарушения круг виновников был известен или сведен к минимуму.

21. Обеспечение всеобщей поддержки защитных мер, предусматривающее комплекс средств, направленных на обеспечение лояльности персонала и его постоянное теоретическое и практическое обучение.

22. Информированность, когда каждый должен иметь возможность ознакомиться с положениями ПолИБ, знать о тех мерах, практиках и процедурах, на которые она ссылается.

23. Соблюдение этики и учет различных прав и законных интересов сотрудников организации, включая право на частную жизнь.

Этот перечень достаточно полон, но при необходимости он может быть расширен с учетом особенностей организации, разрабатывающей ПолИБ, и сферы ее деятельности.

3.4. Содержание политики информационной безопасности

ПолИБ определяет, что должно быть защищено, и какова ответственность в случае несоблюдения ее положений. Защитные меры отражают механизмы реализации ПолИБ на практике и представляют собой полный перечень всех рекомендаций и действий, которые должны предприниматься в определенных обстоятельствах и при конкретных условиях. Защитные меры выбираются таким образом, чтобы устранить так называемые точки провала. Например, служащий внезапно уволился, и его функции по реализации ПолИБ никому не передали, или вышло из строя и не подлежит восстановлению какое-то средство защиты.

ПолИБ содержит общие требования по ОИБ организации в целом. При этом обязательно учитываются особенности организации и ее деятельности, а также выделяются основные направления, связанные с ОИБ организации, и формулируются основные требования по каждому из них.

Еще один важный момент – вид представления и состав документации. ПолИБ может быть описана в одном большом или ряде менее объемных документов. Несколько документов предпочтительнее, так как их проще обновлять. Для организаций не-

большого размера, конечно, легче изложить всю ПолИБ в одном документе.

В ПолИБ обязательно в явном виде присутствуют ответы на следующие вопросы: что (цель политики), кто (на кого распространяется), где (область действия), как (оценка соблюдения политики), когда (когда вступает в действие), почему (необходимость внедрения) (рис. 3.2) [17].

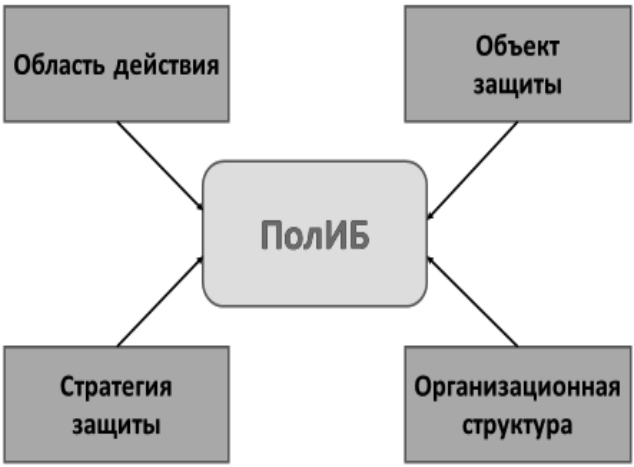

Рис. 3.2. Содержание ПолИБ организации

Выработка конкретных ПолИБ зависит от размера и целей организации. Они должны по возможности носить не рекомендательный, а обязательный характер. Ответственность за их нарушение должна быть четко определена.

Для автоматизации процесса создания ПолИБ и их проверки на соответствие некоторым наиболее популярным международным стандартам предназначены, например, британская система Cobra компании C&A Systems Security Ltd (www.riskworld.net) и российская система «Кондор 2006» компании Digital Security (www.dsec.ru).

3.5. Содержание корпоративной политики информационной безопасности

По своему назначению корпоративная ПолИБ по своей сути является каркасом, объединяющим все остальные документы, регламентирующие обеспечение и управление ИБ в организации. В нее рекомендуется включать следующие положения [75]:

– определение ИБ в терминах деятельности организации, область действия политики, цели, задачи и принципы ОИБ организации;

– изложение намерения ОИБ, направленного на достижение указанных целей и на реализацию принципов ОИБ;

– общие сведения об активах, подлежащих защите, их классификация;

– модели угроз и нарушителей ИБ (внутреннего и внешнего), на противодействие которым ориентирована корпоративная ПолИБ;

– изложение правил и требований по ОИБ, представляющих особую важность для организации (обеспечение соответствия законодательным актам Российской Федерации, нормативным документам в области ОИБ и нормативным актам организации; требованиям к управлению ИБ; требованиям по предотвращению и обнаружению компьютерных вирусов и вредоносного ПО);

– санкции и последствия нарушений корпоративной ПолИБ;

– определение общих ролей и обязанностей, связанных с ОИБ, включая информирование об инцидентах ИБ;

– перечень частных ПолИБ, развивающих и детализирующих положения корпоративной ПолИБ, а также указание подразделениям организации, ответственным за их соблюдение и/или реализацию;

– положения по контролю над реализацией корпоративной ПолИБ;

– ответственность за реализацию и поддержку документа;

– условия пересмотра (выпуска новой редакции) документа.

К разработке и согласованию корпоративной ПолИБ привлекаются представители служб организации, связанных с ее информационной сферой. Корпоративная ПолИБ обязательно утверждается руководителем организации (председатель, генеральный директор, президент), и в ее названии указывается наименование организации.

Цель (назначение)

Корпоративная ПолИБ содержит утверждение, поясняющее, зачем она разработана. Например, если организация предоставляет услуги по поддержке больших БД, тогда ее основными целями могут быть снижение числа ошибок, потерь и искажения данных, а также скорость восстановления после нештатных ситуаций. Для организации, обрабатывающей персональные данные, первостепенной задачей может быть усиленная защита от несанкционированного раскрытия информации о клиентах [78; 79].

Типовыми являются следующие цели:

– обеспечение устойчивого функционирования организации за счет предотвращения реализации угроз ИБ ее активам, защита законных интересов владельца информации от противоправных посягательств, обеспечение нормальной производственной деятельности всех подразделений организации;

– обеспечение уровня ИБ в конкретных функциональных областях, соответствующего нормативным документам организации и риск-ориентированного подхода (с учетом результатов оценки рисков ИБ);

– выработка планов восстановления после критических ситуаций;

– достижение экономической целесообразности при выборе защитных мер;

– анализ регистрационной информации и всех действий пользователей с информационными ресурсами.

Область действия

Перед изложением ПолИБ определяется область ее действия с помощью ограничений и условий, которые представляются в явном виде. Если, например, говорить о ПолИБ при подключении организации к Интернет, то необходимо уточнение, какие соединения (напрямую или опосредованно) охватывает эта политика.

ПолИБ точно определяет, какие активы организации она рассматривает: персонал, информацию, ПО, устройства, технологии и т. п. Например, защищаемые в рамках ПолИБ активы организации можно описать так: «Положения настоящей ПолИБ распространяются на все виды информации, хранящиеся или передающиеся в организации, в том числе на информацию, зафиксированную на материальных носителях или передающуюся в устной или визуальной форме». Корпоративная ПолИБ имеет отношение ко всем системам и сотрудникам организации без исключения.

Основные положения ПолИБ

В явной форме описывается позиция организации по данному вопросу. В ПолИБ требуется кратко описать вес процессы и процедуры СУИБ. В частности, выделяются контроль доступа к активам организации, внесение изменений в ее ИС, взаимодействие с третьими лицами, повышение квалификации сотрудников в области ИБ, расследование инцидентов ИБ, аудит ИБ. В описании каждой процедуры необходимо четко определить цели и задачи процедуры, основные правила ее выполнения, регулярность или сроки выполнения.

Перечисляются конкретные меры, реализующие ПолИБ в организации, дается обоснование выбора именно такого перечня мер и указывается, какие угрозы ИБ для активов наиболее эффективно предотвращаются защитными мерами.

С целью формализации процесса управления ИБ в соответствии с ПолИБ требуется создание организационной структуры, которую следует описать.

Необходимо предусмотреть пересмотр ПолИБ, что может быть изложено, например, следующим образом: «Положения ПолИБ требуют регулярного пересмотра и корректировки – не реже одного раза в полгода. Внеплановый пересмотр политики ИБ проводится в случаях:

– существенных изменений в национальной законодательной базе в области ИБ;

– внесения существенных изменений в интранет организации;

– возникновения инцидентов ИБ.

При внесении изменений в положения политики ИБ организации учитываются:

– результаты анализа функционирования СУИБ со стороны руководства организации;

– результаты аудита ИБ (внешнего и внутреннего);

– рекомендации независимых экспертов по ИБ».

Ответственность (роли и обязанности)

В этом разделе ПолИБ точно устанавливается, кто и за что отвечает. Указывается, на кого конкретно возлагается ответственность за соблюдение ПолИБ (например, менеджеров, владельцев активов, пользователей, администраторов систем). Если для использования ПО сотрудникам требуется разрешение руководства, должно быть известно, у кого и как его можно получить.

Для ПолИБ уместно описание (с краткой детализацией) нарушений, которые неприемлемы, и последствий такого поведения. Могут быть явно перечислены санкции, применяемые к нарушителям ПолИБ.

За нарушение ПолИБ должны быть предусмотрены конкретные дисциплинарные, административные взыскания и матери-

альная ответственность. Но при этом нельзя забывать, что нарушения ПолИБ бывают и непреднамеренными, они могут быть связаны, например, с отсутствием соответствующих знаний.

Устанавливаются как организационные, так и технические меры реагирования на нарушение ПолИБ. Эти меры предусматривают оповещение об инциденте ИБ, соответствующую реакцию, процедуры восстановления, сбор доказательств, проведение расследования и привлечение нарушителя к ответственности. Система мер по реагированию на инциденты ИБ должна быть скоординирована между ИТ-департаментом, службой безопасности и службой персонала.

Также необходимо поставить задачу конкретному подразделению организации следить за соблюдением ПолИБ. Кроме этого, приводится информация о должностных лицах, ответственных за реализацию ПолИБ, и четко устанавливаются их обязанности в отношении разработки и внедрения различных аспектов ПолИБ, а также в случае ее нарушения. Обязанность за общее управление ИБ возлагается на руководство организации. Ответственность сторонних пользователей обязательно оговаривается в соответствующих договорах.

Соблюдение ПолИБ выражается в двух видах соответствий:

— общего, обеспечивающего выполнение требований по разработке ПолИБ и определению ответственности, возложенной на различные организационные структуры поддержания;

— использования установленных санкций и дисциплинарных мер, чем, как правило, занимаются соответствующие структуры, адекватных нарушениям ПолИБ.

Консультанты по вопросам ИБ

Для реализации ПолИБ нужны консультанты, с кем можно связаться в случае необходимости и получить квалифицированную помощь, разъяснения и дополнительную информацию по во-

просам ОИБ. Для решения такого рода вопросов можно назначить сотрудника, занимающего конкретную должность консультанта. Например, по некоторым вопросам консультантом может быть один из менеджеров, по другим – начальник или сотрудник технического отдела, системный администратор или сотрудник службы ИБ. Они должны уметь разъяснять положения ПолИБ и правила работы с конкретной системой. В их обязанности входит ознакомление новых сотрудников организации с ПолИБ при поступлении на работу и сообщение об изменениях в политике по мере их внесения. Должно вестись обучение всех сотрудников основным вопросам ОИБ. Администратор и сотрудники отдела ИБ организации должны регулярно проходить переподготовку с целью повышения квалификации в специализированных учебных заведениях.

Современными стандартами, описывающими общее содержание комплексной ПолИБ организации, являются ISO/IEC 27002:2005 [22] и ГОСТ Р ИСО/МЭК 17799–2005 [13].

В этих документах отмечается, что ПолИБ как неотъемлемая часть общей политики организации включает:

– определение ИБ, ее общих целей и области действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего совместное использование информации;

– изложение целей, принципов и соответствующей стратегии организации, исходя из оценки рисков ИБ;

– краткое изложение наиболее существенных для организации политик, принципов, правил и требований, например, соответствия законодательным требованиям и договорным обязательствам; требования в отношении обучения вопросам ИБ; предотвращения вредоносного ПО; ответственности за нарушения ПолИБ;

– определение обязанностей сотрудников в рамках управления ИБ, включая информирование об инцидентах ИБ;

– ссылки на документы, дополняющие ПолИБ, например, более детальные политики и процедуры безопасности для конкретных ИС.

3.6. Содержание частных политик информационной безопасности

Содержание частных ПолИБ по перечню разделов в целом не отличается от таковых для корпоративной ПолИБ [84]. Все их положения формируются на основании принципов, требований и задач, определенных в корпоративной ПолИБ, с учетом:

– уточнения и дополнительной классификации активов и угроз ИБ;

– определения владельцев защищаемых активов;

– оценки рисков ИБ и возможных последствий реализации угроз ИБ в границах области действия, регламентируемой политикой: области, системы, технологии, подразделения.

Не рекомендуется повторение одинаковых правил в различных частных политиках. Включение в частную ПолИБ правила, содержащегося в другой существующей политике, целесообразно осуществлять посредством соответствующей ссылки.

Частные ПолИБ определяют [75]:

– цели и задачи ОИБ, на обеспечение которых направлена частная ПолИБ;

– область действия, объекты защиты, уязвимости, угрозы ИБ и оценку рисков ИБ, связанных с объектами защиты;

– сведения о виде деятельности, на ОИБ которой направлено действие положений частной ПолИБ, совокупности базовых технологий, применяемых в рамках выполнения данного вида деятельности;

– субъекты, на которых распространяется действие политики (как структурные подразделения организации, так и отдельные исполнители);

– содержательную часть (требования и правила);

– обязанности в рамках действия частной ПолИБ, описание функций субъектов в рамках регламентируемых технологических процессов;

– состав документов, ознакомление с которыми обязательно для адекватного понимания текста политики;

– положения по контролю над реализацией политики;

– ответственность за реализацию и поддержку политики;

– условия модернизации политики.

Вопросы соответствия

Для ряда вопросов политики целесообразно описать ее неприемлемые нарушения. Санкции при этом должны быть сформулированы конкретно и согласованы с кадровой политикой организации, соответствующими должностными лицами и вышестоящими структурами. Необходимо, чтобы конкретное подразделение организации осуществляло контроль над соблюдением такого соответствия.

Контактные лица

Конкретные фамилии в данном разделе не указываются, а пишутся только должности лиц, к которым следует обращаться за дополнительной информацией и разъяснениями.

Например, как это бывает на практике, с вопросами проверки дисков и мобильных устройств, приносимых сотрудниками из дома или привозимых из командировки в другой офис.

Другой пример. В разных подразделениях организации могут применяться различные информационные системы, поэтому частная политика имеет более узкую направленность, чем корпоративная. Она обязательно должна учитывать позицию тех, кто

с этими системами непосредственно работает. Поэтому для частной ПолИБ полезно рассмотреть двухуровневую модель: цели ОИБ и функциональные правила ОИБ, которые тесно взаимосвязаны и часто трудно различимы с технической точки зрения их реализации.

Цели ОИБ системы начинают определяться с анализа обеспечения конфиденциальности, целостности и доступности для достижения основных целей организации. Но только такой общей формулировки недостаточно, цели должны быть указаны более конкретно. Они должны быть достижимы на практике и согласованы с целями других политик организации. Цели должны учитывать допустимые в организации затраты на их достижение, а также функциональные, технические и другие ограничения.

Роли при ОИБ системы

Детализируются и формализуются правила назначения ответственности за ОИБ, правила использования системы и последствия их несоблюдения. При этом выделяются правила функционирования системы. Например, определяется санкционированное и несанкционированное изменение ее настроек, кто (по должности, квалификации) может вносить санкционированные изменения (например, модифицировать, уничтожать данные), при каких условиях. Степень детализации этих положений может быть различна. Чем более точно установлены правила, тем проще выявить, когда и кем они были нарушены, и автоматизировать обнаружение таких событий.

Любые обоснованные отклонения от соблюдения корпоративной ПолИБ или общей практики при работе с рассматриваемой системой должны быть оговорены.

Реализация политики

Описываются все аспекты ОИБ системы, включая организационные, технические и др. Ограничение физического доступа

в помещения, контроль логического доступа, СОВ, защита компьютеров от загрузки с дискет, контроль за работой ПО, регулярный внутренний аудит – лишь некоторые из средств, которые могут применяться при реализации политики на практике.

3.7. Жизненный цикл политики информационной безопасности

Опыт разработки ПолИБ показывает, что жизненный цикл любой из них начинается с определения состава группы разработки и функций каждого сотрудника, входящего в нее. Сразу решается, кто в дальнейшем будет знакомить с ней сотрудников организации и следить за ее реализацией, какие меры будут применяться к тем, кто ее нарушает, а также каковы периодичность и порядок пересмотра ПолИБ в зависимости от изменяющихся условий ведения бизнеса организации (это связано с тем, что соблюдение адекватной ПолИБ в течение длительного времени является практически невыполнимой задачей, так как меняется как окружающая среда, так и сама организация: модифицируются ее активы, информационная инфраструктура и т. п.).

Следующий шаг – это способ выработки ПолИБ, т. е. на основе какой информации будет определяться политика, кем эта информация представляется и какова степень доверия к ней. Как показывает практика, нельзя включать в рассмотрение те факторы, которые часто меняются. Нельзя сводить ПолИБ лишь к детальному плану реализации основных мер по защите всех активов организации (например, недопустима ориентация на конкретные средства защиты и указание конкретных версий продуктов конкретных производителей, иначе при появлении новых версий и выпуске средств новых производителей придется пересматривать всю ПолИБ).

На этом этапе создания ПолИБ необходимо получить ответы руководства, клиентов и пользователей отдельных сервисов ор-

ганизации и всех заинтересованных лиц на следующие вопросы: какие ожидания пользователи и клиенты возлагают на ОИБ организации? Потеряет ли организация клиентов, если ее ИБ будет обеспечена недостаточно серьезно или, если она будет обеспечена настолько серьезно, что это затруднит выполнение ими своих обычных обязанностей? Сколько времени простоя или какие материальные потери уже принесли нарушения ИБ организации в прошлом? Обеспокоена ли организация угрозами ИБ, исходящими от внутренних пользователей? Может ли она доверять своим пользователям? Сколько конфиденциальной информации находится в интерактивном режиме доступа (онлайн) в сети организации? Каковы предполагаемые потери организации, если эта информация будет скомпрометирована или украдена? Нужны ли организации различные уровни ИБ для разных подразделений и категорий пользователей? Существуют ли в организации руководящие принципы, регламентирующие ОИБ, инструкции или законы, которые требуется выполнять? Если да, то следуют ли этим руководящим принципам и правилам в организации? Имеют ли требования основного бизнеса организации приоритет над требованиями по ОИБ при их несоответствии? Если да, то поощряется ли такой подход в организации? Насколько важны конфиденциальность, целостность и доступность информации для полноценной работы организации? Являются ли решения, которые принимаются в организации, соответствующими потребностям ее бизнеса и ее экономическому положению?

После ответа на все эти и, несомненно, другие важные вопросы определяется содержание самой ПолИБ и начинается ее написание.

Руководствуясь признанными в организации принципами ОИБ, проведя идентификацию активов и производственных процессов, оценив риски ИБ, учитывая собственный опыт и лучшие

мировые практики, извлекая уроки по результатам постоянного мониторинга ИБ, разрабатывают две модели ИБ: угроз и нарушителей. Все это вместе является основой ПолИБ.

После соответствующих процедур согласования и утверждения ПолИБ вступает в силу, реализуется силами всех определенных заранее должностных лиц и соблюдается всеми, к кому она применима. ПолИБ является основным документом, выполнение которого на практике оценивается при проведении аудита ИБ (как внешнего, так и внутреннего) и каждодневного мониторинга событий, влияющих на ИБ.

Упрощенный взгляд на разработку и реализацию ПолИБ представлен на рис. 3.3.

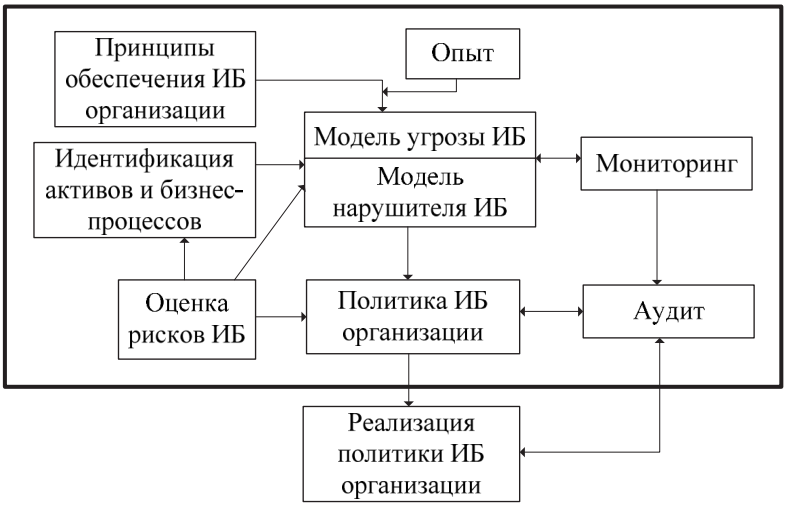

Рис. 3.3. Разработка и реализация ПолИБ

При более детальном рассмотрении в жизненном цикле ПолИБ можно выделить четыре основные стадии: разработку, внедрение, применение, аннулирование, – и соответствующие им 11 шагов, которые нужно выполнить при работе с ПолИБ – начиная с написания и заканчивая изъятием из обращения (рис. 3.4) [80].

На стадии разработки ПолИБ пишется, в нее вносятся одобренные после обсуждения коррективы и в соответствии с установленной заранее процедурой ПолИБ утверждается. Затем на стадии внедрения ПолИБ доводится до сведения всех заинтересованных лиц (сотрудники, бизнес-партнеры, клиенты), обеспечивается ее соответствие всем необходимым стандартам, нормам и требованиям и непосредственное соблюдение, а также определяются исключительные случаи (исключения), когда она невыполнима.

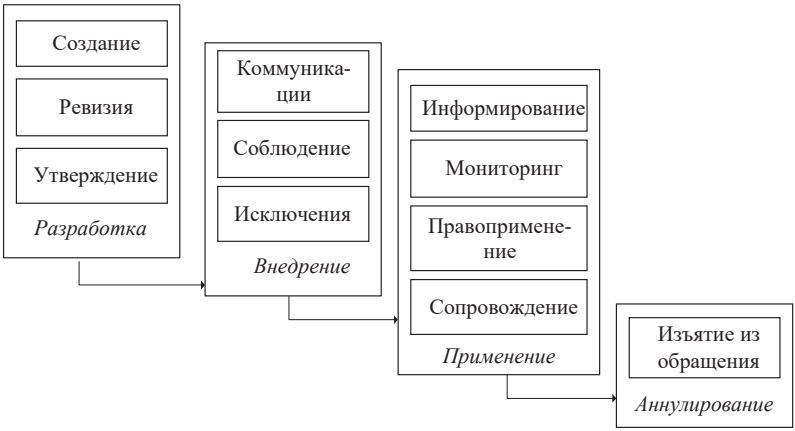

Рис. 3.4. Стадии жизненного цикла ПолИБ

На стадии применения ПолИБ поддерживается в актуальном состоянии (в нее вносятся соответствующие текущему уровню развития организации изменения), ее основные положения с изменениями доводятся до сведения всех заинтересованных лиц, а также постоянно проверяется ее соответствие всем установленным требованиям. Также должным образом контролируется исполнение ПолИБ всеми, на кого она распространяется.

На стадии аннулирования, чаще всего после ее замены новой редакцией или совершенно новым по содержанию документом, ПолИБ изымается из обращения в связи с ненадобностью.

Все шаги жизненного цикла ПолИБ должны быть обязательно выполнены, а некоторые из них, такие как сопровождение, информирование, мониторинг соблюдения и правоприменение, выполняются итерационно во время всего жизненного цикла.

Разработка политики ИБ

Это длительный и трудоемкий процесс, требующий высокого профессионализма, отличного знания нормативной базы в области ИБ и, помимо всего прочего, писательского таланта. Не всегда создание ПолИБ нужно начинать с нуля. Во многих случаях можно воспользоваться существующими наработками, ограничившись адаптацией типового комплекта ПолИБ к специфическим условиям конкретной организации. Этот путь часто позволяет сэкономить многие месяцы работы и повысить качество разрабатываемых документов. Кроме того, он является единственно приемлемым в случае отсутствия в организации собственных ресурсов для квалифицированной разработки ПолИБ.

Сначала разрабатывается корпоративная ПолИБ, затем – частные политики.

Как было отмечено выше, в стадию разработки ПолИБ входят ее создание и согласование (включая коррекцию), ревизия и утверждение.

Создание или написание ПолИБ

Этот самый четко формализованный шаг жизненного цикла ПолИБ включает в себя деятельность по планированию, проведению различных исследований, документированию необходимой информации и написанию самой ПолИБ. На данном этапе обязательно осуществляются следующие мероприятия:

– определяется, зачем ПолИБ нужна в организации;

– устанавливаются границы и область действия;

– выделяются роли и ответственность, связанные с реализацией и внедрением ПолИБ;

– назначается группа конкретных людей, которые будут участвовать во всех процессах создания политики;

– оценивается осуществимость реализации ПолИБ.

Также выявляется применимость различных требований к разработке ПолИБ конкретной организации (требования утверждающих политику, требования по ее согласованию, формат и т. д.), и проводятся исследования в соответствии со стандартизованными для различных отраслей лучшими практиками.

По мере необходимости осуществляется координация деятельности между всеми участвующими в процессе создания ПолИБ сторонами как внутри, так и вне организации. Рекомендуется следующий состав рабочей группы по разработке ПолИБ [92]:

– член совета директоров;

– представитель руководства организации (президент, директор, финансовый директор, директор по развитию и т. п.);

– директор департамента информатизации (автоматизации);

– директор департамента ИБ;

– представитель юридического отдела;

– аналитик ИТ-службы;

– аналитик службы безопасности;

– представитель пользователей;

– технический писатель.

Результатом данного шага является написанная политика, соответствующая стандартам и процедурам, принятым в организации.

Независимая оценка ПолИБ

Как показывает практика, желательно, чтобы до начала ее использования в организации ПолИБ подверглась критической оценке. На этом шаге осуществляется независимая оценка

ПолИБ, предшествующая окончательному ее утверждению. В процессе оценки должны рассматриваться не только технические, но и юридические аспекты ОИБ, поскольку политика имеет непосредственное отношение к практической деятельности организации и напрямую затрагивает работу ее персонала.

Обычно назначается специальная комиссия по оценке ПолИБ, которая анализирует и оценивает ее жизнеспособность. Эта комиссия состоит из группы заинтересованных лиц, работающих в организации, которые несут ответственность за то, чтобы ПолИБ была понятна, полностью согласована и выполнима с точки зрения людей, процессов и технологий, которых она затрагивает. Из-за большого объема ПолИБ комиссия не имеет возможности оценить в короткие сроки все описанные процедуры ОИБ, но к этому нужно стремиться. Особо важные процедуры должны быть оценены обязательно.

Достоинства такой оценки не подлежат сомнению: ПолИБ получается более жизнеспособной, поскольку ее проверяют те, кто может иметь несколько отличные или более широкие взгляды, чем взгляды создателей политики; более широкая поддержка ПолИБ за счет увеличения числа заинтересованных лиц; доверие к ПолИБ возрастает из-за привлечения к ее оценке специалистов различных профилей.

На этом шаге разработки ПолИБ осуществляются следующие действия:

– ПолИБ формально или неформально представляется оценщикам;

– решаются все вопросы, которые могут возникнуть во время оценки;

– обосновывается, почему ПолИБ необходима организации, и объясняются цели, содержание и потенциальная польза от ПолИБ. Разработчики политики дают свои комментарии оценщикам, вы-

рабатывают рекомендации по ее изменению, учитывают важные замечания и вносят изменения в окончательную редакцию, которая после этого готова к утверждению.

Также проводится оценка ПолИБ со стороны самого руководства организации. Входными данными для этого являются следующие сведения [13; 22]:

– обратная реакция заинтересованных сторон;

– результаты независимых анализов;

– статус корректирующих действий;

– результаты анализа со стороны руководства;

– выполнение процессов и соблюдение ПолИБ;

– изменения, которые могут повлиять на подход организации к управлению ИБ, включая изменения в окружении организации, направленности ее производства, доступности ресурсов, в договорных, нормативных и юридических условиях или технической среде;

– тенденции, связанные с угрозами ИБ и уязвимостями;

– инциденты ИБ;

– рекомендации, представленные соответствующими органами.

Отчет с результатами анализа ПолИБ со стороны руководства включает решения и действия, касающиеся улучшения подхода организации к управлению ИБ и ее процессами, целей и средств управления и распределения ресурсов и/или обязанностей.

Утверждение ПолИБ

Данный процесс представляет одобрение руководством окончательной редакции документа. На бумажном документе с ПолИБ ставится подпись уполномоченного должностного лица организации, после чего ПолИБ готова к непосредственному использованию.

Утверждение требует от разработчиков ПолИБ выполнения ряда действий:

– дать обоснованные разъяснения официальному лицу, имеющему полномочия утвердить ПолИБ;

– координировать все действия по утверждению ПолИБ с этим официальным лицом;

– представить рекомендации, появившиеся после оценки ПолИБ;

– предпринимать должные усилия по расширению поддержки ПолИБ со стороны руководства организации.

Если уполномоченное лицо не полностью одобряют ПолИБ, разработчики политики должны решить вопрос ее временного утверждения.

Внедрение политики ИБ

После официального утверждения ПолИБ начинает претворяться в жизнь. Опыт показывает, что с наибольшими трудностями организациям приходится сталкиваться именно на этом этапе, который, как правило, связан с необходимостью решения технических, организационных и иных проблем. Часть пользователей может сознательно либо бессознательно сопротивляться введению новых правил поведения, которым теперь необходимо следовать, а также программно-техническим механизмам защиты информации, в той или иной степени неизбежно ограничивающим доступ к информации.

Чтобы внедрение завершилось успешно, должна быть создана группа по внедрению ПолИБ, действующая по согласованному плану в соответствии с установленными сроками выполнения работ.

В стадию внедрения ПолИБ входят три основных шага: коммуникации по ее распространению, собственно соблюдение ПолИБ теми, на кого она распространяется, и обработка исключительных ситуаций.

Коммуникации. Основной целью данного шага является распространение ПолИБ внутри организации и среди тех, на кого

она распространяется: партнеров, клиентов и т. д. При этом обязательно:

– определяются степень и метод начального распространения политики;

– решаются языковые проблемы;

– предотвращается несанкционированное распространение;

– устанавливается система контроля за распространением.

Для повышения эффективности перечисленных мероприятий разрабатывается и реализуется план, в котором рассматриваются все эти вопросы, а также выделяются ресурсы для данного шага, документируется ознакомление сотрудников с ПолИБ и вырабатываются способы повышения ее наглядности.

Соблюдение ПолИБ. Этот шаг заключается в непосредственном выполнении ПолИБ и всех ее требований на практике, для чего:

– проводится работа с сотрудниками, разъясняющая, как наилучшим образом исполнять ПолИБ в различных ситуациях и организационных моментах;

– обеспечивается понимание политики теми, от кого требуется ее реализация, контроль и поддержка соблюдения;

– осуществляется мониторинг, отслеживание и составление отчетности по темпам, масштабам и эффективности деятельности по осуществлению ПолИБ;

– измеряется непосредственное влияние политики на деятельность организации;

– проводится информирование руководства о ходе осуществления ПолИБ.

Систематизируя лучшие практики по эффективному внедрению ПолИБ, можно сделать вывод, что ее соблюдение ПолИБ в значительной степени является элементом корпоративной этики.

Поэтому на уровень ИБ организации серьезное влияние оказывают отношения как в коллективе, так и между коллективом и собственником или руководством, представляющим интересы собственника. Следовательно, этими отношениями необходимо грамотно и своевременно управлять. Понимая, что наиболее критичным элементом ОИБ организации является ее персонал, собственник должен всемерно поощрять заинтересованность и осведомленность персонала в решении проблем ИБ и строгом соблюдении ПолИБ [11].

Исключения из ПолИБ. Основная деятельность на этом шаге – разрешение ситуаций, когда исполнение ПолИБ невозможно либо частично, либо полностью. Из-за нехватки времени, персонала и других эксплуатационных требований не все политики могут быть выполнены так, как это первоначально предполагалось. Таким образом, исключения из политики, в полной мере не отвечающие ее требованиям, рассматриваются и согласуются с соответствующими лицами, возможно, с руководством организации.

Определяется процедура фиксации запросов в соответствующие службы на признание, отслеживание, оценку и одобрение/неодобрение исключений. После этого такие исключения документируются и контролируются на протяжении утвержденного срока признания исключения. Все наиболее часто повторяющиеся исключения из политики, а также временные отказы от выполнения требований из-за краткосрочных обстоятельств фиксируются. Данной деятельностью может заниматься упомянутая выше комиссия, проводящая оценку ПолИБ.

Применение политики ИБ

За внедрением ПолИБ логически следует этап ее применения. В него входят информирование, мониторинг, правоприменение и сопровождение.

Информирование о ПолИБ. Этот шаг включает постоянную деятельность по ознакомлению сотрудников организации и всех заинтересованных лиц и лиц, на которых она распространяется, с содержанием ПолИБ с целью выполнения ими ее требований. Для этого:

– определяются потребности в информировании различных целевых групп (исполнители, руководители, пользователи и т. д.) в рамках организации;

– устанавливаются наиболее эффективные методы информирования для каждой из групп: брифинги, обучение, рассылки сообщений и т. п.;

– разрабатываются и распространяются различные информационные материалы о необходимости соблюдения ПолИБ: видеоролики, презентации, плакаты, почтовые рассылки и т. д.;

– измеряется уровень информированности сотрудников о ПолИБ (например, посредством тестирования), и по полученным результатам данная деятельность корректируется.

Информирование также включает в себя освещение вопросов соответствия ПолИБ текущему бизнесу организации и правоприменения политики (с разъяснением наказаний за ее нарушение), а также рассмотрение текущих угроз ИБ, что свидетельствует об актуальности и реальности проблем ОИБ в организации.

В различных стандартах и рекомендациях в области ИБ особо отмечается, что необходимо не просто довести содержание ПолИБ до сведения всех целевых групп, но также провести обучение и дать необходимые разъяснения сомневающимся, которые пытаются обойти новые правила и продолжать работать по-старому.

За осуществление информирования назначаются ответственные (в пределах организации, если рассматривать, например, корпоративную ПолИБ, или в пределах подразделений, если

рассматривать частные ПолИБ). Обычно они работают совместно с департаментом персонала или департаментом, отвечающим за обучение персонала, что обеспечивает общность их совместных действий и оптимизирует использование задействованных в процессе информирования ресурсов. Такими ответственными чаще всего становятся сотрудники департамента ИБ.

Мониторинг ПолИБ. Соблюдение положений и требований ПолИБ является обязательным для всех сотрудников организации и должно непрерывно контролироваться. Информация для отслеживания и написания отчетов по эффективности соблюдения ПолИБ собирается из разных источников: наблюдений сотрудников и руководителей, отчетов с результатами различных плановых проверок (внешний и внутренний аудит ИБ, различные оценки, анализы и т. п.) и постоянного мониторинга в ИС (в первую очередь, на основе журналов регистрации событий, влияющих на ИБ этих систем), а также отчетов и действий при реагировании на инциденты ИБ.

В данном контексте мониторинг заключается в постоянной деятельности по контролю за соблюдением или несоблюдением ПолИБ с использованием формальных и неформальных методов и подготовке отчетов для соответствующих лиц с целью принятия определенных мер.

Проведение систематически повторяемого (по заранее составленному графику) планового внешнего или внутреннего аудита ИБ является одним из основных методов контроля жизнеспособности ПолИБ, позволяющего оценить эффективность ее использования. Результаты аудита ИБ могут служить основанием для пересмотра некоторых положений ПолИБ и внесения в нее необходимых корректировок.

Ответственность за осуществление деятельности в рамках мониторинга распределяется между всеми сотрудниками и руко-

водителями организации, внутренними аудиторами, сотрудниками, отвечающими за ИБ, и т. д.

Каждый сотрудник, на которого распространяются определенные требования по ОИБ в соответствии с ПолИБ, должен помогать в проведении мониторинга ПолИБ, сообщая обо всех замеченных отклонениях как в самой политике, так и защитных мерах, реализующих ее.

Правоприменение ПолИБ. Правоприменение включает в себя ответную реакцию со стороны руководства на действия или бездействие, результатом которых стали нарушения ПолИБ. Это означает, что как только нарушение выявлено, определяются соответствующие корректирующие действия, которые применяются к нарушителям (в виде дисциплинарных мер), а также к процессам (их изменение) и технологиям (их обновление), что в дальнейшем предотвращает или затрудняет повторение подобных нарушений в будущем. Как уже отмечалось выше, включение информации о таких корректирующих действиях в информирование целевых групп является достаточно эффективным средством.

Основная ответственность за осуществление данной деятельности возлагается на руководителей, сотрудников, на которых распространяется ПолИБ.

Сопровождение ПолИБ. Данный шаг состоит в обеспечении широкого применения и поддержания целостности ПолИБ. Он включает следующие действия:

– отслеживаются основные побудительные мотивы и события для внесения изменений в ПолИБ (например, изменения в технологиях, процессах, людях, самой организации, направленности производства), которые могут влиять на политику;

– вырабатываются рекомендации и согласуются коррективы, которые требуется внести в ПолИБ в соответствии с вышеперечисленными изменениями;

– осуществляется документирование изменений в ПолИБ и регистрируется деятельность по ее корректировке.

Все это обеспечивает как постоянную доступность ПолИБ для всех сторон, на которых она распространяется, так и поддержание целостности политики посредством эффективного контроля ее редакций. Если в ПолИБ требуется внести изменения, то должны быть обязательно повторно выполнены шаги по пересмотру, утверждению, информированию, коммуникациям и соблюдению.

Ответственность за выполнение данного шага применительно к различным политикам несут все, на кого они распространяются: от руководства организации до ответственных за ИБ в подразделениях и рядовых сотрудников.

Аннулирование политики ИБ

Заключительная стадия жизненного цикла ПолИБ. Чтобы избежать путаницы, отслужившая свой срок «лишняя» политика удаляется из перечня действующих, архивируется для дальнейших ссылок на нее, а решение об отмене ПолИБ (включая обоснование, дату и т. д.) документируется.

Изъятие из обращения устаревшей редакции ПолИБ, которая уже послужила своей цели, производится по различным причинам.

Первая из причин состоит в том, что ПолИБ не в полной мере отвечает всем потребностям организации, уже не охватываются все области, которые должны быть регламентированы сформулированными в политике требованиями. На стадии разработки организации часто пытаются реализовать ПолИБ без проведения ее независимой оценки, в результате политики не очень хорошо продуманы и надлежащим образом одобрены. Недальновидные руководители часто не уделяют должного внимания рассмотрению исключений (стадия внедрения ПолИБ), ошибочно думая, что не может быть таких обстоятельств, при которых соблюде-

ние политики невозможно. Многие организации не в состоянии постоянно оценивать потребность в установленной ПолИБ на стадии ее применения, принижают важность обеспечения ее целостности и доступности политики. Скорее всего, после наблюдения за процессом применения ПолИБ и оценки эффективности ее использования потребуется выполнить ряд существенных доработок. Тогда появится потребность в новой редакции той же ПолИБ.

Вторая причина – это то, что организация больше не применяет технологию, для которой разрабатывалась ПолИБ, или используемые технологии и организация производственных процессов существенно изменились, что приводит к необходимости корректировать существующие подходы к ОИБ и отказаться от данной ПолИБ как таковой.

Ответственностью за аннулирование ПолИБ наделяется соответствующее официальное лицо в организации.

3.8. Ответственность за исполнение политики информационной безопасности

Согласно основным стандартам в области ИБ [13; 14; 21; 22], для полноценной реализации всех стадий и шагов жизненного цикла ПолИБ и адекватного назначения ответственности за их осуществление в организации создается соответствующая инфраструктура, обеспечивающая правильное понимание и постоянное исполнение политики, устанавливающая иерархические связи взаимоподдерживающих друг друга уровней и эффективно подстраивающаяся под частые изменения технологического и организационного характера. Обязательно определяются специалисты, непосредственно осуществляющие деятельность по управлению ИБ и таким образом внедряющие основные положения ПолИБ, например, обучающие сотрудников, разраба-

тывающие критерии для оценки эффективности, планирующие мероприятия по управлению ИБ.

Обычно создается рабочая группа по управлению ИБ, в которую, как правило, включены руководители различных подразделений организации. В обязанности группы входит утверждение документов по ОИБ, разработка и утверждение стратегии управления рисками ИБ, контроль выполнения процедур СУИБ, оценка эффективности функционирования СУИБ и др.

Также определяются назначаемые сотрудникам роли, связанные со всеми стадиями жизненного цикла ПолИБ. Под ролью понимается заранее определенная совокупность правил, устанавливающая допустимое взаимодействие между субъектом и объектом [11]. К субъектам могут относиться сотрудники, клиенты, партнеры и иные лица и инициируемые от их имени процессы по выполнению действий над объектами. Объектами, в свою очередь, могут быть программные и аппаратные средства, информационные ресурсы, сервисы, процессы, системы. При этом необходимо учитывать:

– производственные цели организации и цели ОИБ, а также необходимые и достаточные ресурсы для реализации этих целей;

– функциональные и процедурные требования;

– разделение производственного процесса на подпроцессы для присвоения ролей, руководствуясь принципом «один процесс – несколько ролей»;

– возможность группирования и взаимодействия ролей;

– наличие контроля своевременности и качества выполнения ролей, для чего определяются дополнительные роли по ОИБ и критерии оценки эффективности выполнения правил для каждой роли, иначе могут возникнуть новые уязвимости;

– установление ответственности за выполнение каждой роли. Практика использования ПолИБ в различных организаци-

ях показывает, что наиболее часто используемыми типовыми ролями являются:

1) создатель ресурса – сотрудник, непосредственно создавший ресурс;

2) владелец ресурса – сотрудник, несущий конечную ответственность за ИБ ресурса и определяющий правила использования ресурса. Он организует ОИБ своего ресурса в виде формализованных правил, технических политик, настроек конфигурации, организационных мероприятий и регламентов;

3) пользователь ресурса – сотрудник, привлеченный работник, использующий ресурс для своих производственных задач и несущий ответственность согласно корпоративным стандартам в рамках правил, определенных владельцем;

4) администратор ресурса – сотрудник, ответственный за применение правил использования ресурса, определенного владельцем. Он обязан осуществить и поддерживать настройку среды работы ресурса для применения технических средств, обеспечивающих поддержку правил использования ресурса. Он должен сообщать контролеру и/или владельцу о нарушениях, недостатках и ошибках, выявленных при работе с ресурсом;

5) контролер ресурса – сотрудник, ответственный за соответствие ресурса правилам, которые установлены владельцем. Он обязан имеющимися средствами мониторинга и аудита обеспечить уверенность в соблюдении пользователями и администраторами правил использования ресурса либо выявлять факты нарушения таких правил. Контролер обязан принять меры для прекращения и предотвращения нарушений.

Подобное распределение ролей позволяет правильно планировать процессы и обязанности отдельных субъектов. Если при разработке ПолИБ обнаруживается, что роли пересекаются, это дает повод усомниться в правильности планиро-

вания данного процесса либо распределения обязанностей его субъектов.

Ответственность за исполнение ПолИБ имеет непосредственное отношение к управлению ИБ в организации. Все вопросы, которые так или иначе относятся к человеческому фактору, эффективнее всего решаются при участии департамента персонала. Ответственность, связанная с непосредственным выполнением процедур ОИБ, существенно зависит от технического аспекта и, следовательно, определяется совместно с представителями департаментов, сопровождающих работу программных и аппаратных средств. Эти процедуры часто выполняются децентрализованно (в разное время, «на местах» – в географически удаленных друг от друга офисах одной организации), но они должны обязательно быть согласованы с общей корпоративной ПолИБ и проверены для установления возможности их выполнения при оценке политики.

Ответственность на различных стадиях жизненного цикла ПолИБ во многом похожа (особенно это касается подготовки, информирования, сопровождения и аннулирования), но имеется и ряд различий. Они, прежде всего, связаны с тем, в рамках какой ПолИБ – корпоративной или частной – описывается ответственность.

Рассмотрение ответственности, связанной с ПолИБ, возможно и с других точек зрения. Ответственность по ОИБ активов организации может быть долгосрочной, возлагаемой на весь период жизненного цикла политики, или краткосрочной, предполагающей выполнение обязанностей в повседневной деятельности. Ответственность может возлагаться на всех сотрудников организации, что относится к корпоративной или частной ПолИБ для одной технологии или одной системы, эксплуатируемой во всех подразделениях организации, или на часть со-

трудников, работающих в одном или нескольких подразделениях с только там используемой системой или технологией. Контроль выполнения обязанностей в отношении ПолИБ может осуществляться централизованно или децентрализованно (чаще в отношении соблюдения частных ПолИБ) силами самой организации и ее подразделений. При вовлечении в соблюдение ПолИБ сторонних лиц, не работающих в данной организации на постоянной основе, возлагаемая на них ответственность может контролироваться из самой организации лишь в ограниченном объеме.

Выделяют несколько основных принципов, которыми руководствуются, устанавливая ответственность и распределяя роли и обязанности, связанные с ПолИБ [80].

Принцип разделения полномочий (обязанностей) предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Данный принцип должен применяться при определении ответственности за конкретную функцию ОИБ в соответствии с требованиями ПолИБ, что обеспечивает выполнение необходимых проверок и баланса между обязанностями. При этом нельзя допускать конфликта интересов. Так, например, не следует совмещать обязанности по разработке, сопровождению, исполнению, администрированию или контролю систем с обязанностями исполнителя и администратора, администратора и аудитора, разработчика и аудитора [11].

Руководствуясь соображениями эффективности, может потребоваться возложить ответственность за определенные функции в отношении ПолИБ не только на главного ответственного за ПолИБ, но и на других сотрудников организации. Например, распространение политики и коммуникации по вопросам ПолИБ лучше всего могут осуществить подразделения, обычно исполняющие подобные функции (например, департамент коммуника-

ций и т. п.). С другой стороны, деятельность по информированию эффективнее всего реализуется подразделением, занимающимся вопросами обучения сотрудников организации. Например, учебный департамент может оказать поддержку при начальном распространении политики и в оценке эффективности деятельности по информированию сотрудников. Такая деятельность должна осуществляться на постоянной основе, поскольку она хорошо контролирует соблюдение ПолИБ и правоприменение ее положений, и определять требования по обновлению программ информирования, каждая из которых является важным элементом эффективного повышения осведомленности сотрудников организации в вопросах, относящихся к политике.

Границы и время средств управления в отношении ПолИБ влияют на установление ответственности за выполнение конкретных требований политики. Как правило, ответственный за ПолИБ играет лишь ограниченную роль в мониторинге ее соблюдения, поскольку он должен одновременно участвовать во всех процессах реализации политики.

Руководители среднего звена из-за их близости к обычным сотрудникам, подпадающим под действие ПолИБ, могут наиболее эффективно контролировать и обеспечивать соблюдение политики и поэтому должны нести ответственность за эти функции. Именно они могут гарантировать, что ПолИБ в настоящее время соблюдается, а все ее нарушения своевременно и эффективно рассматриваются.

Ограничения на полномочия соответствующего органа или лица также могут повлиять на успешное исполнение требований ПолИБ. Эффективность политики часто оценивается ее наглядностью и важностью, придаваемой ей руководством организации, и во многих случаях зависит от уполномоченных органов и лиц, на которых возлагается ответственность за ее внедре-

ние и контроль за соблюдением. Чтобы политика имела широкую поддержку, утверждающее ее должностное лицо должно иметь в пределах организации, признанные всеми полномочия. Как правило, функции по ОИБ в соответствии ПолИБ распределяются между различными подразделениями и требуют поддержки при их исполнении со стороны руководства верхнего уровня. Следовательно, ответственность за внедрение и соблюдение ПолИБ лучше всего возлагать на исполнительную дирекцию организации.

Привлечение комиссии по оценке ПолИБ может обеспечить более широкое понимание деятельности, на которую распространяется политика. Ее компетентная оценка поможет правильно написать ПолИБ, что будет способствовать ее принятию и успешной реализации. Эта оценка может быть также использована для прогнозирования потенциальных проблем с реализацией ПолИБ и эффективной оценки ситуаций, когда оправданы исключения из политики.

Должна быть ответственность за осуществление ПолИБ на всех стадиях ее жизненного цикла и отдельных шагах. На какую часть организации распространяется ПолИБ? Применима она только к одному подразделению, пользователям отдельной технологии или ко всей организации в целом? От ответа на эти вопросы зависит ответственность соответствующих лиц на уровне всей организации или ее отдельных технологий и систем.

Рекомендуется, чтобы все сотрудники организации давали письменное обязательство о соблюдении конфиденциальности, приверженности правилам корпоративной этики, включая требования по недопущению конфликта интересов [11]. При этом условие о соблюдении конфиденциальности должно распространяться на всю защищаемую от разглашения информацию, доверенную сотруднику или ставшую ему известной в процес-

се выполнения им своих служебных обязанностей. Обязанности сотрудников по выполнению требований ИБ в соответствии с ПолИБ должны включаться в трудовые контракты (соглашения, договоры). При приеме на работу новые сотрудники также должны подписывать соглашения об обязательности выполнения требований ПолИБ. При изменении служебных обязанностей сотрудников документы должны быть пересмотрены и подписаны заново. Для внешних организаций требования по соблюдению ПолИБ должны регламентироваться положениями, включаемыми в договоры (соглашения).

ПолИБ не должна налагать обязанности, которые невыполнимы на практике. Это будет провоцировать сотрудников на нарушение политики. Например, до сих пор встречаются требования ежедневно полностью сканировать жесткий диск рабочей станции на наличие вирусов. Или требование официально оформлять каждый, даже самый мелкий инцидент ИБ. Понятно, что буквальное выполнение таких требований может просто парализовать производственный процесс.

Вопросы для самоконтроля

1. Какие определения ПолИБ даются в различных международных стандартах?
2. В чем различие политик, стандартов, правил и процедур ОИБ?
3. Что такое трастовые модели?
4. С каких точек зрения и как можно описать виды ПолИБ?
5. Что понимают под ПолИБ в широком и узком смысле?
6. Для чего разрабатываются организационные (административные) и технические ПолИБ?
7. Перечислите основные требования, предъявляемые в различных источниках к ПолИБ.

8. Каковы основные принципы, позволяющие разработать эффективную ПолИБ?

9. Каково содержание документа, описывающего корпоративную ПолИБ? Что излагается в каждом из разделов этой политики?

10. Перечислите типовые цели корпоративной ПолИБ.

11. Каковы отличительные особенности содержания частной ПолИБ для отдельной области, требующей ОИБ, и для отдельной системы, используемой в организации? Что общего между этими политиками? Что излагается в каждом из разделов этих политик?

12. Перечислите основные стадии жизненного цикла ПолИБ. Из каких шагов они состоят? Какие из этих шагов выполняются итерационно и почему?

13. Сформулируйте цель и основные мероприятия, осуществляемые на каждом шаге жизненного цикла ПолИБ.

14. Как происходит процесс информирования в отношении ПолИБ?

15. Для чего и кем осуществляются ревизия, мониторинг и аудит ПолИБ?

16. Что понимается под исключениями из ПолИБ?

17. Зачем необходим пересмотр ПолИБ?

18. В каких случаях ПолИБ может быть аннулирована?

19. Что такое роль? Какие роли связаны с использованием ПолИБ?

20. Какие виды ответственности связаны со стадиями жизненного цикла ПолИБ?

21. Какими принципами необходимо руководствоваться при установлении ответственности в отношении соблюдения ПолИБ?

Глава 4. СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

4.1. Управление обеспечением информационной безопасности организации

Как подчеркивается в различных стандартах по ОИБ [11; 13; 14; 21; 22], для противодействия угрозам, снижения рисков и эффективной обработки инцидентов ИБ необходимо обеспечивать и на протяжении длительного времени сохранять достаточный уровень ИБ. Поэтому в настоящее время ОИБ является одним из основополагающих аспектов успешной производственной деятельности организации.

В современных условиях ОИБ присущи следующие специфические черты [93; 94]:

1. *Прогнозный характер проблем и задач в области ОИБ.* Подобно общему управлению организацией, управление ИБ включает задачи прогнозирования, ориентированные на предвидение возникновения нарушений ИБ. Этот прогноз включает выявление причинно-следственных связей возможных проблем, моделирование действий нарушителей ИБ и последствий от их действий, планирование необходимых защитных мер и оценку положительного эффекта от их применения.

2. *Деградация мер и средств, обеспечивающих ИБ.* Даже в отсутствие злоумышленной деятельности, требующей специального вмешательства, защитные меры со временем неминуемо деградируют, в результате чего риски ИБ возрастают. Это связано с тем, что угрозы, их источники и риски ИБ через некоторое время изменяются под воздействием среды организации.

Другая причина состоит в том, что защитные меры всегда тем или иным образом ограничивают сотрудников и само производство.

Даже если в организации устанавливается самая современная система управления и разграничения доступа, через короткое время выясняется, что она «прозрачна» из-за неправильного распределения ролей и ответственности и плохо отлаженного механизма выделения полномочий всем. В итоге организация несет потери и имеет зря потраченные на систему немалые средства.

3. *Стохастичность производства.* Производство развивается в условиях изменчивой среды, при большой неопределенности. Это естественное свойство среды, которое должно учитываться организацией в ее деятельности. В указанных условиях на производственном уровне принимаются решения о необходимости осуществить то или иное действие, отсрочить его, позаботиться о дополнительных гарантиях или ресурсах либо вообще отказаться от выполнения действий. Ясно, что изменчивость требует постоянной подстройки ОИБ под изменения внутренней и внешней среды развития производства организации. Однако эффективность ОИБ, как правило, выявляется только при нарушении ИБ.

4. *Рост масштабов и сложности задач ОИБ организации* требует их эффективного решения, что не может быть достигнуто без целенаправленного управления процессами ОИБ, основанного на системном подходе.

5. *Своевременность обнаружения проблем в области ОИБ.* Организация должна своевременно обнаруживать проблемы, прямо или косвенно относящиеся к ИБ и потенциально способные повлиять на успех достижения организацией ее производственных целей.

4.2. Обеспечение информационной безопасности как процесс

Обеспечение защищенности интересов организации непосредственно связано с ее основной производственной деятель-

ностью, а ОИБ является вспомогательной по отношению к нему. При этом главное предназначение ОИБ организации – содействие основным, управленческим и иным процессам ведения производства. Модель, представленная на рис. 4.1, иллюстрирует связи основной деятельности организации и ее деятельности по ОИБ как систему процессов [4].

Планируя осуществление ОИБ, организация должна ответить на ряд важных вопросов: что может случиться, каковы последствия реализации угроз ИБ для ее отдельных активов и производства в целом и т. п.

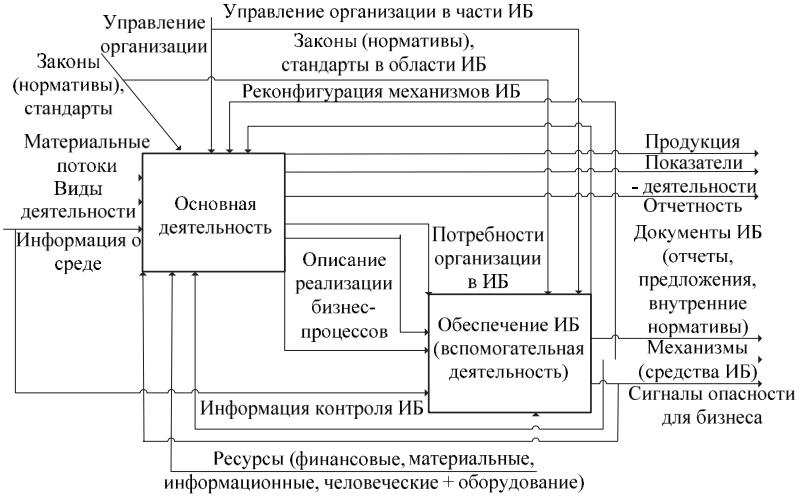

Рис. 4.1. Связи основной деятельности и деятельности по ОИБ

Поэтому входными данными для процесса ОИБ являются:

– информация о среде развития производства организации;

– потребности организации в ИБ;

– описание производственных процессов и их реализации;

– информация, используемая для контроля ОИБ.

Кроме этого, учитываются нормативы и стандарты в области ИБ и управление в этой части, а также ресурсы (финансовые, материально-технические, информационные, кадровые и иные).

Важнейшими исходными данными для эффективного ОИБ служат информационные модели основной деятельности организации, описания производственных процессов, реализуемых технологий и т. п. Модели определяют контекст всей деятельности по ОИБ, так как позволяют понять, где в структуре организации в части ИТ имеются уязвимости, при каких условиях могут проявиться те или иные угрозы ИБ и действия ее нарушителей, каковы активы, требующие защиты, какие защитные меры (организационные, программно-аппаратные, технические) могут потребоваться, и какие из них наиболее эффективны в каждом конкретном случае.

На ОИБ организации влияют:

– регламентирующие ИБ документы для всех ее структурных подразделений;

– обучение персонала и работа с ним по вопросам ИБ;

– приобретение и регламентация использования сервисов и систем ОИБ;

– контроль за ОИБ, в том числе на основе информации об инцидентах, данных мониторинга и аудита ИБ;

– сигналы опасности для интересов деятельности организации, направляемые всем ее подразделениям.

Выходом (результатом) деятельности ОИБ в организации являются:

– документы по ИБ (отчеты, предложения, в том числе – по обучению и переподготовке персонала, внутренние нормативные документы);

– приобретение и регламентация использования механизмов ИБ на объектах и системах организации;

– сигналы опасности для основной деятельности организации.

Механизмы (средства, защитные меры) ОИБ, являющиеся результатом деятельности по ОИБ и выступающие важным ресурсным обеспечением для производственной деятельности организации, применяются службами информатизации и в ряде случаев – основными функциональными подразделениями.

Рассмотренная связь задает контекст, позволяющий в первую очередь позиционировать управленческие, информационные, материальные и ресурсные потоки в рамках взаимоотношений по ОИБ (как вспомогательной деятельности) с основной и другими процессами в рамках организации.

Как показывает опыт ОИБ в организации, ее успешность зависит следующих факторов [13; 21]:

– утвержденная и соблюдаемая ПолИБ, учитывающая цели организации;

– методы, структура реализации, поддерживающие в рабочем состоянии деятельность организации;

– поддержка руководства всех уровней;

– понимание требований ПолИБ, оценки и управления рисками ИБ;

– информирование сотрудников и связанных с организацией сторон по ОИБ, принципах ПолИБ и стандартах в области ИБ;

– финансирование ОИБ;

– надлежащая подготовка в области ИБ сотрудников организации;

– результативное управление инцидентами ИБ;

– внедрение системы измерения и оценки ОИБ, выработка предложений по ее совершенствованию.

К деятельности по ОИБ применим подход, называемый «Колесо безопасности», который наглядно отражает применение ПолИБ (рис. 4.2).

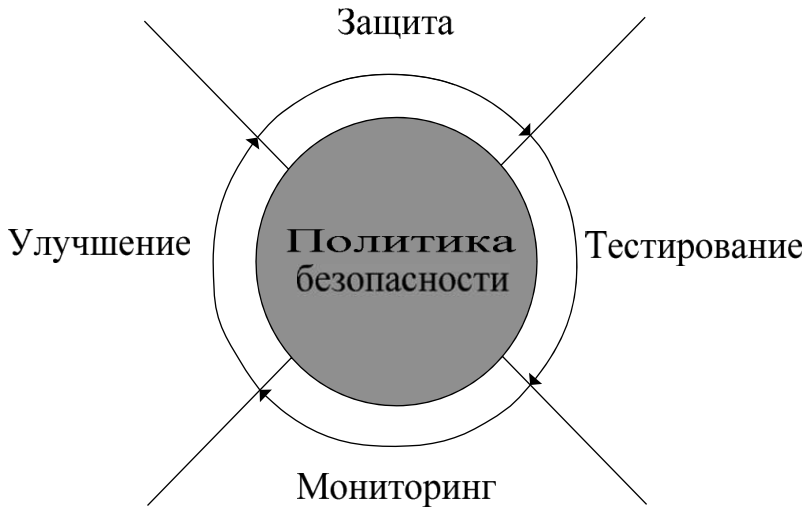

Рис. 4.2. «Колесо безопасности» в реализации ПолИБ

Защита подразумевает применение описанных и одобренных в ПолИБ для организации защитных мер. Мониторинг выявляет нарушения ПолИБ в режиме реального времени и то, насколько корректно на предыдущем этапе выбраны и настроены защитные меры. Тестирование (внутренний и внешний аудит ИБ) используется для определения эффективности используемых защитных мер, которые определяют, насколько текущее состояние дел соответствует правилам и процедурам, реализованным в соответствии с ПолИБ. Улучшение защитных мер и самой ПолИБ осуществляется на основе информации, собранной и проанализированной на этапах мониторинга, и тестирования.

«Колесо безопасности» отражает его сущность – постоянное, циклическое совершенствование и уточнение ПолИБ и эксплуатируемых в соответствии с ней защитных мер. При этом результаты, получаемые на всех этапах, всегда сравниваются с начальной ПолИБ, чтобы убедиться в выполнении всех задач по ОИБ.

Специальный стандарт NIST SP80033 «Underlying Technical Models for Information Technology Security» [95] описывает модель, лежащую в основе защиты ИТ и предназначенную для использования технических средств защиты ИТ. Эта модель предлагает рекомендации по созданию системы защиты ИТ с учетом рисков ИБ и обеспечению конфиденциальности, целостности, доступности и учета (фиксации всех событий ИБ), а также гарантирует соблюдение этих свойств для систем и данных ИТ. В стандарте описана модель защиты для всех перечисленных свойств, предполагающая распределение и взаимосвязь по различным уровням защищаемых ИТ.

4.3. Определение управления информационной безопасностью организации

Управление ИБ – это процесс, представляющий логически взаимосвязанную между собой и непрерывную во времени последовательность работ, направленных на достижение цели ОИБ [14; 21].

При этом сделаем важное замечание, касающееся терминологии. В российских документах при их гармонизации с международными стандартами по ИТ и ИБ в переводе английского слова *«management»* встречаются оба термина – «управление» и «менеджмент».Ппредпочтение отдается первому, т. е. управлению ИБ, как более привычному для российских специалистов.

В настоящее время, к сожалению, нет общепринятого определения управления ИБ. Хотя этот термин весьма распространен, используется многими производителями и продавцами средств защиты, системными интеграторами, специалистами, представителями средств массовой информации (СМИ) и др. Так, первые две категории понимают под этим термином техническую

составляющую процесса управления с единой консоли при решении в сетевой среде различных задач по ОИБ: обнаружение вторжений и вирусов, управление настройками систем защиты и т. д. Журналисты называют системами управления ИБ любое ПО, которое чем-то управляет. Многие пользователи понимают под управлением ИБ только управление программными или аппаратными СЗИ. Все эти взгляды являются слишком узкими и ограниченными в своей интерпретации.

Более правильно рассматривать управление ИБ как систему целенаправленных действий, обеспечивающих нормальное функционирование основных процессов и в конечном счете достижение производственных целей организации посредством обеспечения защищенности ее информационной сферы.

Информационная сфера состоит из информационной инфраструктуры, банков данных и знаний, коммуникационных систем и т. п., субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений [11]. Совокупность целенаправленных действий включает оценку ситуации и состояния объекта управления (например, оценку и управление рисками ИБ), выбор управляющих влияний и их реализацию (планирование, внедрение, реализацию и обслуживание защитных мер и средств) и многое другое.

Обобщая сказанное, можно достаточно пространно определить управление ИБ организации как циклический процесс, состоящий из совокупности действий, осуществляемых для достижения заявленных целей организации посредством обеспечения защищенности ее информационной сферы и включающий необходимость ОИБ, постановку задач по ОИБ, оценку текущей ситуации и состояния объекта управления, планирование мер по обработке рисков ИБ, реализацию, внедрение

и оценку эффективности защитных мероприятий и средств управления, распределение ролей и ответственности в области ОИБ, обучение и мотивацию сотрудников, выбор управляющих и корректирующих воздействий и их реализацию. Очевидно, что определение, приведенное в начале настоящего раздела, более логичное и четкое.

Управление ИБ организации – это не разовое мероприятие. Его следует рассматривать как непрерывную деятельность по постоянному поддержанию требуемого организацией уровня ИБ, так как правильно управляемая ИБ – инструмент успешного развития производственного процесса.

Основными этапами управления ИБ в организации являются:

– планирование работ по ОИБ, включая разработку и развитие соответствующей документации;

– участие в реализации защитных мер;

– осуществление контроля за ОИБ и уровнем ИБ;

– совершенствование работ по ОИБ на основе лучших практик.

В целом процесс управления ИБ организации заключается:

– в описании объектов управления и защищаемых активов организации и сборе данных об их состоянии;

– выявлении, формализации возможных угроз и анализе рисков ИБ;

– оценке защищенности объектов управления (с выявлением уязвимостей) и ее сравнении с требованиями по ОИБ организации, сформулированными в ПолИБ;

– формировании управляющих воздействий;

– оценке итоговой деятельности по управлению ИБ.

Таким образом, управление ИБ в организации включает в себя две важнейшие составляющие – процесс управления ИБ и систему управления ИБ (СУИБ) организации.

Высшее руководство организации должно быть всесторонне проинформировано по вопросам ОИБ, определять направления управления политикой и стратегией в этой области, ресурсно обеспечивать деятельность по ОИБ, устанавливать приоритеты, осуществлять необходимые корректировки, выделять защищаемые активы и подлежащие оценке риски ИБ, страховать остаточные риски, а также учитывать эффективность ОИБ.

Руководство организации должно участвовать в создании ее ПолИБ, учитывать влияние политики на производственный процесс. После утверждения ПолИБ организация должна гарантировать:

– определенность ролей, ответственных за ОИБ;

– наличие моделей угроз и нарушителей ИБ;

– реализацию инфраструктуры ОИБ и средств управления ею, включая стандарты, критерии оценки, практические приемы и процедуры, своевременный учет приоритетов;

– мониторинг возникающих уязвимостей и регулярную отчетность по результатам анализа защищенности;

– обучение сотрудников по вопросам ИБ.

Можно сделать еще большее обобщение и определить управление ИБ как часть общего управления организацией, а не только управление ее ИТ.

Цель управления ИБ в организации заключается в том, что соответствующие мероприятия по ОИБ осуществляются так, что надлежащим образом:

– снижены риски ИБ;

– осуществляются инвестиции в ОИБ;

– руководство ознакомлено со всеми проводимыми мероприятиями и поддерживает их;

– корректно сформулированы критерии оценки эффективности ОИБ.

Основные задачи управления применительно к ИБ [96]:

1. *Целеполагание* (определение требуемого состояния или поведения) ОИБ и соответствующего уровня ИБ организации на основе риск-ориентированного подхода (подразумевает отсутствие недопустимого риска ИБ) и выполнения требований законодательных и нормативных документов по ОИБ.

2. *Стабилизация* (удержание в определенном состоянии в условиях возмущающих воздействий) – выбор и реализация таких управляющих воздействий по ОИБ (планирование, внедрение, реализация и поддержание защитных мер), которые позволят сохранить требуемый уровень ИБ в течение конкретного времени.

3. *Выполнение программы* (перевод в требуемое состояние в условиях, когда значения управляемых величин изменяются по известным законам) – соблюдение планов обработки инцидентов и рисков, проведения аудитов ИБ, корректирующих воздействий в отношении ОИБ в соответствии с результатами контроля.

4. *Слежение* (удержание втребуемом состоянии или поведении) – оценка по установленным критериям уровня ИБ в условиях изменения угроз ИБ, появления новых атак и обнаружения новых уязвимостей, поддержания требуемого уровня ИБ за счет реализации корректирующих воздействий.

5. *Оптимизация* (удержание или перевод в состояние с экстремальными значениями характеристик при заданных условиях и ограничениях) – достижение экономической целесообразности в выборе защитных мер и поддержании всех процессов ОИБ.

Уровни управления ИБ представлены на рис. 4.3 [93]. На самом верхнем уровне принимаются стратегические решения. Ниже располагаются уровни тактического и оперативного управления ИБ.

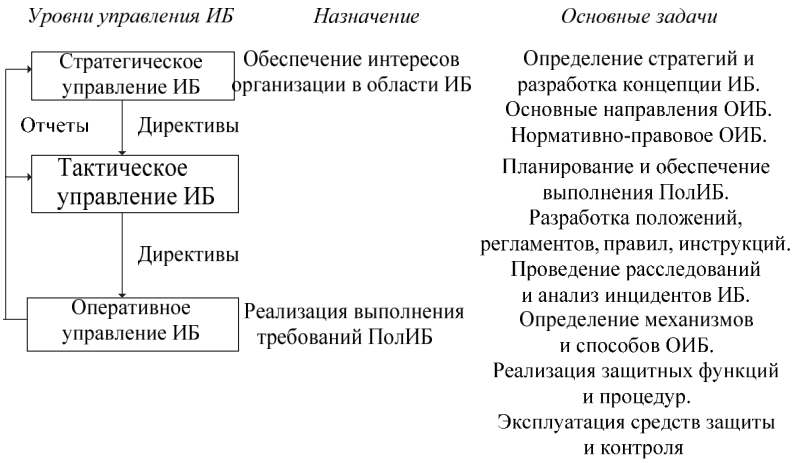

Рис. 4.3. Уровни управления информационной безопасностью организации

При построении системы управления на уровне тактического управления создается Центр управления ИБ. Основными задачами данного уровня являются формирование и контроль ПолИБ. Нижний же уровень реализует выполнение ПолИБ. Создание Центра управления ИБ позволяет облегчить проведение анализа и выработку корректирующих действий.

4.4. Система управления информационной безопасностью организации

Процесс управления ИБ организации реализуется СУИБ. Она определяется как часть общей системы управления организации, основанная на оценке и анализе рисков, предназначенная для разработки, внедрения, эксплуатации, постоянного контроля, анализа, поддержания и улучшения ИБ и включающая организационную структуру, политику, планирование действий, обязанности, установившийся порядок, процедуры, процессы и ресурсы в области ИБ [14; 21].

СУИБ в организации выполняет следующие функции:

– реализует целенаправленный комплексный подход к управлению ИБ защищаемых активов, что приводит к повышению уровня их защищенности;

– объединяет все применяемые в организации защитные и организационные меры в единый, адекватный реальным угрозам ИБ и управляемый комплекс, позволяющий достигать целей ОИБ на уровне всей организации;

– позволяет четко установить, как взаимосвязаны процессы и подсистемы ОИБ, кто за них отвечает, какие финансовые и трудовые ресурсы необходимы для их эффективного функционирования;

– проводит процесс выполнения ПолИБ и позволяет находить и устранять слабые места в ОИБ;

– охватывает людей, процессы и ИТ-структуру организации.

Систематизируя представленные в различных источниках сведения об отдельных элементах СУИБ, следует подчеркнуть, что для выполнения перечисленных выше функций СУИБ конкретной организации должна включать в себя следующие компоненты:

– соответствующую организационную структуру с поддерживающими ее подсистемами СУИБ (документооборот, обработка, хранение и передача данных), организации управления и собственной защиты;

– модель функционирования СУИБ (например, процессно-ролевая);

– методики и методы управления ИБ (общий свод правил, алгоритмов, приемов управления ИБ; путь практического осуществления деятельности по управлению ИБ, достижения определенной цели в рамках ОИБ);

– документальное обеспечение функционирования СУИБ (политика СУИБ, планы СУИБ, процедуры, регламенты);

– деятельность по планированию, реализации, проверке и совершенствованию СУИБ с соответствующими средствами выполнения конкретной деятельности;

– ответственность участвующих в процессе управления ИБ, и тех, кто попадает в область действия СУИБ;

– процессы управления ИБ, выполняемые на основе СУИБ;

– средства управления ИБ;

– необходимые ресурсы.

Средства управления ИБ организации, используемые в рамках СУИБ, выбираются на основе результата оценки рисков ИБ как части более общего процесса управления рисками ИБ и снижают риск до приемлемого уровня, при этом принимая во внимание и другие риски организации. Обязательно должны быть определены, документированы, реализованы и поддерживаемы в рабочем состоянии технические средства управления ИБ. Но со временем действие различных внутренних и внешних обстоятельств (например, изменение ИС, реконфигурирование функций защиты, изменения окружающей среды, появление новых атак) может негативно сказаться на эффективности используемых в организации средств управления ИБ и в конечном счете потребовать пересмотра стандартов ИБ организации. Поэтому так важно адекватно изменять средства управления ИБ, что делается на основе постоянного анализа и технической проверки (вручную или с использованием инструментальных средств) правильности их реализации и функционирования.

Более наглядное представление основных компонентов СУИБ показано на рис. 4.4 [16]. Процессы ОИБ поддерживаются ПолИБ и концепцией ОИБ, в которых сформулированы цели и стратегия ОИБ, а также организация самих процессов. Следовательно, СУИБ является неотъемлемой частью ОИБ.

Область действия СУИБ, ее администрирование и ресурсы зависят от размеров организации и защищаемых активов.

Чтобы быть действительно полезной для организации, СУИБ должна быть эффективной. Правильно разработанная, должным образом реализованная и применяемая СУИБ позволит не только компенсировать затраченные на нее средства, но и внесет положительный вклад в развитие производства организации.

Рис. 4.4. Основные компоненты СУИБ

Как показывает накопленный в данной области опыт, эксплуатация СУИБ даст организации ряд бесспорных выгод от ее использования:

– обеспечение соответствия уровня ИБ законодательным, отраслевым, контрактным, внутрикорпоративным требованиям и целям бизнеса;

– усиление стремления руководства к ОИБ в необходимом объеме в соответствии с установленными требованиями;

– повышение доверия партнеров, клиентов, заказчиков за счет демонстрации высокого уровня ОИБ;

– управляемое ОИБ и ИБ (особенно в критичных ситуациях);

– систематизация процессов ОИБ;

– расстановка приоритетов в области ИБ;

– достижение «прозрачности» в ОИБ;

– систематизация защищаемых активов;

– выявление угроз ИБ для производственных процессов;

– достижение соответствия ОИБ существующим рискам;

– предупреждение инцидентов ИБ и снижение ущерба в случае их возникновения;

– повышение культуры ИБ в организации;

– интеграция защитных мер в производственные процессы;

– оптимизация и обоснование расходов на ИБ;

– снижение финансовых рисков и рисков прямых потерь;

– снижение рисков за счет повышения эффективности ОИБ;

– снижение рисков для инвесторов за счет повышения прозрачности процессов внутри организации;

– экономия времени, ресурсов и затрат на начальной стадии сбора информации при проведении аудитов ИБ.

Внедрение СУИБ должно стать стратегическим решением руководства организации. На ее проектирование и использование оказывают влияние потребности и цели, требования по ОИБ, применяемые процессы, а также размер и структура организации. Все эти элементы и поддерживающие их системы изменяются во времени. Поэтому и СУИБ будет также меняться соответственно потребностям организации.

Область действия СУИБ

Стандарты по управлению ИБ, в частности, ГОСТ Р ИСО/МЭК 27001, оперируют понятием области действия СУИБ. Это область и границы ее применения в терминах характеристик бизнеса, организации, ее расположения, ресурсов и техноло-

гий [14; 21]. Область действия СУИБ должна соответствовать как возможностям организации, так и ее ответственности за ОИБ в соответствии с требованиями, определенными в применимых к данной организации законодательных, нормативных и иных документах.

Установление области действия СУИБ полностью зависит от того, чтобы она была правильно определена и реально примененной, учитывала требования по ОИБ, включая интерфейсы с частями организации, а также другими системами, сторонними организациями.

В область действия СУИБ организации должны быть включены:

– производственные процессы;

– технологии;

– активы (кадры, финансовые средства, средства вычислительной техники и телекоммуникаций, различные виды информации, процессы, продукты и предоставляемые услуги);

– части организации (перечисление конкретных офисов, входящих в область действия) или всей организации в целом.

При выборе области действия, в которой силами специально созданной рабочей группы будут внедряться процессы СУИБ, учитываются следующие факторы:

– продукция и услуги, предоставляемые организацией;

– целевая информация, защита которой должна быть обеспечена;

– процессы, обеспечивающие обработку целевой информации;

– подразделения и сотрудники организации, задействованные в производственных процессах;

– программно-аппаратные и технические средства, обеспечивающие функционирование производственных процессов;

– территориальные площадки организации, в рамках которых происходят сбор, обработка и передача целевой информации.

В стандарте ISO/IEC 27003:2010 приведены примеры возможных целей управления ИБ для определения первоначальной области действия СУИБ [23]:

– содействие восстановлению производства после сбоев;

– повышение устойчивости к инцидентам ИБ;

– соответствие правовым требованиям и договорным обязательствам;

– создание условий для сертификации по стандартам ISO/IEC;

– создание благоприятных условий для развития организации и укрепления ее позиций;

– сокращение расходов на средства управления ИБ;

– защита активов, имеющих стратегическое значение;

– создание жизнеспособной и эффективной системы внутреннего контроля;

– обеспечение гарантий того, что информационные ресурсы защищены надлежащим образом.

Удачной практикой при определении области действия будущей СУИБ является выбор одного из ключевых производственных процессов организации. Это объясняется тем, что в рамках наиболее критичных процессов можно наиболее адекватно ощутить преимущества построения СУИБ, так как основной из целей ее создания является обеспечение соразмерных средств управления ИБ, которые защищают активы. Также появляется возможность постоянного мониторинга ОИБ в рамках выбранной области действия СУИБ, что позволяет своевременно принимать оперативные решения, затрагивающие все аспекты ИБ, и повысить доверие к организации в целом.

Основной результат деятельности по определению области действия СУИБ – это документ, включающий:

– сводку поручений по управлению ИБ, установленных руководством организации;

– описание взаимодействия с другими системами управления;

– список целей управления ИБ;

– список критических производственных процессов, систем, информационных активов, организационных структур, где будет применяться СУИБ;

– взаимоотношения существующих систем управления и регулирующих, надзорных органов;

– характеристики производства, самой организации, ее активов и используемых технологий.

Выбор области действия будущей СУИБ не такая простая задача, как кажется на первый взгляд. В рамках большой организации, предоставляющей услуги своим заказчикам, для выбора области действия может потребоваться ведение отдельного проекта. В его основе должен лежать глубокий анализ существующих производственных процессов организации, их взаимосвязей, выходных результатов каждого из процессов. Даже в небольшой организации, где всего несколько ключевых процессов, в результате может быть получена картина, в которой проявятся неочевидные взаимосвязи между процессами, и фокус оценки их критичности может быть значимо смещен.

В случае, если существует необходимость охватить СУИБ более, чем одно подразделение организации, управление ею и аудит все равно осуществляется централизованным образом, подвергаясь контролю со стороны высшего руководства. Для всех подразделений, где функционирует СУИБ, аудит ИБ проводится в соответствии с внутренними процедурами организации. Осо-

бое внимание следует уделить тому, чтобы соответствующим образом определить риски ИБ, а результаты этой оценки надлежащим образом отразить в системе реализуемых процессов управления ИБ.

Можно поступить иначе и для каждого подразделения построить разные СУИБ, которые будут управляться локально. При достижении зрелости локальных систем возможно их объединение в единую СУИБ, область деятельности которой будет распространяться сразу на несколько распределенных подразделений организации.

Документальное обеспечение СУИБ

Любые процессы управления базируются на их документальном обеспечении. Управление СУИБ не являются исключением. Все российские и международные стандарты для СУИБ требуют, чтобы в процессе ее внедрения был разработан значительный пакет документации. Неправильно организованный процесс ее разработки может привести к серьезному перерасходу ресурсов и снизить эффект от внедрения СУИБ.

В рамках СУИБ используется достаточно большое количество различных документов, которые имеют свой жизненный цикл. Они создаются, согласуются, пересматриваются, исполняются, прекращают свое действие, хранятся определенный срок. По отдельным процессам управления ИБ создаются документы, содержащие записи, свидетельствующие о работе этих процессов (например, протокол аудита ИБ и заполненные формы разрешения доступа). Регистрация таких записей предусматривает идентификацию, сбор, заполнение, ведение и хранение зарегистрированных данных. Все документы, относящиеся к СУИБ, должны находиться под ее управлением, а именно: учитываться, легко идентифицироваться, контролироваться с точки зрения версий и актуальности [5; 14; 21].

Существующие стандарты по управлению ИБ определяют совокупность обязательных требований по управлению документами и записями, которые должны обеспечить их адекватную защищенность и управляемость с использованием соответствующих процедур и процессов [14; 21]. Эти требования согласованы с процедурами, содержащимися в других стандартах по системам управления, например в ГОСТ Р ИСО 9000–2001 [5]. Соблюдение указанных процедур дает организации ряд преимуществ, включая возможность проведения совместных комплексных аудитов. Позволяет сэкономить средства, необходимые для управления и сопровождения документации СУИБ, помогает лучше контролировать активы и в результате – обеспечить комплексное управление ИБ. Управление документами и записями составляет важную часть процесса управления рисками ИБ, который должен реализовываться параллельно с другими подобными процессами.

Наличие документации СУИБ для организации очевидно – детальное описание СУИБ и представление информации о ней всем заинтересованным и компетентным лицам для лучшего понимания деятельности по управлению ИБ и своего места в этой деятельности.

В документацию СУИБ обычно включаются:

– политика СУИБ;

– руководства по процессам управления ИБ;

– документированные процедуры;

– рабочие инструкции;

– формы и шаблоны;

– планы работ;

– спецификации;

– внешние документы (международные и российские стандарты);

– отчетные документы.

Чтобы определить иерархию документации СУИБ, следует воспользоваться примером, описанным в рекомендациях РС БР ИББС-2.0-2007 «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], где определяется состав внутренних документов по ОИБ.

По аналогии иерархия документов СУИБ может быть составлена следующим образом (рис. 4.5).

Документы СУИБ *первого уровня* включают политику СУИБ и детализирующие ее подполитики (например, обработки рисков ИБ, инцидентов ИБ).

Второй уровень представлен документами СУИБ – планами работ по управлению ИБ. В их состав входят планы:

– мероприятий по обеспечению деятельности в рамках управления ИБ, реализации и внедрению процедур, требований и мер по ОИБ, управлению документами, связанными с СУИБ;

– обработки рисков ИБ; мероприятий на случаи инцидентов ИБ; работ по обслуживанию аппаратных средств и программных систем, используемых для ОИБ; обучению и повышению осведомленности работников организации. В них описываются перечень, последовательность, объем, сроки выполнения работ, а также руководители, исполнители и ответственные за выполнение работ.

Описания (стандарты) технологий ОИБ устанавливают требования и характеристики, касающиеся деятельности по ОИБ, осуществляемой в рамках и на основе СУИБ. Они могут разрабатываться в отношении как специализированных технологий ОИБ, так и технологий, реализуемых ИС, применяемых в процессах производства организации.

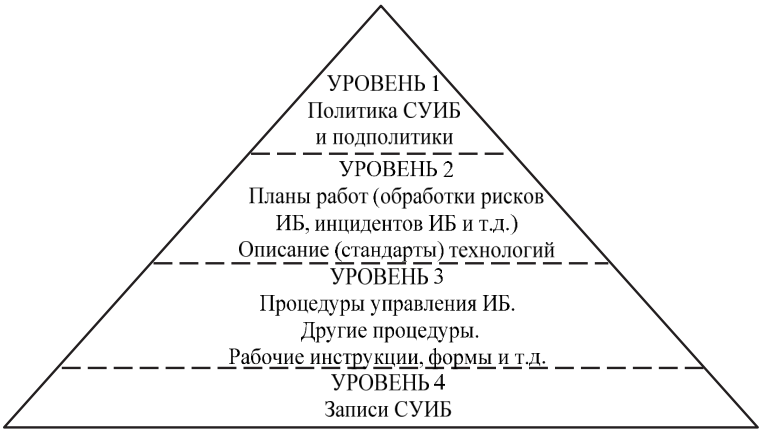

Рис. 4.5. Пример иерархии документов СУИБ

Третий уровень – наиболее объемная часть документации, описывающей конкретные действия участников процесса управления ИБ. Этот уровень составляют документы СУИБ, содержащие требования к процедурам управления ИБ, выполняемым как структурными подразделениями организации, так и ее сотрудниками в рамках технологических процессов, реализующих технологии, требования по ОИБ, определенных в ПолИБ организации.

В этих документах даются детализированные описания, приводятся конкретные приемы и порядки выполняемых действий, вводимых ограничений, что позволяет четко определить правила решения задач управления ИБ на каждом рабочем месте, для каждой роли ИБ, а также установить конкретную ответственность за выполнение предписанных требований. В разработке документов принимают участие специалисты по ИБ, отдела кадров, управления ИТ, службы физической защиты, юридического отдела и других подразделений.

Основными пользователями данной группы документов являются руководители подразделений, системные администраторы, ответственные за ОИБ конкретных активов.

Документы СУИБ третьего уровня должны быть утверждены ответственными за управление ИБ. К этой группе документов относятся:

– инструкции, в том числе должностные;

– руководства по классификации защищаемых активов;

– методические указания;

– документы, содержащие требования к конфигурациям программно-аппаратных СЗИ с указанием конкретных значений параметров систем и их компонентов, а также способы их настройки, позволяющие обеспечить требуемый уровень ИБ.

Инструкции, руководства, методические указания, к которым предъявляются повышенные требования к ясности изложения, содержат правила, устанавливающие порядок и способ выполнения отдельных операций по управлению ИБ. Эти документы обычно определяют:

– субъектов этой деятельности;

– ресурсы, необходимые для выполнения деятельности;

– детальное описание операций, включая ограничения и результаты их выполнения;

– обязанности субъектов в рамках выполнения регла ментируемой деятельности;

– права и ответственность субъектов.

Четвертый уровень составляют документы СУИБ, содержащие записи о результатах деятельности по управлению ИБ, регламентированной документами верхних уровней иерархии управления. Все эти документы СУИБ могут служить доказательством реализации деятельности по управлению ИБ при проведении внутреннего контроля и аудитов ИБ организации.

К данной группе документов относятся: реестры и описи (например, опись активов), регистрационные журналы (включая журналы регистрации инцидентов ИБ), протоколы (например,

протокол проведения испытаний), листы ознакомления, обязательства (например, обязательства о неразглашении), акты, договоры, отчеты. Наличие документов СУИБ этого уровня определяется требованиями, зафиксированными в документах СУИБ верхних уровней иерархии. Должно обеспечиваться их архивное хранение, время которого определяется требованиями как законодательных актов, так и нормативными документами самой организации.

В состав документов по управлению ИБ организации рекомендуется включить классификатор, содержащий перечень и назначение всех документов СУИБ для каждого из уровней иерархической структуры [75].

При наличии у организации филиалов в каждом из них рекомендуется иметь утвержденный комплект документов по управлению ИБ. При необходимости учета специфики конкретных филиалов в них должны быть разработаны собственные документы, ее учитывающие, но базирующиеся на положениях документов СУИБ, принятых головной организацией, и не противоречащих им.

Все документы СУИБ обязательно защищаются, и ими нужно управлять. СУИБ как документированная система управления должна удовлетворять следующим требованиям [14; 21]:

– документы проверяются на адекватность до их утверждения и выпуска;

– осуществляется обновление документов по мере необходимости с их последующим повторным утверждением;

– обеспечивается идентификация изменений и статуса текущей редакции документов, а также доступность актуальных версий;

– обеспечивается доступность документов тем, кому они требуются, а также их перемещение, хранение и, наконец, уничтожение согласно установленным процедурам;

– обеспечивается идентификация документов внешнего происхождения;

– обеспечивается контроль и управление над распространением документов;

– предпринимаются меры по предотвращению случайного использования устаревших документов.

Также должны создаваться и поддерживаться в рабочем состоянии записи, содержащие свидетельства соответствия требованиям эффективного функционирования СУИБ [14; 21]. В записях отражаются показатели процессов управления ИБ и все эпизоды значительных инцидентов ИБ, связанные с СУИБ. Эти записи должны быть защищены и легко идентифицируемы.

Как было отмечено, записи играют важную роль в управлении ИБ. Например, при обработке инцидента ИБ важно, чтобы он был рассмотрен с той степенью оперативности и с тем уровнем приоритета, которые соответствуют его серьезности. Чтобы обработать инцидент ИБ оптимальным образом, требуются детальные данные о том, где и когда он произошел, при каких обстоятельствах, какие возникли последствия и т. д. Такие данные могут быть очень часто получены из системно ведущихся, точных записей. И, конечно, существуют правовые требования по сбору и представлению доказательств в случае инцидента ИБ с уголовно-правовыми последствиями. Поэтому важно не только вести записи, но и обеспечивать их защиту, включая целостность, доступность и конфиденциальность.

Управление документацией СУИБ направлено на обеспечение разработки, учета, использования, хранения, проверки, обновления (поддержания актуального состояния) и изменения документов и записей. Все документальное обеспечение СУИБ проходит несколько стадий жизненного цикла: начальную оценку необходимости разработки документа, исходя из наме-

ченных целей, собственно его разработку специально определенной группой лиц с соответствующими полномочиями и предоставленными для этого ресурсами, утверждение уполномоченным лицом и установление дат его введения и пересмотра, публикацию (доведение до сведения всех заинтересованных лиц), использование документа и непосредственное исполнение его положений, сопровождение с последующим внесением изменений или изъятием из обращения после процедуры пересмотра. Если принято решение о внесении изменений и выпуске следующей редакции, то новый цикл опять начинается со стадии разработки.

Организация может согласовывать документацию СУИБ с документацией других систем управления (системы менеджмента качества, охраны труда, экологического менеджмента) [32; 33].

Политика СУИБ

Залогом эффективного функционирования СУИБ является ее хорошо продуманная политика. Это тот документ, на основе которого формулируются директивы, стандарты, процедуры, руководства и другая документация в области ОИБ. Поэтому, определив область действия, организация должна установить понятную политику СУИБ. Имея и применяя такую политику, организация берет под системный контроль направления своего развития и его результаты.

Политика СУИБ рассматривается как расширенное множество ПолИБ организации [21], хотя обе политики могут быть описаны в одном документе. Небольшим организациям может быть достаточно одной политики; организациям большего размера могут понадобиться различные ее подмножества. Если это необходимо, то подмножества должны определяться на стадии начала основной политики СУИБ.

Политика СУИБ – документ о целях организации, задачах и средствах достижения целей в определенной области ее действия. Его цель – обеспечение управления и поддержки ИБ со стороны руководства организации, поскольку для эффективного управления рисками ИБ требуется привлечение значительных ресурсов. предназначен для создания программы ОИБ, установления целей и задач функционирования СУИБ и распределения ответственности в рамках действия политики.

Таким образом, политика СУИБ должна [23]:

– соответствовать области ее действия;

– включать в себя основные положения для определения целей;

– устанавливать цели функционирования СУИБ, основанные на требованиях и приоритетах в отношении ИБ организации;

– определять общие направления и принципы деятельности по отношению к ИБ, которые должны быть достигнуты при использовании СУИБ;

– учитывать производственные требования, а также требования нормативно-правовой базы и договорных обязательств;

– опираться риск-ориентированный подход, принятый в организации, вводить критерии оценки рисков ИБ и определять алгоритмы оценки рисков ИБ (например, в соответствии с ГОСТ Р ИСО/МЭК 27005–2010 [31] и ISO/IEC 27005:2008 [26]);

– устанавливать ответственность высшего руководства организации, связанную с СУИБ;

– управлять взаимосвязями с партнерами, которые имеют влияние на ИБ защищаемых активов;

– устанавливать контекст управления стратегическими рисками организации, в котором будут осуществляться разработка и сопровождение СУИБ.

При этом все сотрудники организации и заинтересованные стороны, входящие в заявленную область действия СУИБ, должны быть ознакомлены с данной политикой, и понимать, исполняя ее, какое влияние она оказывает на их работу.

Рекомендуется иметь политику СУИБ в кратком изложении, концентрирующуюся на стратегических аспектах. В ней не должно быть особо детального описания шагов, необходимых для ее внедрения и исполнения.

Чтобы удовлетворить всем требованиям, хорошая политика СУИБ, как и ПолИБ, должна соответствовать целям организации, быть осуществимой для внедрения, легкой в понимании, избегать абсолютных понятий. Важно, чтобы она воспринималась как программный документ.

Политика СУИБ должна охватывать следующие ключевые процессы:

– управление рисками ИБ;

– управление инцидентами ИБ;

– управление аудитами ИБ;

– управление эффективностью СУИБ;

– управление персоналом;

– управление документацией и записями СУИБ;

– анализ функционирования СУИБ руководством организации;

– пересмотр и совершенствование СУИБ;

– управление корректирующими действия ми в области ОИБ.

Политику СУИБ, как и ПолИБ, необходимо периодически пересматривать на предмет актуализации ее целей и основных положений.

Поддержка СУИБ со стороны руководства организации

Руководство организации играет весьма важную роль на всех этапах жизненного цикла СУИБ, начиная от разработ-

ки и заканчивая ее постоянным совершенствованием. В связи с этим стандарты ISO/IEC 27001 и ГОСТ Р ИСО/МЭК 27001 вводят ряд требований [14; 21]. Руководство должно продемонстрировать свою поддержку разработки, ее внедрения, обеспечения функционирования, мониторинга, анализа и улучшения СУИБ посредством:

– разработки и утверждения политики СУИБ;

– обеспечения разработки целей и планов СУИБ;

– определения функций и ответственности в области ИБ;

– информирования сотрудников организации о важности достижения целей ОИБ и ее соответствия требованиям политики организации, об их ответственности за непрерывное совершенствование защитных мер;

– предоставления необходимых ресурсов для внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СУИБ;

– установления критериев принятия рисков ИБ и уровней их приемлемости;

– обеспечения проведения внутренних аудитов и анализа СУИБ.

Прямо выраженная реальная поддержка со стороны руководства организации требуется при определении и предоставлении ресурсов, которые необходимы:

– для разработки, внедрения, обеспечения функционирования, мониторинга, анализа и улучшения СУИБ;

– поддержки требований производства процедурами ОИБ и рассмотрения вопросов ОИБ для всех процессов и проектов, где используется информация и ИТ;

– выявления и обеспечения выполнения требований законов, нормативных актов, а также договорных обязательств в области ОИБ;

– поддержания адекватной ИБ путем применения всех мер управления ею;

– повышения результативности СУИБ.

Также при поддержке руководства организация должна обеспечить необходимую квалификацию персонала, на который возложены обязанности выполнения задач в рамках СУИБ за счет:

– определения требуемого уровня знаний и навыков для выполнения работы в СУИБ;

– обучения персонала или наема компетентного персонала для удовлетворения возникающих потребностей с обеспечением работы СУИБ.

В рамках жизненного цикла СУИБ требуется постоянное внимание высшего руководства к принятию дополнительных управленческих решений.

Так, введение СУИБ в действие должно быть утверждено руководством организации соответствующим приказом по организации. После регулярного анализа результатов работы СУИБ руководство должно принимать необходимые решения по улучшению процессов управления ИБ. На рассмотрение руководства организации выносятся вопросы функционирования СУИБ, статистика по процессам управления ИБ, запросы заинтересованных сторон на внесение изменений в СУИБ и т. д.

Все решения, принимаемые руководством, согласованы с общей стратегией организации. Это очень важно, в самом определении СУИБ подчеркивается, что она является частью общей системы управления организации, и все решения, принимаемые в рамках СУИБ, должны учитывать цели и задачи производственного процесса организации.

4.5. Процессный подход в рамках управления информационной безопасностью

Организация должна качественно управлять различными видами осуществляемой деятельности, чтобы функционировать эффективно. Как отмечено ранее, любое действие, использующее ресурсы и управляемое с целью преобразования входных данных в выходные, может рассматриваться как процесс. Говоря упрощенно, реализация системы процессов в организации, осуществление взаимодействия этих процессов, а также управление ими может быть названо процессным подходом. Все это справедливо и в отношении обеспечения и управления ИБ, так как любые действия в рамках данных видов деятельности могут рассматриваться как процессы. К управлению ИБ применим процессный подход, который распространяется на разработку, реализацию, эксплуатацию, мониторинг, анализ, сопровождение и совершенствование СУИБ организации. Поддержание на должном уровне СУИБ требует применения такого же подхода, как и любая другая система управления. Используемая в ISO/IEC 27001 и ГОСТ Р ИСО/МЭК 27001 для описания процессов СУИБ циклическая модель PDCA предусматривает непрерывный цикл мероприятий: «планирование – реализация – проверка – совершенствование» [11; 21]. При таком подходе к управлению ИБ особое значение придается:

– пониманию требований ОИБ организации и необходимости определения политики и цели ОИБ;

– внедрению и использованию обоснованных защитных мер для управления рисками ИБ организации в контексте общих производственных рисков организации;

– мониторингу и анализу результативности и эффективности СУИБ;

– постоянному совершенствованию, основанному на объективных показателях.

Интерес к циклической модели связан, прежде всего, с проблемами внедрения и совершенствования современных систем управления, в частности СУИБ. Одна из основных целей внедрения СУИБ – создание таких условий в организации, когда происходят постоянный мониторинг и улучшение каждого из процессов ОИБ и смежных с ним процессов. Взаимно усиливая друг друга, они позволяют создать все более совершенную систему.

Частным критерием улучшения каждого из процессов может служить снижение числа несоответствий, выявляемых в ходе различных проверок, таких как внутренние аудиты ИБ, мониторинг эффективности процессов и т. д. Появление несоответствий можно рассматривать как возникновение некоторой проблемы, решение которой ведет к улучшению процесса, а следовательно, к достижению запланированных результатов и удовлетворению интересов заинтересованных сторон.

Каждый факт выявления несоответствия должен приводить к выполнению последовательности действий:

– анализ несоответствия;

– коррекция (устранение несоответствия);

– установление коренной причины его появления;

– определение корректирующих действий, направленных на устранение причины несоответствия;

– анализ эффективности корректирующих действий.

Процессный подход к СУИБ показан на рис. 4.6 [11; 14; 21]. СУИБ в качестве входных данных принимает требования по ОИБ и ожидания заинтересованных сторон, в результате осуществления необходимых процессов на выходе возникает управляемая ИБ, которая удовлетворяет этим требованиям и ожиданиям.

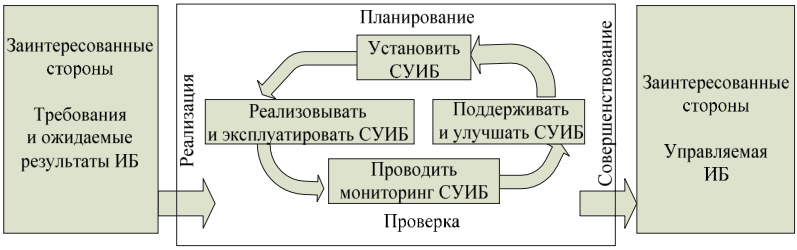

Рис. 4.6. Цикл PDCA в применении к процессам СУИБ

На стадии планирования обеспечивается правильное задание контекста и масштаба СУИБ, оцениваются риски ИБ, предлагается соответствующий план их обработки, а на стадии реализации внедряются спланированные решения.

Чтобы гарантировать, что СУИБ в целом достигает своих целей, необходимы периодические проверки. На стадиях проверки и совершенствования усиливают, исправляют и улучшают решения по СУИБ, которые были реализованы. В зависимости от конкретной ситуации проверки СУИБ могут проводиться в любое время и с любой периодичностью.

В некоторых системах с целью немедленного реагирования они должны быть автоматизированы. В других системах реагирование происходит только в случае инцидентов ИБ либо, когда произошли изменения угроз ИБ и уязвимостей.

Детально содержание деятельности в рамках названных стадий показано на рис. 4.7.

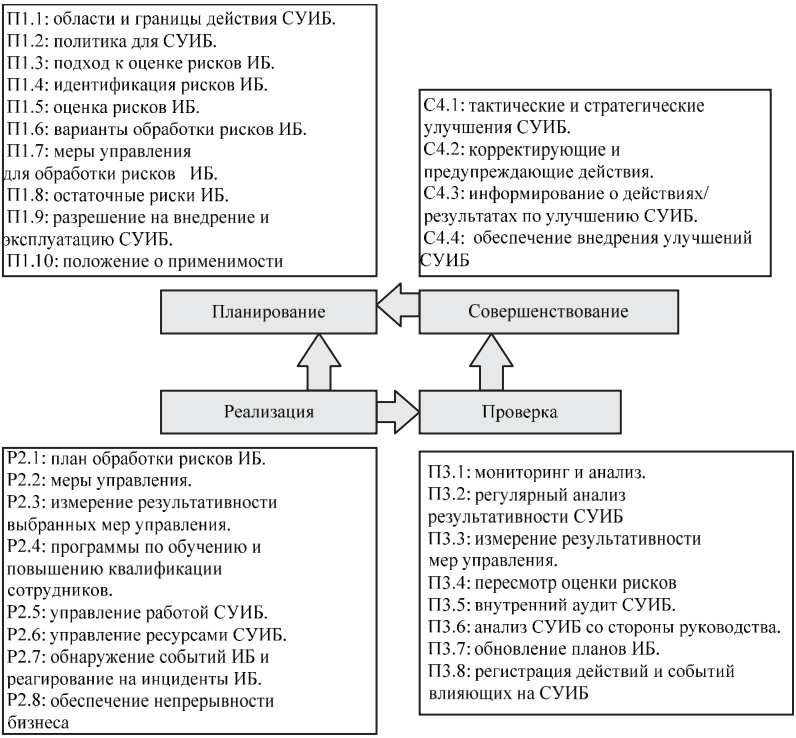

Рис. 4.7. Процессы цикла PDCA в применении к процессам СУИБ

Планирование СУИБ

Применительно к СУИБ на этапе планирования осуществляется ее непосредственная разработка: устанавливается область действия и политика для СУИБ, определяются цели, задачи, процессы и процедуры, адекватные потребностям бизнеса в управлении рисками ИБ и позволяющие повысить уровень ИБ, а также получить результаты, соответствующие общим политикам и целям организации.

Целью деятельности в рамках группы процессов «планирование» является запуск цикла СУИБ путем определения первоначальных планов ее построения, ввода в действие и контроля, а также определения планов по улучшению на основании ре-

шений, принятых на этапе «Совершенствование» (если это уже не первый цикл).

Сочетая при создании СУИБ различные принципы управления в каждом отдельном контуре защиты, можно добиться оптимального соотношения эффективности и стоимости ОИБ. Разработка СУИБ основывается на трех принципах управления [97]:

1. *Разомкнутое управление*. Заранее сформированные требования реализуются исполнителями ОИБ, воздействуя на объект защиты. Достоинство – простота; недостаток – низкая эффективность защиты, так как трудно заранее предугадать момент воздействия и вид угрозы ИБ.

2. *Компенсация*. В контур управления ИБ оперативно вводится информация об обнаруженной угрозе ИБ, в результате чего исполнители ОИБ концентрируют свои усилия на противодействии ей. Достоинство – более высокая эффективность; недостатки – трудность правильного обнаружения угрозы ИБ и невозможность устранения последствий внутренних угроз.

3. *Обратная связь.* Обнаруживается не сама угроза ИБ, а реакция системы на нее и степень нанесенного ущерба. Достоинства – конкретность и точность отработки последствий внешних и внутренних угроз ИБ (экономическая целесообразность); недостаток – запаздывание (инерционность) принимаемых защитных мер.

Выполнение деятельности на стадии планирования заключается в обследовании организации с целью определения степени соответствия требованиям по ОИБ и к СУИБ, корректировке области действия СУИБ, разработке плана мероприятий по построению СУИБ с учетом выбранной области деятельности и степени соответствия требованиям к СУИБ в границах области, формализации подхода к оценке рисков ИБ и распределении ресурсов, проведении оценки рисков ИБ и определении/коррекции планов

их обработки, разработке механизмов и процессов управления ИБ [14; 21].

Основными источниками информации при проведении обследования организации являются документы организации (политики, процедуры, инструкции и т. д.) и результаты интервьюирования ее сотрудников.

После обследования организация должна выполнить следующие шаги (рис. 4.8) [14; 21; 93]:

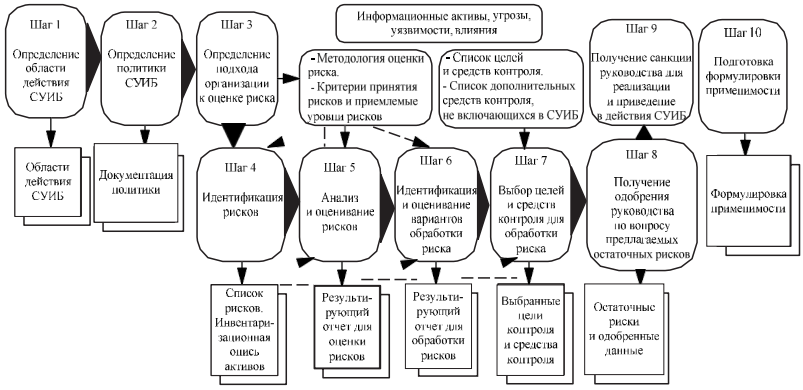

Рис. 4.8. Шаги планирования СУИБ

1. Наметить/уточнить область и границы действия СУИБ с учетом характеристик производства, организации, ее активов и технологий, обоснования исключений из области действия; при этом важно учесть все риски для организации (операционные, репутационные и т. п.).

2. Определить/уточнить политику СУИБ на основе характеристик организации, ее активов и технологий, которая:

– включает установку целей, основных направлений и принципов действия в отношении ИБ;

– учитывает производственные и нормативно-правовые требования (включая национальные и международные стандарты в области ОИБ), а также договорные обязательства по ОИБ;

– согласуется со стратегическим управлением рисками организации, в рамках которого происходят разработка и под держка СУИБ;

– устанавливает критерии оценки рисков;

– утверждается руководством.

3. Установить/уточнить подход к оценке рисков ИБ для наиболее критичных активов и производственных процессов организации, включая:

– методологию оценки рисков ИБ, которая применима для СУИБ и соответствует установленным требованиям по ОИБ и нормативно-правовым документам; она должна давать сравнимые и воспроизводимые результаты;

– критерии принятия рисков и их приемлемые уровни.

4. Выявить и идентифицировать риски ИБ, определив:

– защищаемые активы в области действия СУИБ, а также владельцев этих активов;

– угрозы ИБ для активов;

– уязвимости активов, которые могут быть реализованы через угрозы ИБ;

– негативные последствия, ведущие к потере конфиденциальности, целостности и доступности информационных активов.

5. Проанализировать риски ИБ, для чего необходимо оценить:

– ущерб для деятельности организации в результате сбоя в ОИБ;

– вероятность сбоя в ОИБ с учетом превалирующих угроз, уязвимостей и их последствий, связанных с активами, а также применяемыми мерами управления ИБ;

– уровни рисков;

– приемлемость рисков.

6. Определить и оценить различные варианты обработки рисков ИБ, среди которых:

– применение подходящих мер управления;

– объективное принятие рисков при условии, что они соответствуют требованиям политики и критериям организации;

– избежание рисков;

– передача рисков сторонним организациям, например, страховщикам или поставщикам.

7. Выбрать цели и меры управления рисками ИБ с учетом критериев принятия рисков и нормативно-правовых требований и договорных обязательств.

8. Получить утверждение руководством остаточных рисков ИБ.

9. Получить разрешение руководства на внедрение и эксплуатацию СУИБ.

10. Подготовить Положение о применимости, которое включает:

– цели, меры управления и обоснование соответствующего выбора;

– цели и меры управления, реализуемые в текущий момент времени;

– перечень исключений целей и мер управления, обоснования их исключения.

Фактически представленные шаги этапа планирования СУИБ преследуют цель принятия решения организацией по трем основным вопросам:

– установление области действия и политики СУИБ (шаги 1 и 2);

– выбор защитных мер на основе управления рисками ИБ (шаги 3–7);

– получение одобрения руководства по мерам обработки рисков ИБ и формулирование применимости требований, так как это влечет организационные и возможные финансовые издержки организации (шаги 8–10).

Перечисленные действия являются весьма трудоемкими. Для их осуществления необходимо создание рабочей группы специалистов из разных подразделений организации, обладающих достаточными знаниями и полномочиями для принятия корректных управленческих решений на всех этапах построения и последующего внедрения СУИБ.

Выходом этапа планирования являются разработанные процессы управления ИБ, процедуры, поддерживающие и обеспечивающие реализацию этих процессов, а также инструкции для пользователей и исполнителей ролей в рамках процессов.

Реализация СУИБ

На данном этапе происходят внедрение системы и разработанных процессов управления ИБ, их последующая эксплуатация, а именно внедрение и применение политики, защитных мер, процессов и процедур в отношении СУИБ. Это трудоемкий процесс, требующий назначения исполнителей ролей участников разработанных процессов и проведения обучения исполнителей работ, оперативной корректировки процессов [14; 21].

Этап «Реализация» осуществляется по результатам выполнения этапов «Планирование» и/или «Совершенствование» и заключается в выполнении планов, связанных с построением, вводом в действие и совершенствованием СУИБ. Важным на этом этапе является выполнение таких видов деятельности, как организация обучения и повышение компетентности персонала в области ИБ, реализация обнаружения и реагирования на инциденты ИБ.

Организация должна выбирать защитные меры, адекватные моделям угроз и нарушителей ИБ, с учетом затрат на реализацию таких мер и объема возможного ущерба от реализации угроз ИБ. При этом должны применяться только те защитные меры, корректность применения которых может быть проверена. Для этого

организация должна регулярно оценивать адекватность защитных мер и эффективность их реализации с учетом влияния защитных мер на производственные цели.

Для реализации СУИБ организация должна [14; 21]:

– разработать и реализовать план обработки рисков ИБ, определяющий действия руководства, ресурсы, обязанности и приоритеты в отношении управления рисками ИБ;

– внедрить необходимые меры для достижения целей управления;

– определить способы измерения результативности выбранных мер и использования этих измерений для оценки эффективности управления с целью получения сравнимых и воспроизводимых данных;

– реализовать программы по обучению и повышению квалификации персонала;

– целенаправленно и целесообразно управлять работой и ресурсам СУИБ;

– внедрить процедуры, обеспечивающие оперативное обнаружение событий ИБ и реагирование на инциденты ИБ;

– обеспечить непрерывность производственных процессов организации.

Подробно поэтапные действия по внедрению СУИБ, составленные в соответствии с требованиями ГОСТ Р ИСО/МЭК 27001, ISO/IEC 27001, выглядят следующим образом [14; 16; 17; 21; 23]:

Этап 1 – *управленческий*:

– рассмотреть цели и выгоды внедрения СУИБ;

– получить поддержку руководства на внедрение и ввод в эксплуатацию СУИБ;

– распределить ответственность по внедрению СУИБ.

Этап 2 – *организационный*:

– создать и обучить группу по внедрению и поддержке СУИБ;

– определить область действия СУИБ.

Этап 3 – *анализ существующей СУИБ*:

– провести анализ СУИБ;

– определить перечень работ по доработке СУИБ.

Этап 4 – *определение политики и целей СУИБ* по каждому процессу.

Этап 5 – *сравнение текущей ситуации со стандартом 27001*:

– обучить ответственных за СУИБ требованиям стандарта;

– сравнить требования стандарта с существующим положением дел.

Этап 6 – *планирование внедрения СУИБ*:

– определить перечень мероприятий для достижения требований стандарта;

– разработать руководства по ИБ.

Этап 7 – *внедрение системы управления рисками ИБ*:

– разработать процедуру идентификации рисков ИБ;

– идентифицировать и ранжировать активы;

– оценить активы;

– определить ответственных за активы;

– идентифицировать угрозы ИБ и уязвимости активов;

– рассчитать и ранжировать риски ИБ;

– разработать план по снижению рисков ИБ;

– определить неприменимые средства управления ИБ (приложение А стандарта 27001);

– разработать положение о средствах управления ИБ.

Этап 8 – *разработка документации СУИБ*:

– определить для разработки перечень документов (процедуры, записи, инструкции);

– разработать следующие процедуры и документы:

а) управленческие процедуры (стандарт на разработку документов, мероприятия по управлению документами и записями; корректирующие мероприятия; проведение внутреннего аудита ИБ; мероприятия по управлению персоналом и т. д.);

б) технические процедуры (приобретение, развитие и поддержка ИС; управление доступом; регистрация и анализ инцидентов ИБ; резервное копирование; управление съемными носителями и т. д.);

в) отчетность (отчеты о внутренних аудитах ИБ; анализ СУИБ со стороны руководства организации; анализ рисков ИБ; отчет о состоянии корректирующих действий; договоры; личные дела сотрудников и т. д.);

г) технические записи (план организации, реестр активов, план физического размещения активов, план компьютерной сети, журнал регистрации резервного копирования, журнал регистрации технического контроля после изменений в ОС, журнал событий ИС, журнал регистрации действий системного администратора; журнал регистрации инцидентов ИБ, журнал регистрации тестов по непрерывности производственных процессов и т. д.);

д) инструкции, положения (правила работы с ИС, правила обращения с паролями, инструкция по восстановлению данных из резервных копий, политика удаленного доступа, правила работы с переносным оборудованием и т. д.).

Этап 9 – *обучение персонала* (руководители, сотрудники) требованиям ИБ.

Этап 10 – *разработка и принятие мер по обеспечению работы СУИБ*: внедрение средств защиты (административные, программно-аппаратные, технические).

Этап 11 – *внутренний аудит СУИБ*: подбор команды, планирование и проведение.

Этап 12 – *анализ работы СУИБ со стороны руководства*.

Этап 13 – *официальный запуск СУИБ*: приказ о введении в действие СУИБ.

Этап 14 – *информирование заинтересованных сторон о запуске СУИБ*: пользователей, клиентов, партнеров.

Важным фактором успешного внедрения СУИБ является создание рабочей группы, ответственной за внедрение системы. В ее состав должны войти представители:

– руководства организации;

– подразделений, охватываемых СУИБ;

– подразделений, обеспечивающих ИБ, имеющие соответствующую подготовку, знающие лучшие практики в области ИБ.

Перечисленные сотрудники должны понимать меры защиты и процессы СУИБ, знать требования нормативной и правовой базы, поддерживаемой в организации, и пройти обучение по вопросам создания и эксплуатации СУИБ. В состав рабочей группы также могут входить привлеченные консультанты, специализирующиеся в вопросах СУИБ.

Процедуры реализации и управления СУИБ могут быть организованы как система процессов (в терминах процессного подхода). Отдельные шаги реализации СУИБ могут быть представлены как целевые процессы деятельности, инициируемые и завершаемые по принятым критериям (по времени или событию) и имеющие организационную и ресурсную поддержку [93].

Проверка СУИБ

Реализация СУИБ на практике неотделима от соответствующих процедур контроля, сформулированных в отдельном блоке требований СУИБ. На этапе проверки производятся мониторинг и анализ системы, включающие оценку и измерение эффективности процессов для проверки соответствия требованиям по-

литики, целям ОИБ и практическому опыту функционирования СУИБ, а также информирования руководства организации.

Целью деятельности в рамках процессов проверки является обеспечение достаточной уверенности в том, что СУИБ функционирует надлежащим образом и адекватна существующим угрозам ИБ, а также условиям функционирования организации, влияющим на ИБ. Организация должна своевременно обнаруживать проблемы, относящиеся к ИБ, потенциально способные повлиять на ее цели. Рекомендуется точно выявлять причинно-следственную связь возможных проблем и строить на этой основе прогноз их развития. На этапе проверки необходимо осуществлять мониторинг и контроль используемых защитных мер, проводить аудит ИБ (внутренний и внешний), анализировать функционирование СУИБ в целом [11; 14; 21]. Необходимо интегрировать процессы мониторинга и анализа СУИБ в систему внутреннего контроля организации.

Результаты проверки являются основой для совершенствования СУИБ. Поэтому в процессе проверки СУИБ организация должна [14; 21] выполнять процедуры мониторинга и анализа, а также использовать другие средства управления, чтобы:

– способствовать своевременному выявлению событий ИБ (ошибки в обработке информации, попытки нарушения ИБ) и таким образом предотвращать инциденты ИБ;

– представлять руководству информацию для принятия решений о ходе ОИБ;

– определять, являются ли эффективными действия, предпринимаемые СУИБ для устранения нарушений ИБ;

– проводить регулярный анализ результативности СУИБ (включая проверку ее соответствия политике и целям СУИБ) с учетом результатов аудиторских проверок и инцидентов ИБ, результатов измерений эффективности СУИБ, а также другой информации от всех заинтересованных сторон;

– измерять результативность средств управления для проверки соответствия требованиям по ОИБ;

– переоценивать риски ИБ через определенные периоды времени, анализировать остаточные риски и установленные приемлемые уровни рисков, учитывая изменения в целях деятельности, технологиях и процессах, выявленных угрозах ИБ, результативности мер управления ИБ, внешних условиях, например, в нормативно-правовых требованиях, договорных обязательств;

– проводить внутренние аудиты СУИБ через установленные периоды времени;

– осуществлять анализ СУИБ руководством организации в целях подтверждения адекватности ее функционирования в рамках установленной области действия и определения направлений совершенствования;

– обновлять планы ОИБ с учетом результатов анализа и мониторинга;

– регистрировать действия и события, способные повлиять на результативность функционирования СУИБ.

Совершенствование СУИБ

Группа процессов «Совершенствование» включает в себя деятельность по принятию решений о реализации тактических и/или стратегических улучшений СУИБ. Переход к этому этапу осуществляется только тогда, когда выполнение процессов этапа «Проверка» привело к выводу, что требуется совершенствование СУИБ.

При этом сама деятельность по совершенствованию СУИБ должна реализовываться в рамках групп процессов «Реализация» и «Планирование» (идентификация новой угрозы ИБ и последующие оценки рисков на стадии планирования). При этом важно, чтобы все заинтересованные стороны немедленно извещались о проводимых улучшениях СУИБ и при необходимости проводилось соответствующее обучение [11; 14; 21].

Реализация и внедрение данного процесса позволяет достичь намеченных целей:

– в организации действует механизм непрерывного улучшения СУИБ в целом и отдельных ее процессов;

– все выявленные или прогнозируемые отклонения показателей функционирования СУИБ от нормальных значений учитываются, и предпринимаются действия для исправления ситуации.

Основной задачей данного процесса являются предупреждение и устранение причин несоответствий ситуаций, когда процессы или меры по ОИБ не соответствуют требованиям, заданным законодательством, международными стандартами, нормативно-распорядительными или иными документами, регламентирующими вопросы ОИБ в рамках области действия СУИБ организации.

Более детально для совершенствования СУИБ организация должна [1; 21]:

– выявлять возможности тактического и стратегического улучшений СУИБ;

– предпринимать корректирующие действия, использовать на практике опыт ОИБ, полученный как в самой организации, так и в других структурах;

– передавать подробную информацию о действиях/результатах по улучшению СУИБ всем заинтересованным сторонам, при этом степень детализации должна соответствовать обстоятельствам, а при необходимости согласовываться дальнейшие действия;

– обеспечивать улучшения СУИБ для достижения запланированных целей.

На этапе совершенствования СУИБ с целью обеспечения его непрерывности производится разработка и внедрение корректирующих действий по результатам внутреннего аудита и анализа СУИБ, а также на основе другой значимой информации. *Корректирующее действие* – это действие, предпринятое для устране-

ния причины обнаруженного несоответствия. Оно предпринимается для предотвращения повторного возникновения несоответствия. Нужно отметить, что действие по предупреждению несоответствий часто является экономически более выгодным, чем корректирующее действие.

При корректировке функционирования СУИБ в первую очередь устраняются несоответствия двух видов:

– отсутствие или невозможность реализации некоторых требований СУИБ;

– неспособность СУИБ обеспечить соблюдение ПолИБ или реализовывать цели организации.

Документированная процедура для корректирующего действия должна определять требования [13; 22]:

– для выявления несоответствий (имеющихся и возможных);

– определения причин несоответствий;

– оценивания потребности в действиях, гарантирующих, что несоответствия не возникнут снова;

– определения и реализации требующихся действий;

– учета результатов предпринятых действий;

– анализа предпринятого действия.

Организация должна определить и предпринять действия по устранению причины несоответствия требованиям СУИБ (включая определение изменившихся рисков). Причины несоответствий могут быть разделены:

– на организационные недостатки;

– ошибки персонала;

– технические сбои;

– злоумышленные действия;

– обстоятельства непреодолимой силы.

Выявление и прогноз несоответствий защитных мер и процессов по управлению ИБ осуществляют, как правило, лица, от-

ветственные за эксплуатацию средств защиты. Несоответствия могут быть выявлены также любыми сотрудниками организации. Лицо, выявившее или спрогнозировавшее несоответствие, сообщает об этом, как правило, ответственному лицу, которое оформляет данный факт в виде необходимой записи СУИБ.

Источниками информации по выявленным или прогнозируемым несоответствиям являются:

– отчеты о внутренних и внешних аудитах ИБ;

– жалобы и рекомендации пользователей организации;

– результаты анализа функционирования СУИБ руководством;

– результаты мониторинга эффективности СУИБ;

– данные по инцидентам ИБ;

– любая другая информация, указывающая на наличие действующих или потенциальных несоответствий.

Записи о несоответствиях или о потенциальных несоответствиях должны регистрироваться. При регистрации несоответствия лучше группировать по некоторым категориям. Например, согласно тому, к какому процессу управления ИБ или к какой группе защитных мер относится несоответствие. Это может оказаться полезным для последующего анализа корректирующих действий.

В разработке (а потом – и в организации выполнения) корректирующего действия принимают участие владелец процесса СУИБ или руководитель структурного подразделения, в котором возможно возникновение или уже возникло несоответствие. Руководитель подразделения по своему усмотрению может назначить одного из сотрудников подразделения ответственным за внедрение корректирующего действия.

При разработке корректирующих действий обязательно проводятся оценка необходимости и адекватность затрат на их проведение.

При этом должны учитываться следующие факторы:

– документ или требование, к которому относится данное несоответствие;

– причины несоответствий в процессе;

– целесообразность разработки корректирующих действий;

– сроки выполнения корректирующих действий;

– сроки проверки эффективности корректирующего действия;

– ответственность за выполнение корректирующего действия и проверку его эффективности.

Решение о корректирующем действии принимается только при условии, если это действие не влияет на целостность СУИБ. Действие признается нарушающим целостность СУИБ, если его выполнение влечет за собой:

– несоответствие требованиям внутренних и внешних нормативных документов;

– нарушение требований документации СУИБ;

– снижение эффективности организационной структуры из-за появления у подразделений задач, дублирующих существующие, или появление участков с неопределенной ответственностью;

– нарушение баланса между ответственностью и полномочиями.

4.6. Основные процессы системы управления информационной безопасностью организации

В рамках процессного подхода к управлению ИБ и циклической модели PDCA приходится оперировать понятием процесса. Поэтому целесообразно определить основные способы задания и анализа процессов управления ИБ организации, реализуемых в рамках всего жизненного цикла СУИБ (процессами СУИБ). Эти процессы затрагивают все аспекты ОИБ органи-

зации, так как ИБ – это результат функционирования многих процессов, связанных с производственным процессом организации. Примерами основных процессов СУИБ являются целевые виды деятельности, называемые частными управлениями (рис. 4.9) [93].

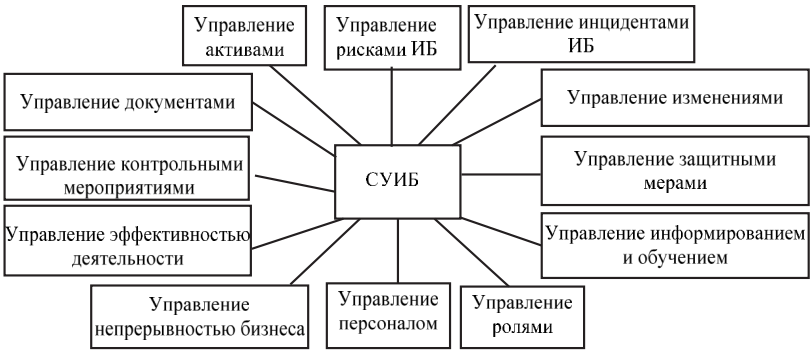

Рис. 4.9. Основные процессы СУИБ

Отдельный процесс СУИБ – связанная между собой и непрерывная во времени последовательность работ, направленная на достижение поставленной специфичной цели ОИБ [14; 21]. В то же время информационные потоки в организации могут содержать реализации согласованных действий, формально относящихся к их различным видам деятельности, частным управлениям в организации.

Задание процесса СУИБ

Прежде, чем приступать к анализу процесса СУИБ, следует определить, каковы его параметры и какие из них представляют наибольший интерес. Как отмечается во многих стандартах, при задании процесса СУИБ или его описании необходимо учитывать следующие параметры [5; 23; 89; 90; 98]:

– название (определение) процесса;

– реализуемые в рамках процесса функции или их совокупность;

– структура процесса – элементы и взаимосвязи между ними;

– взаимосвязи процесса с другими процессами в организации;

– порядок деятельности в рамках реализации процесса;

– алгоритм процесса;

– участники процесса;

– ответственное лицо – руководитель (владелец) процесса;

– входные и выходные данные (потоки), а также их поставщики (или потребители);

– требуемые ресурсы (производственные, технические, материальные, информационные и т. п.);

– цель (цели) процесса;

– оценка эффективности процесса, метрики процесса, процедуры мониторинга процесса;

– риски процесса;

– глоссарий процесса с описанием терминов;

– место документа «Описание процесса СУИБ» в системе документации организации более высокого уровня;

– статус документа «Описание процесса СУИБ»: рабочая версия, когда утвержден, дата создания, автор, лицо, утвердившее документ, дата изменения и дата сдачи в архив и т. д.

В различных ситуациях могут использоваться разные параметры процессов, реализуемых в рамках СУИБ. Так, например, знание целей процессов может существенно помочь на этапе выбора области действия будущей СУИБ, так как на их основе определяется важность и потребность в защите тех или иных производственных процессов организации. При анализе рисков ИБ сбор информации об активах потребует обращения к владельцам процессов, а также об активах, используемых в этих процессах. Для анализа рисков ИБ важна информация о входах/выходах процесса и о его участниках. Заранее определенные ме-

трики процесса упрощают мониторинг процесса, в частности, сравнение результатов разных видов мониторинга позволит сделать выводы о тенденциях в работе процесса и о возможных несоответствиях и разработать корректирующие действия, устраняющие причины несоответствий.

Из приведенных примеров видно, что описания процессов крайне желательны, так как это существенно облегчает процессы разработки СУИБ, ее внедрения и эксплуатации.

Одним из определяющих параметров в описании процесса СУИБ является его цель. Каждый процесс должен иметь цель или систему целей, на достижение которых он направлен. Они устанавливаются, исходя из требований потребителей результатов (выходных потоков) процесса. Стандарты, рассматривающие СУИБ, рекомендуют сформулировать одну, наиболее важную цель процесса, поскольку именно на ее основе формируется метрика данного процесса. Использование нескольких целей потребует определения их интегральной оценки путем введения весовых коэффициентов. Интегральная оценка необходима для определения единой метрики процесса СУИБ.

Цели могут меняться с течением времени. Например, на начальном этапе жизненного цикла у процесса СУИБ одни цели. Через некоторое время, когда процесс выстроен и оптимизирован настолько, что достижение ранее поставленных целей гарантируется, цель процесса может изменяться.

Идентификация процессов СУИБ организации

Под идентификацией понимают определение состава процессов СУИБ, имеющих ключевое значение в рамках области действия ОИБ, составление их перечня, а также разработку модели каждого процесса, включающей краткую характеристику, последовательность действий и процедур процесса, показатели оценки процесса [5; 89; 90; 98].

Идентификацию процессов СУИБ упрощает составленный до начала работ по ее созданию перечень производственных процессов организации, нуждающихся в обеспечении их ИБ. Наличие такого перечня может существенно снизить трудозатраты на выбор области и границ действия СУИБ и сделать это наиболее корректным образом, исходя из целей организации.

Исходными данными для идентификации процессов СУИБ служит точная информация о характеристиках производимой продукции или услугах, активах, инцидентах, рисках ИБ.

Схему взаимодействия процессов СУИБ следует представлять уже на этом этапе, чтобы проверить корректность входов и выходов, а также названий процессов. Входы и выходы помогут более четко определить границы процессов СУИБ, на каком этапе и чем заканчивается тот или иной процесс, что «запускает» данный процесс вслед за собой. С помощью указанной схемы взаимодействия можно выявить пересечения и несоответствия процессов.

При выборе названий процессов СУИБ предпочтительны короткие словосочетания, отражающие суть выполняемой деятельности и ее результат, например, «управление инцидентами ИБ» – или просто «инциденты ИБ», «управление активами» – или просто «активы».

Лучшие практики в отношении СУИБ обычно рекомендуют придерживаться правила: «один процесс СУИБ – одно подразделение – один бюджет – один руководитель процесса». Процессная модель управления не противопоставляет и не отвергает распространенную функциональную модель с вертикальной иерархической структурой и не противоречит проектному управлению. Процессная модель – еще одно представление функций и взаимосвязей в организации, базовым элементом управления которой являются виды деятельности и их результаты, причем

акцент делается именно на управлении результатами с заданными параметрами, а не только на исполнении функции.

В большинстве организаций руководители подразделений в рамках своих полномочий распоряжаются ресурсами, несут ответственность и являются руководителями своих процессов. Поэтому при идентификации процессов СУИБ требуется уточнить обязанности, этапы и взаимосвязи процессов. Исключением из правила являются процессы, охватывающие деятельность нескольких подразделений: управление документацией, внутренние аудиты, анализ СУИБ со стороны руководства и т. п.

После составления начального варианта процессов СУИБ и схемы взаимодействия каждый процесс обеспечивается ресурсами. Следовательно, для функционирования СУИБ необходимы обеспечивающие процессы, поставщики ресурсов: персонала, оборудования, технологий, методик, средств измерений и т. д. Классифицировав виды ресурсов, для каждого процесса СУИБ следует определить процессы-поставщики.

Далее производится идентификация процессов оценки для продукции или услуг, самих процессов СУИБ, их потребителей и поставщиков. При этом оценка может быть частью какого-либо процесса СУИБ. Выделять ее в отдельный процесс целесообразно при необходимости отслеживать результаты (выходы). Здесь должны учитываться результаты мониторинга и измерения параметров процессов СУИБ, внутренних аудитов ИБ, анализа СУИБ со стороны руководства и т. д.

Допускается объединение процессов поставщиков ресурсов и процессов измерения параметров в группу «обеспечивающие процессы», при этом понимая обеспечение более широко, как обеспечение функционирования СУИБ.

Помимо непосредственной идентификации, необходимо назначить руководителей (владельцев), связанных с производ-

ственными процессами выявленных процессов СУИБ. Руководитель процесса СУИБ – должностное лицо или коллегиальный орган, который имеет в своем распоряжении ресурсы процесса, информацию о нем, управляет ходом процесса и несет ответственность за его результат перед вышестоящим руководителем. Руководитель не касается функций, выполняемых в рамках процесса отдельными исполнителями; ему важна успешная реализация всего процесса.

Руководитель процесса СУИБ обеспечивает взаимодействие с поставщиками входных потоков процесса и с потребителями его результатов. Он обладает наиболее полными знаниями о процессах СУИБ, владельцем которых он является, поэтому в случае необходимости описания процессов или получения каких-либо других сведений о процессе необходимо обращаться именно к нему.

Критерии выбора руководителя процесса СУИБ:

1) детальное знание производственного процесса, компетентность и профессиональные знания;

2) возможность влиять на персонал и способствовать изменениям (достаточный уровень полномочий);

3) коммуникативные способности, поскольку любые изменения в процессе СУИБ могут приводить к возникновению различных конфликтов;

4) понимание важности возложенных обязанностей, заинтересованность и надлежащая мотивация.

В обязанности руководителей процессов СУИБ входят:

– разработка и организация процесса для достижения заданных результатов (выходов) процесса;

– расчет и обоснование ресурсов процесса;

– обеспечение выхода процесса установленным требованиям;

– обеспечение удовлетворенности потребителей процесса.

Помимо этого, руководители процессов СУИБ должны обладать достаточными полномочиями:

– для распоряжения ресурсами процесса (планирование работ, контроль, оценка результатов, поощрение сотрудников и т. д.);

– измерения параметров и анализа процесса;

– решения проблем и улучшения процесса.

После определения состава процессов оформляется перечень процессов СУИБ с присвоенным каждому процессу названием, обозначением и руководителем. Для каждой организации перечень процессов будет индивидуальным, отражающим присущие виды деятельности, производимую продукцию и услуги. Проверить этот перечень на соответствие требованиям ГОСТ Р ИСО/МЭК 9001 [89; 90] можно сопоставлением пунктов стандарта и процессов СУИБ.

Поскольку любую операцию можно считать процессом, надо ограничить степень детализации при определении состава процессов СУИБ. Необходимо, прежде всего, учитывать результат процесса, который важно отслеживать в СУИБ как значимый фактор или условие достижения целей организации.

Следующей задачей после составления предварительного перечня процессов СУИБ является создание моделей процессов, обладающих:

– наглядностью и полнотой описываемого процесса без дублирования информации;

– возможностью анализа процесса руководителями, аудиторами и проектными группами;

– рациональным использование разработанной и подтвердившей на практике свою ценность документации организации.

Документирование и описание процесса СУИБ

Цель документирования процессов СУИБ – описание их текущего состояния, что является первым шагом к совершенство-

ванию. При этом необходимо стремиться к описанию реального, а не идеального состояния.

Описание процесса СУИБ определяет его сущность и структуру, позволяя эффективно планировать, обеспечивать, управлять и улучшать его. Можно выделить следующие цели описания [5; 89; 90; 98]:

– отображение реально существующих процессов;

– разработка системы управления процессами;

– управление работающими процессами;

– внедрение стандартных методов представления и описания процессов;

– формулирование измеримой цели для каждого процесса;

– создание упорядоченной структуры взаимосвязанных процессов, однозначно понимаемой и воспринимаемой всеми сотрудниками организации;

– получение возможности повторного использования отдельных процессов в других процессах (модульный принцип);

– разработка показателей эффективности, позволяющих оценить степень достижения цели процесса;

– снижение стоимости и повышение качества выполнения процессов;

– уточнение количества и вида ресурсов для осуществления процессов;

– распределение полномочий и ответственности участников процесса;

– создание системы рабочих групп, занимающихся организацией процессов в подразделениях.

Отдельный процесс СУИБ может состоять из подпроцессов, которые, в свою очередь, также могут состоять из подпроцессов. Степень декомпозиции процессов определяется самой организацией.

Степень детализации процессов СУИБ должна определяться, исходя из необходимости обеспечения эффективности управления процессами, их сложности, размеров и потребностей в новых методах управления организацией. В соответствии с ГОСТ Р ИСО/МЭК 9001 документированию в рамках процесса подлежат: планирование и обеспечение, управление ходом процесса, ресурсы, процессы контроля [89; 90].

Документированной процедурой называется оформленное и поддерживаемое в актуальном состоянии описание последовательности действий в рамках системы процессов. Суть процедуры – алгоритм исполнения процесса в конкретных условиях, обеспечивающий его заданное качество. Для одного процесса может разрабатываться несколько процедур, различающихся, например, условиями их выполнения, последовательностью действий и т. п. [89; 90].

Документированная процедура включает:

– цель процедуры (с учетом направления деятельности, описанной в процедуре);

– область действия;

– нормативные ссылки;

– термины, определения, аббревиатуры и сокращения;

– ответственность и полномочия;

– описание деятельности в соответствии с назначением процедуры (входные данные, ресурсы (персонал, документация, оборудование, материалы), алгоритм выполняемой деятельности, последовательность выполняемых действий в соответствии с установленной целью, способы и средства мониторинга, анализируемые данные о результатах деятельности, выходные данные);

– регистрируемые данные;

– сведения о согласовании, утверждении, пересмотре процедуры;

– приложения.

Описание процесса СУИБ, отражающее последовательность действий, состав и содержание отдельных процедур, также можно представить в виде блок-схем. Такая форма описания достаточно информативна и удобна в работе, поскольку дает наглядное представление о последовательности работ, требованиях к выполнению этапов, ответственных исполнителях.

Также должен быть составлен общий перечень всех процессов СУИБ, в котором отражаются:

– записи, позволяющие идентифицировать описания процессов;

– информация, определяющая место «Перечня процессов СУИБ» в документации более высокого уровня, например, руководстве по качеству;

– информация, идентифицирующая состояние документа «Перечень процессов СУИБ»: статус (рабочая версия, утвержден и пр.), дата создания, автор, дата утверждения, лицо, утвердившее документ, дата изменения, дата сдачи в архив и т. д.

Мониторинг и измерение параметров процесса СУИБ

С целью определения состояния, возможностей совершенствования и соответствия установленным требованиям процессы СУИБ должны подвергаться контролю и проверке. Процесс оценивания включает этапы (рис. 4.10) [4]:

1) определения входных данных: назначение, область действия, ограничения (по времени, доступности и т. п.), особенности, подход, критерии компетентности специалиста по оценке;

2) определения основных ролей и обязанностей;

3) представления руководства для планирования, сбора данных, проверки достоверности, определения характеристик процесса и сообщения результатов оценки;

4) фиксирование выходных данных оценки.

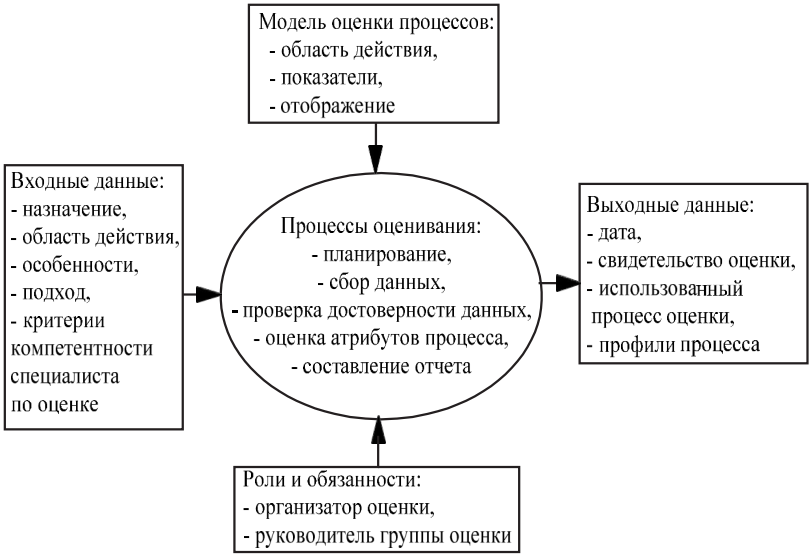

Рис. 4.10. Основные элементы процесса оценивания процессов СУИБ

Процесс оценивания процессов СУИБ основан на модели их оценки, включающей область действия; показатели, используемые для определения степени достижения целей процессов.

В рамках функционирования СУИБ осуществляются периодический мониторинг, измерение параметров и анализ работы ее процессов. Мониторинг процесса СУИБ означает постоянное наблюдение (слежение) за его показателями. *Измерение параметров процесса СУИБ* – это совокупность операций для установления значения величины параметров процесса.

Анализ процесса СУИБ – деятельность, предпринимаемая для установления адекватности, эффективности рассматриваемого процесса для достижения установленных целей [5].

Основными методами мониторинга и измерения параметров процесса являются:

– инструментальный (с помощью измерительного оборудования);

– социологический (анкетирование, опрос);

– экспертный (оценки специалистов-экспертов).

Мониторинг СУИБ как непрерывный процесс начинается с установления и определения потребностей и действий по наблюдению, требует постоянной координации. Должно быть определено, что подлежит мониторингу, когда и что конкретно свидетельствует об отклонениях от нормального функционирования (например, что относится к инцидентам ИБ). Результаты мониторинга обязательно фиксируются с требуемой степенью детализации.

Для достижения целей мониторинга, измерения параметров и анализа для каждого процесса СУИБ определяются количественные показатели, являющиеся результатом измерения или расчета, и/или качественные характеристики какого-либо свойства процессов СУИБ.

Под показателем процесса СУИБ понимают обобщенную характеристику, дающую качественную или количественную оценку степени достижения процессом управления ИБ своей цели. Она рассчитывается по определенной методике, адекватно характеризуя результат функционирования процесса.

При этом должно быть определено целевое (нормативное) значение или критерий, величина или интервал величины, которым должен соответствовать тот или иной показатель процесса СУИБ. Критерий устанавливается в зависимости от целей процесса и статистических данных о характеристиках процесса за предыдущие периоды.

Для оценки процессов СУИБ можно использовать показатели, которые должны быть адекватными назначению процесса, требованиям его внутренних и внешних потребителей, целям организации [98]:

1) *результативность* – степень реализации запланированной деятельности и достижения запланированных результатов;

2) *корректность* – степень соответствия реализации реального процесса его описанию;

3) *управляемость* – степень, в которой производится управление выполнением процесса и получение результатов, отвечающих определенным целевым показателям;

4) *эффективность* – соотношение между достигнутым результатом и использованными ресурсами (время, финансы и т. д.);

5) *повторяемость* – способность процесса создавать выходные потоки с одинаковыми характеристиками при повторных его реализациях;

6) *гибкость* (адаптируемость) – способность процесса приспосабливаться к изменениям внешних условий, перестраиваться так, чтобы не снижались ни результативность, ни эффективность;

7) *экономичность* (стоимость) – совокупная стоимость выполнения функций процесса и передачи результатов от одной функции к другой.

Взаимосвязь трех важных понятий «результативность», «эффективность» и «экономичность» применительно к СУИБ показана на рис. 4.11.

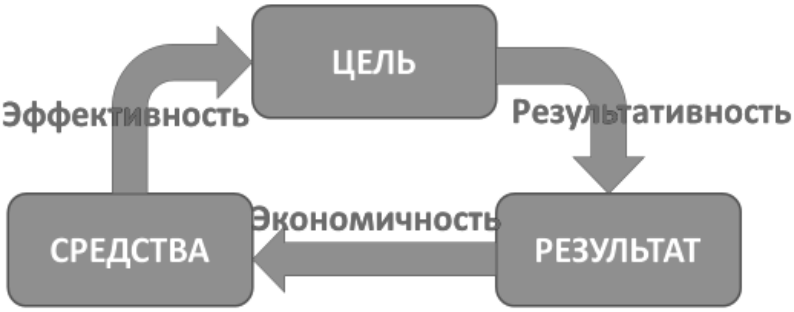

Рис. 4.11. Взаимосвязь понятий «эффективность», «результативность» и «экономичность»

Эффективность связана с затратами на проведение деятельности по ОИБ для реализации целей функционирования СУИБ, направленной на достижение планируемого результата. *Экономичность* оценивает затраты на достижение конкретного результата, который в общем случае может не совпадать с целью деятельности. *Результативность* СУИБ есть своего рода разность между экономичностью и эффективностью СУИБ.

Показатели оценки процессов СУИБ должны быть измеримыми величинами, рассчитываемыми на основе данных, полученных из достоверных источников информации. Для показателей определяются название, единицы измерения, нормативные значения, с которыми будут сравниваться измеренные значения, источники данных, расчетные формулы, периодичность оценки.

При упрощенном подходе, если показатели оценки находятся в пределах нормативных значений, то процесс считается результативным. При отклонениях от нормы можно подсчитать, насколько процесс результативен. Если трудно определить результат (выход) процесса и показатели его оценки, то, возможно, при этом потребуется внесение изменений в перечень процессов СУИБ, так как отсутствие или «размытость» результата противоречит сути процессного подхода: каждая деятельность должна быть направлена на получение измеримого результата при достижении общих целей организации.

Информацию, задающую показатели оценки процессов СУИБ, можно оформить отдельными, периодически пересматриваемыми документами по каждому процессу с названием «План мониторинга процесса СУИБ». Решение о пересмотре показателей оценки процессов может приниматься при анализе СУИБ. Отчеты по результатам мониторинга процессов СУИБ должны соответствовать стандартам ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004–2011 [24; 25].

4.7. Стратегии построения и внедрения системы управления информационной безопасностью

Когда перед организацией стоит задача внедрения СУИБ, можно выбрать один из двух подходов, каждый из которых имеет свои преимущества и недостатки:

– построение и внедрение СУИБ в целом;

– построение и внедрение процессов управления ИБ по отдельности с последующим объединением их в единую СУИБ.

При выборе первого подхода через непродолжительное время возможно обеспечить логическую связь между процессами управления ИБ и создать условия для работы СУИБ на всех этапах цикла PDCA. Например, по результатам внутренних аудитов ИБ можно исправить причины несоответствий критериям аудита посредством внедрения корректирующих действий. При таком варианте от начала разработки СУИБ до ее внедрения в эксплуатацию проходит, как правило, около года.

При последовательном построении процессов управления ИБ также существуют свои преимущества. Основное из них – процессы будут внедряться постепенно, тщательнее будут отлаживаться и корректироваться в соответствии с потребностями организации. Например, если начать процесс внедрения СУИБ с процесса управления инцидентами ИБ, уже через полгода эффективной работы процесса будет накоплена существенная статистика по угрозам ИБ, характерным для данной организации и ее активов. Наличие такой базы даст возможность приступить к разработке процесса анализа рисков ИБ и в качестве каталога угроз ИБ использовать данные, накопленные в результате работы процесса управления инцидентами ИБ.

Использование угроз ИБ, типичных для активов данной организации, позволяет более точно оценить риски ИБ для ее активов по сравнению с использованием каталогов типовых угроз

ИБ. В качестве другого примера можно взять процесс внутренних аудитов ИБ, который начинает приносить свои плоды уже с момента внедрения и проведения первых аудитов. И хотя данный вариант внедрения СУИБ сулит множество преимуществ, внедрение всей системы может занять не один год.

Для любой стратегии построения и внедрения СУИБ важнейшим вопросом является ее интеграция в общую деятельность организации, включая определение того, как и в какой мере затраты на СУИБ найдут отражение в результатах производственного процесса. Поэтому построению и внедрению СУИБ должно предшествовать определение уязвимостей в информационной инфраструктуре организации, и в связи с этим должны быть сформулированы цели и задачи ОИБ. Перед внедрением СУИБ необходимо разработать большое количество процессов и документов, поддерживающих и обеспечивающих работу основных процессов управления ИБ, выявить исполнителей этих процессов и тех, кто будет управлять данными процессами и работой СУИБ в целом.

Важно определить и желательно закрепить за конкретными участниками базовые роли СУИБ, в рамках которых будет осуществляться управление. Так, например, необходима роль менеджера СУИБ. Он назначается из состава руководства организации, наиболее подготовленного для данной роли. Менеджер по ИБ отвечает за общее руководство деятельностью по ОИБ в рамках СУИБ организации. В его обязанности входят, следующие функции:

– обеспечивать планирование мероприятий в рамках СУИБ;

– согласовывать внесение изменений в документацию и процессы СУИБ;

– обеспечивать руководство работой ответственных по вопросам ОИБ;

– консультировать по спорным вопросам СУИБ;

– составлять годовые планы обучения по СУИБ;

– составлять годовые планы внутренних аудитов, а также планы каждого из внутренних аудитов;

– участвовать в работе процессов управления ИБ;

– доводить до руководства информацию о критичных инцидентах ИБ, решения по внесению изменений и т. д.

Исполнители ролей в рамках СУИБ и отдельных процессов управления ИБ должны обладать достаточными полномочиями для принятия всех необходимых решений и выполнения всех обязательных функций в рамках этих ролей. Например:

1) владелец, несущий ответственность за актив, организует его ОИБ в виде формализованных правил, технических политик, настроек конфигурации, организационных мероприятий и регламентов;

2) владелец процесса управления ИБ – должностное лицо (сотрудник) подразделения, входящего в область действия СУИБ, которое управляет процессом, имеет в своем распоряжении персонал, инфраструктуру и информацию о ходе (состоянии) процесса и отвечает за результативность и эффективность своего процесса;

3) пользователь СУИБ – любой сотрудник подразделения организации.

Подобное распределение ролей хорошо тем, что позволяет правильно планировать процессы и обязанности отдельных субъектов в рамках функционирования СУИБ.

Но помимо того, что необходимо распределить роли и закрепить их за конкретными исполнителями, требуется обучить исполнителей ролей. Организация должна гарантировать, что все сотрудники, на которых возложены обязанности, определенные в СУИБ, имеют надлежащую квалификацию для решения необходимых задач. Для этого организация должна [14; 21]:

– определить необходимый уровень квалификации сотрудников, выполняющих работы, связанные с СУИБ;

– обеспечить обучение или принять другие меры (например, нанять квалифицированный персонал) для удовлетворения этих потребностей;

– оценить эффективность принятых мер;

– вести записи об образовании, обучении, навыках, опыте и квалификации.

Организация должна также гарантировать, что весь задействованный персонал осведомлен о значимости и важности его деятельности по ОИБ, а также о том, каким образом этот персонал участвует в достижении целей СУИБ.

Построение и внедрение СУИБ в целом – трудоемкая задача, так как на этапе разработки требуется отследить все взаимосвязи между процессами управления ИБ, а также сконструировать и связать большое количество процессов таким образом, чтобы они заработали эффективно.

Объемы и сложность решаемых задач требуют слаженной работы команды специалистов. При построении СУИБ, внедряемой по данной схеме, необходимо организовать рабочую группу, которая включает в себя специалистов в разных областях: специалистов по ИБ, владельцев производственных процессов (например, это линейные руководители подразделений), специалистов по информационно-технологической поддержке, кадровых работников, представителей финансового подразделения и т. д. Помимо этого, необходимо не забывать про роль высшего руководства в этом процессе.

Как правило, при данной схеме внедрения СУИБ большой объем работ идет параллельно. При внедрении СУИБ в целом осуществляется разработка и практически одновременное внедрение перечисленных ранее процессов управления ИБ,

реализуемых в рамках функционирования СУИБ: управление рисками ИБ, инцидентами ИБ и т. д. В такой ситуации важную роль играют грамотное планирование работ и их хорошая координация.

Для построения ряда процессов необходимо соблюдать определенную последовательность. Так, после утверждения области действия будущей СУИБ и разработки ее политики следует приступить к анализу рисков ИБ. И только после получения результатов работы данного процесса, отчета по результатам анализа рисков ИБ и плана обработки рисков ИБ можно приступить к разработке необходимых процессов и процедур, учитывающих, если это необходимо, планируемые защитные меры.

Поскольку в рамках СУИБ составляется достаточно большое количество документов, а по процессам управления ИБ создаются записи, еще на ранних стадиях разработки СУИБ необходимо разработать и внедрить функционирующие под ее контролем процессы управления документами и записями. После этого можно приступать к разработке группы процессов анализа и улучшения СУИБ (внутренние аудиты ИБ; мониторинг эффективности процессов и защитных мер; управление корректирующими действиями), а также процессов управления инцидентами ИБ.

При выборе стратегии внедрения СУИБ в целом существуют различные варианты ее построения, которые в основном затрагивают аспекты выбора области действия. Существует две возможности – внедрение СУИБ для небольшой (ограниченной) области действия с последующим расширением или сразу для всей области действия.

СУИБ для небольшой области действия с последующим расширением

В качестве области действия СУИБ может быть выбран несложный процесс, в котором участвует ограниченное количество

сотрудников. Основными преимуществами такого подхода являются:

– возможность более легкой модификации процессов управления ИБ на этапе их внедрения;

– более тесная работа с сотрудниками, входящими в область действия СУИБ, в части внедрения процессов управления ИБ в культуру организации;

– оперативная связь с сотрудниками в ходе внедрения процессов управления ИБ;

– использование области действия в качестве «испытательного полигона» для отработки всех процессов управления ИБ.

Проект по построению СУИБ для достаточно простой области действия занимает меньше времени и требует на первых этапах менее тщательной отработки всех процессов. Помимо этого, данная область может быть использована в качестве полигона: процессы, разработанные в рамках данной области действия, могут быть впоследствии использованы в качестве шаблонов при расширении области действия СУИБ на другие процессы.

В рамках расширения области действия СУИБ могут применяться отработанные методики анализа рисков ИБ, обработки инцидентов ИБ, обучения сотрудников и т. д. При этом совершенно необязательно расширять зону действия всех процессов управления ИБ одновременно. Возможно постепенное ее расширение, начиная с тех процессов, которые уже хорошо отработаны на полигоне и могут принести существенную пользу при своем расширении.

При принятии решения о добавлении в область действия СУИБ новых активов организации нужно четко определить цели расширения СУИБ на них и цели самой СУИБ в рамках данных активов. Следует отметить, что расширение единой СУИБ возможно и на смежные активы. Если рассматривать отдельные,

не взаимосвязанные процессы, то, скорее всего, нужно внедрять разные локальные СУИБ.

СУИБ для большой области действия. Построение СУИБ сразу для большой области действия обладает рядом своих преимуществ и недостатков. Из преимуществ можно выделить то, что если такой проект реально запускается, то, скорее всего, имеется действительная заинтересованность руководства в нем, и для построения и внедрения СУИБ все управленческие решения будут приниматься оперативно, а необходимые ресурсы – предоставляться вовремя.

При таком подходе на этапах внедрения и дальнейшего функционирования СУИБ практически невозможно быстро вносить изменения в процессы управления ИБ. Это обусловлено тем, что такие процессы чаще всего затрагивают большое количество сотрудников. Их оповещение и обучение новым правилам не такая простая задача. Помимо этого, в связи с обширностью области действия управленческая ролевая структура, скорее всего, будет весьма разветвленной и негибкой, что повлечет за собой сложности в согласовании вносимых изменений. Механизмы получения обратной связи от пользователей СУИБ также не будут такими простыми и гибкими, как в случае внедрения СУИБ для небольшой области действия.

Однако подход, при котором СУИБ охватывает большую часть организации, может свидетельствовать о серьезном подходе руководства организации к ОИБ и управлению ею.

Построение и внедрение процессов СУИБ по отдельности

При построении и внедрении процессов управления ИБ, выполняемых в рамках функционирования СУИБ, можно выделить те же преимущества, что и для СУИБ для небольшой области действия. Однако ошибочно думать, что эти преимущества достигаются только лишь при внедрении отдельных процессов для

небольшой области действия. Если внедрять процессы постепенно, то этих же преимуществ можно добиться и при внедрении сразу же для большой области действия.

При выборе стратегии внедрения процессов СУИБ по отдельности с последующим их объединением в единую СУИБ последовательность работ, разработки и внедрения процессов будет примерно такой же, как и при внедрении СУИБ в целом. Возможно, потребуется оформление политик для каждого из процессов, которые по структуре будут совпадать со структурой общей политики СУИБ.

При внедрении отдельных процессов необходимо делать это постепенно, отводя время на внедрение процесса в культуру, обучение пользователей, внесение изменений в процесс по результатам первых циклов его работы. Именно в таком случае будут достигнуты преимущества данной стратегии внедрения СУИБ.

Поскольку процессы будут разрабатываться отдельно, возможно, разными людьми, то при их постепенном внедрении и последующем объединении в единую систему могут возникнуть проблемы с организацией взаимосвязей между процессами. Это может быть вызвано несоответствием выходных данных одного процесса и входных данных следующего за ним процесса управления ИБ, несоответствием ролей и исполнителей ролей в разных процессах и т. д. Чтобы избежать этого, необходимо иметь четкую стратегию развития процессов и СУИБ в целом, последовательно ее отслеживать и строить СУИБ в соответствии с ней.

Вопросы для самоконтроля

1. Дайте определения ОИБ, управления ИБ и СУИБ организации.

2. Опишите деятельность по ОИБ организации как процесс. Каковы его входные и выходные данные, ресурсы и управляющие воздействия?

3. Как процесс ОИБ в организации связан с процессами ее основной деятельности?

4. Какие стратегии выбора области действия СУИБ существуют?

5. Какие факторы необходимо учитывать при выборе области действия СУИБ?

6. Какие параметры процессов наиболее значимы при выборе области действия проектируемой СУИБ?

7. Что входит в документальное обеспечение СУИБ? Каковы этапы его жизненного цикла?

8. Какие уровни включает в себя иерархия документов СУИБ? Какие виды конкретных документов создаются на каждом из уровней?

9. В чем основное различие между понятиями «документ» и «запись»?

10. В чем заключается процесс управления документами и записями?

11. Какова взаимосвязь между понятиями «ПолИБ» и «политика СУИБ»?

12. Что должна включать в себя политика СУИБ?

13. На каких этапах руководство организации должно продемонстрировать свою приверженность разработке, реализации, эксплуатации, мониторингу, анализу, сопровождению и совершенствованию СУИБ?

14. В чем основная необходимость участия высшего руководства в жизненном цикле СУИБ?

15. Дайте определение процесса управления ИБ организации.

16. Какие действия и процессы выполняются на стадии планирования СУИБ? Каковы задачи данного этапа?

17. Специалистов каких подразделений необходимо включать в рабочую группу по построению СУИБ и почему?

18. Какие действия и процессы выполняются на стадии реализации и внедрения СУИБ, задачи данного этапа?

19. Какие действия и процессы выполняются на стадии проверки СУИБ, задачи данного этапа?

20. Какие действия и процессы выполняются на стадии совершенствования СУИБ, задачи данного этапа?

21. Что такое корректирующее действие?

22. Почему в рамках процессного подхода к управлению ИБ следует особое внимание уделять мониторингу и анализу эффективности СУИБ?

23. В чем различия между эффективностью и результативностью?

24. Какие этапы включает в себя идентификация процессов управления ИБ?

25. Каковы основные преимущества документирования процессов управления ИБ организации?

26. Каковы основные элементы процесса мониторинга процессов управления ИБ организации?

27. На что может указывать расхождение между целевым и текущим значениями метрик мониторинга для процессов управления ИБ?

28. Какой тип процессов управления ИБ представляет наибольший интерес для анализа и мониторинга при эксплуатации СУИБ?

29. Возможно ли построение СУИБ, охватывающей несколько территориальных подразделений организации? Какие особенности при этом необходимо учитывать?

30. В чем состоят основные преимущества и недостатки стратегии построения и внедрения СУИБ в целом?

31. В чем заключаются преимущества и недостатки стратегии построения и внедрения отдельных процессов управления ИБ с последующим их объединением в СУИБ?

32. В чем состоят преимущества и недостатки построения СУИБ для небольшой области действия с возможным расширением в будущем?

33. Каковы преимущества и недостатки построения СУИБ для большой области действия?

34. Наличие каких ролей необходимо в рамках ролевой структуры СУИБ?

35. В чем состоит преимущество использования ролевого принципа в рамках СУИБ?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Леонов, Г. А. Теория управления / Г. А. Леонов. – СПб. : СПбГУ, 2006.

2. Репин, В. Процессный подход к управлению. Моделирование бизнес-процессов / В. Репин, В. Елиферов. – М. : Стандарты и качество, 2004.

3. Акофф, Р. Планирование будущего корпорации / Р. Акофф. – М. : Сирин, 2002.

4. Аудит информационной безопасности / под ред. А. П. Курило. – М. : БДЦ-Пресс, 2006.

5. ГОСТ Р ИСО 9000–2001. Системы менеджмента качества. Основные положения и словарь. – М. : Госстандарт России, 2001. – 32 с.

6. Лигинчук, Г. Г. Основы менеджмента : учебный курс. Ч. 1 / Г. Г. Лигинчук. – М. : Московский институт экономики, менеджмента и права, 2009.

7. Нив, Г. Пространство доктора Деминга / Г. Нив. – М. : Альпина Бизнес Букс, 2007.

8. Гостехкомиссия России. Защита от несанкционированного доступа к информации. Термины и определения. – М., 1992.

9. Рекомендации по стандартизации Р 50.1.053–2005. Информациионные технологии. Основные термины и определения в области технической защиты информации : утв. приказом Ростехрегулирования от 6 апреля 2005 г. № 77-ст. – М. : Стандартинформ, 2005.

10. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. – М. : Стандартинформ, 2008.

11. Стандарт Банка России СТО БР ИББС-1.0. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. – М. : Банк России, 2001.

12. Галатенко, В. А. Основы информационной безопасности / В. А. Галатенко. – М. : Бином : Лаборатория знаний «Интуит», 2008.

13. ГОСТ Р ИСО/МЭК 17799–2005. Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью. – М. : Стандартинформ, 2006.

14. ГОСТ Р ИСО/МЭК 27001–2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М. : Стандартинформ, 2008.

15. ГОСТ Р 53113.1–2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Ч. 1: Общие положения. – М. : Стандартинформ, 2009.

16. Information Security Management Systems (ISMS), BSI Standard 1001, Version 1.5, Mai 2008. – URL: http://www.bsi.bund.de.

17. lTGrundschutz Methodology, BSI Standard 1002, Version 2.0, Mai. – URL: http://www.bsi.bund.de.

18. Risk Analysis on the Basis of ITGrundschutz, BSI Standard 1003, Version 2.5, Mai 2008. – URL: http://www.bsi.bund.de.

19. Business Continuity Management, BSI Standard 1001, Version 1.0, November 2008. – URL: http://www.bsi.bund.de.

20. ISO/IEC 27000:2009. Information technology. Security techniques. Information security management systems. Overview and vocabulary. – URL: http://www.iso.org.

21. ISO/IEC 27001:2005. Information technology. Security techniques. Information security management systems. Requirements. – URL: http://www.iso.org.

22. ISO/IEC 27002:2005. Information technology. Security techniques. Code of practice for information security management. – URL: http://www.iso.org.

23. ISO/IEC 27003:2010. Information Technology. Security Techniques. Information Security Management Systems Implementation Guidance. – URL: http://www.iso.org.

24. ISO/IEC 27004:2009. Information technology. Security techniques. Information security management. Measurement. – URL: http://www.iso.org.

25. ГОСТ Р ИСО/МЭК 27004–2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. – М. : Стандартинформ, 2012.

26. ISO/IEC 27005:2011. Information technology. Security techniques. Information security risk management. – URL: http://www.iso.org.

27. ISO/IEC 133353:1998. Information technology. Guidelines for the management of IT Security. Part 3: Techniques for the management of IT Security. – Curso : Universidad de Cadiz, 2003.

28. ISO/IEC 133354:2000. Information technology. Guidelines for the management of IT Security. Part 4: Selection of safeguards. – Curso : Universidad de Cadiz, 2003.

29. ГОСТ Р ИСО/МЭК 51897–2002. Менеджмент риска. Термины и определения. – М. : Госстандарт России, 2003.

30. BS 77993:2006. Information security management systems. Guidelines for information security risk management. – Gaithersburg : National Institute of Standards and Technology, 2007.

31. ГОСТ Р ИСО/МЭК 27005–2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – М. : Стандартинформ, 2011.

32. ISO/IEC 27006:2011. Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems. – URL: http://www.iso.org.

33. ГОСТ Р ИСО/МЭК 27006:2008. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, обеспечивающим аудит и сертификацию систем менеджмента информационной безопасности. – М. : Стандартинформ, 2010.

34. ISO/IEC 27007:2011. Information technology. Security techniques. Guidelines for Information Security Management Systems auditing. – URL: http://www.iso.org.

35. ISO/IEC 27008:2011. Information technology. Security techniques. Guidance for auditors on ISMS controls. – URL: http://www.iso.org.

36. ISO/IEC 27011:2008. Information technology. Security techniques. Information security management guidelines for telecommunications organizations based on ISO/IEC 27002. – URL: http://www.iso.org.

37. ITUT Recommendation X.1051 Information security management system. Requirements for telecommunications (ISMST). – URL: http://www.itu.int.

38. ISO/IEC 27013. Information technology. Security techniques. Guideline on the integrated implementation of ISO/IEC 200001 and ISO/IEC 27001. – URL: http://www.iso.org.

39. ISO/IEC 200001:2005. Information technology service management. Specification for Service Management. – URL: http://www.iso.org.

40. ISO/IEC 200002:2005. Information technology service management. Code of Practice for Service Management. – URL: http://www.iso.org.

41. ISO/IEC 27014. Information technology. Security techniques. Information security governance framework. – URL: http://www.iso.org.

42. ISO/IEC 27031:2011. Information technology. Security techniques. Guidelines for information and communications technology readiness for business continuity. – URL: http://www.iso.org.

43. BS 25777:2008. Information and communications technology continuity management. Code of practice. – Gaithersburg : National Institute of Standards and Technology, 2009.

44. PAS 77:2006. IT Service Continuity Management. Code of practice. – URL: http://www.bsi.bund.de.

45. ISO/IEC 270331:2009. Information technology. Security techniques. Network security. Part 1: Overview and concepts. – URL: http://www.iso.org.

46. ГОСТ Р ИСО/МЭК 270331–2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Ч. 1: Обзор и концепции. – М. : Стандартинформ, 2012.

47. ISO/IEC 270333:2010. Information technology. Security techniques. Network security. Part 3: Reference networking scenarios. Threats, design techniques and control issues. – URL: http://www.iso.org.

48. ISO/IEC 27035:2011. Information technology. Security techniques. Information security incident management. – URL: http://www.iso.org.

49. ISO/IEC TR 18044:2004. Information technology. Security techniques. Information security incident management. – URL: http://www.iso.org.

50. ГОСТ Р ИСО/МЭК ТО 18044–2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. – М. : Стандартинформ, 2009.

51. BS 10008:2008. Evidential weight and legal admissibility of electronic information. Specification. – Gaithersburg : National Institute of Standards and Technology, 2009.

52. ISO/IEC 133351:2004. Information technology. Security techniques. Management of information and communications technology security. Part 1: Concepts and models for information and communications technology security management. – URL: http://www.iso.org.

53. ISO/IEC 133355:2001. Information technology. Security techniques. Management of information and communications technology security. Part 5: Management guidance on network security. – URL: http://www.iso.org.

54. ГОСТ Р ИСО/МЭК 13335-1–2006. Информационная технология. Методы и средства обеспечения безопасности. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. – М. : Стандартинформ, 2007.

55. ГОСТ Р ИСО/МЭК ТО 13335-3–2007. Информационная технология. Методы и средства обеспечения безопасности. Методы менеджмента безопасности информационных технологий. – М. : Стандартинформ, 2007.

56. ГОСТ Р ИСО/МЭК ТО 13335-4–2007. Информационная технология. Методы и средства обеспечения безопасности. Выбор защитных мер. – М. : Стандартинформ, 2008.

57. ГОСТ Р ИСО/МЭК ТО 13335-5–2006. Информационная технология. Методы и средства обеспечения безопасности. Руководство по менеджменту безопасности сети. – М. : Стандартинформ, 2007.

58. ISO/IEC 154081:2009. The Common Criteria for Information Technology Security Evaluation. 1: Introduction and general model. – URL: http://www.iso.org.

59. ISO/IEC 15408-2:2008. The Common Criteria for Information Technology Security Evaluation. Security functional components. – URL: http://www.iso.org.

60. ISO/IEC 154083:2008. The Common Criteria for Information Technology Security Evaluation. Security assurance components. – URL: http://www.iso.org.

61. ГОСТ Р ИСО/МЭК 15408-1–2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1: Введение и общая модель. – М. : Стандартинформ, 2009.

62. ГОСТ Р ИСО/МЭК 15408-2–2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2: Функциональные требования безопасности. – М. : Стандартинформ, 2009.

63. ГОСТ Р ИСО/МЭК 154083–2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 3: Требования доверия к безопасности. – М. : Стандартинформ, 2009.

64. ISO/IEC 18045:2008. Information technology. Security techniques. Methodology for IT security evaluation. – URL: http://www.iso.org.

65. ГОСТ Р ИСО/МЭК 18045–2008. Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий. – М. : Стандартинформ, 2009.

66. ISO 19011:2011. Guidelines for auditing management systems. – URL: http://www.iso.org.

67. ГОСТ Р ИСО 19011–2003. Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента. – М. : Стандартинформ, 2004.

68. BS 259991:2006. Business continuity management. Code of practice. – Gaithersburg : National Institute of Standards and Technology, 2009.

69. BS 259992:2007. Business continuity management. Specification. – Gaithersburg : National Institute of Standards and Technology, 2009.

70. ГОСТ Р 53647.1–2009. Менеджмент непрерывности бизнеса. Ч. 1: Практическое руководство. – М. : Стандартинформ, 2011.

71. ГОСТ Р 53647.2–2009. Менеджмент непрерывности бизнеса. Ч. 2: Требования. – М. : Стандартинформ, 2011.

72. ГОСТ Р 53647.3–2010. Менеджмент непрерывности бизнеса. Ч. 3: Руководство по внедрению. – М. : Стандартинформ, 2011.

73. Стандарт Банка России СТО БР ИББС-1.1. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности. – М. : Банк России, 2007.

74. 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. – М. : Банк России, 2007.

75. 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. – М. : Банк России, 2010.

76. Рекомендации в области стандартизации Банка России РС 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. – М. : Банк России, 2011.

77. 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. – М. : Банк России, 2012.

78. 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. – М. : Банк России, 2012.

79. 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. – М. : Банк России, 2012.

80. Tipton, H. F. Information Security Management Handbook / H. F. Tipton, M. Krause. – 6th edition. – Taylor & Francis Group, USA, 2007.

81. Department of Defense Trusted Compute System Evaluation Criteria, DoD 5200.28STD, 1985.

82. Гостехкомиссия России. Информационная безопасность и защита информации : Сборник терминов и определений. – М. : Гостехкомиссия России, 2001.

83. Бармен, С. Разработка правил информационной безопасности / С. Бармен. – М. : Вильямс, 2002.

84. Guttman, B. An Introduction to Computer Security: The NIST Handbook / B. Guttman, E. Roback. – NIST Special Publication 80012. – 1995.

85. Запечников, С. В. Информационная безопасность открытых систем : учебник для вузов : в 2 т. Т. 1: Угрозы, уязвимости, атаки и подходы к защите / С. В. Запечников, Н. Г. Милославская, А. И. Толстой [и др.]. – М. : Горячая линия – Телеком, 2006. – 536 с.

86. ITUT Recommendation X.509 «Information Technology. Open Systems Interconnection. The Directory: Public Key and Attribute Certificate Frameworks». June 2000.

87. Mui, L. A computational model of trust and reputation / L. Mui, M. Mohtashemi, A. Halberstadt // System Sciences. – 2002. – P. 2431–2439.

88. Гражданский кодекс Российской Федерации : ГК : принят Государственной Думой Российской Федерации в 2004 г. – М. : Инфра-М : Норма, 2004.

89. ISO/IEC 9001:2008. Quality management systems. Requirements. – URL: http://www.iso.org.

90. ГОСТ Р ИСО/МЭК 9001–2001. Системы менеджмента качества. Требования. – М. : Стандартинформ, 2002.

91. Галатенко, В. Информационная безопасность в Интранет: концепции и решения / В. Галатенко, И. Трифаленков // Jet Info Online. – 1996. – № 23–24 (30–31).

92. A Guide to Developing Computing Policy Documents (SAGE Short Topics in System Administration). Edited by B. L. Dijker. 1996.

93. Обеспечение информационной безопасности бизнеса / под ред. А. И. Курило. – М. : Альпина Паблишер, 2011.

94. Проблемы управления информационной безопасностью : сборник трудов ИСА РАН / под ред. Д. С. Черешкина. – М. : Едиториал УРСС, 1998.

95. Underlying Technical Models for Information Technology Security (NIST Special Publication 80033). U.S. Government Printing Office Washington, 2001.

96. Алесинская, Т. В. Основы логистики. Общие вопросы логистического управления : учебное пособие / Т. В. Алесинская. – Таганрог : ТРТУ, 2005.

97. Теория автоматического управления : в 2 ч. / под ред. А. А. Воронова. – М. : Высшая школа, 1986.

Приложение

ЧАСТНЫЕ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. ПОЛИТИКА ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРОВ ИНТРАНЕТА

Обзор. Данная политика не накладывает ограничений, противоречащих установившейся в организации культуре открытости, доверия и целостности. Она защищает сотрудников, партнеров и саму организацию от незаконных или разрушительных действий индивидуумов, случайных или намеренных.

Системы Интернета/интранета/экстранета, включая (но не ограничиваясь) компьютеры, ПО, ОС, носители данных, учетные записи для электронной почты, средства работы с WWW и FTP, являются собственностью организации. Эти системы при их обычном функционировании должны использоваться для целей бизнеса и служить интересам организации, а также для ее клиентов и партнеров (ознакомьтесь, пожалуйста, с кадровой политикой организации).

Действенная ИБ – это результат работы команды, предполагающий участие и поддержку каждого сотрудника и подразделения организации, работающих с информацией и/или ИС. Каждый пользователь компьютера должен знать эти руководящие принципы и вести себя в соответствии с ними.

Цель политики – определить допустимое использование компьютеров организации. Данные правила защищают сотрудников организации. Недопустимое использование компьютеров создает для организации угрозы заражения компьютерными вирусами и взлома интранета и его сетевых сервисов, а также проблемы юридического характера.

Область действия. Политика применяется ко всем сотрудникам, временным рабочим, консультантам, внештатным сотрудникам и другим работникам организации, включая всех третьих лиц. политика распространяется на все компьютеры, которыми владеет или получила в лизинг организация.

Основные положения. Настоящий документ определяет:

– порядок предоставления сотрудникам доступа к компьютерам, входящим в интранет организации;

– порядок отмены доступа;

– порядок изменения прав доступа;

– требования, предъявляемые к сотрудникам организации в связи с предоставлением им доступа к компьютерам интранета;

– порядок осуществления контроля доступа;

– ответственность сотрудников организации.

Общее использование и владение. Поскольку администрация интранета организации стремится обеспечить разумный уровень секретности, пользователи должны знать, что данные, которые они создают на ее компьютерах, являются собственностью организации. Администрация интранета организации вправе знакомиться с личной конфиденциальной информацией сотрудников, хранимой на любом компьютере, принадлежащем организации.

Сотрудники должны исходить из здравого смысла при персональном использовании компьютеров интранета.

За разработку руководств по персональному использованию систем Интернета/интранета/экстранета ответственность несут отдельные департаменты. При отсутствии такой политики сотрудники должны руководствоваться ведомственной политикой персонального использования. Если сотрудники в чем-то не уверены, то они должны консультироваться со своим руководителем или администратором.

Любую информацию, которую пользователи считают конфиденциальной или уязвимой, рекомендуется шифровать. Руководство по классификации информации дано в политике работы с конфиденциальной информацией. Шифрование почтовых сообщений и документов регламентируется политикой шифрования.

С целью обеспечения функционирования интранета и его защиты уполномоченные лица внутри организации могут в любое время осуществлять мониторинг оборудования, систем и сетевого трафика (см. политику аудита ИБ).

С целью проверки на соответствие политике организация оставляет за собой право проводить аудит ИБ интранета и систем на регулярной основе.

Безопасность и составляющие информационной собственности организации. Пользовательские интерфейсы для доступа к информации, содержащейся в системах Интернета/интранета экстранета, должны быть отнесены к классу либо конфиденциальному, либо открытому (как это определено в руководствах по конфиденциальности организации). Некоторыми примерами конфиденциальной информации являются: частная собственность организации, корпоративные стратегии, требующие защиты от конкурентов производственные секреты, спецификации, списки клиентов, исследовательские данные и т. п. Сотрудники должны делать все возможное, чтобы предотвратить НСД к этой информации.

Храните пароли должным образом и не используйте совместно одну учетную запись. Авторизированные пользователи несут ответственность за защиту своих паролей и учетных записей. Системные пароли должны меняться ежеквартально, пользовательские – каждые полгода.

Все ПК, ноутбуки и рабочие станции должны быть защищены заставками с паролями, активизируемыми через 10 мин пассивности пользователя, или средствами перезагрузки.

Шифруйте данные в соответствии с политикой шифрования. Поскольку информация на переносных компьютерах особо уязвима, нужно быть особо внимательными. Защищайте ноутбуки в соответствии с рекомендациями по их защите.

Посылка сообщений в группы новостей с электронных адресов организации должна содержать приписку, что выраженное мнение является личным мнением отправителя, а не всей организации, если такая отправка сообщений не входит в обязанности сотрудника.

Все используемые сотрудниками компьютеры, соединенные с Интернетом/интранетом/экстранетом организации и являющиеся собственностью сотрудника или организации, должны постоянно сканироваться антивирусным ПО с актуальной энциклопедией обнаруживаемых вирусов, если это не нарушает ведомственную или групповую политику.

Сотрудники должны проявлять особую бдительность при открытии прикреплений к почтовым сообщениям, полученным от незнакомых отправителей, поскольку там могут находиться вирусы, почтовые бомбы или троянские программы.

Недопустимое использование. В общем случае запрещены перечисленные ниже действия. Приведенный список не является исчерпывающим, но он может служить основой для определения действий, которые попадают в категорию недопустимого использования.

Сотрудники могут быть освобождены от этих ограничений при выполнении своих законных рабочих обязанностей (например, системным администраторам может потребоваться отключить доступ компьютера к сети, если он мешает работе сервисов).

Ни при каких обстоятельствах сотрудникам организации не разрешается участвовать в каких-либо действиях по исполь-

зованию компьютеров организации, являющихся незаконными в соответствии с местным, федеральным, государственным или международным законодательством.

Работа с системами и сетями. Строго запрещаются следующие действия, все без исключения:

– нарушение прав любого человека или компании, защищенных авторским правом, торговым секретом, патентом или другой интеллектуальной собственностью, или другими законами, или актами, включая (но не ограничиваясь) установку или распространение «украденных» или других программных продуктов, на использование которых организация не имеет соответствующих лицензий;

– несанкционированное копирование авторского материала, включая (но не ограничиваясь) оцифровку и распространение фотографий из журналов, книг или других авторских источников, авторской музыки и установку любого авторского ПО, на которые организация или конечный пользователь не имеет действующей лицензии;

– экспорт ПО, технической информации, технологий и ПО для шифрования, предусмотренных международными или региональными экспортными законами (при сомнениях требуется консультация со специалистами);

– внедрение разрушающих программ в Интернет/интранет/экстранет (например, вирусов, червей, троянских коней, почтовых бомб и т. п.); передача пароля своей учетной записи или разрешение использовать эту учетную запись другим лицам (например, членам семьи при работе в домашних условиях);

– использование компьютеров организации в личных целях; мошеннические предложения продукции, изделий или услуг, исходящие с любой учетной записи организации;

– заверения о гарантиях явно или неявно, если это не является частью обычных рабочих обязанностей;

– нарушение ИБ или разрушение связей интранета («нарушение ИБ» включает (но не ограничивается) доступ к данным, вход на сервер или учетную запись, к которым сотруднику доступ не предусмотрен, если это не входит в круг его обычных рабочих обязанностей; «разрушение» включает (но не ограничивается) перехват трафика, наводнение ping-запросами, подмену пакетов, «отказ в обслуживании» и подделку информации о маршрутизации с конкретными целями); сканирование портов или защиты;

– выполнение любых форм мониторинга интранета, позволяющее перехватить данные, не предназначенные для компьютеров сотрудников, если это не является частью их обычных рабочих обязанностей; обход аутентификации пользователя или защиты любого компьютера, сегмента интранета или учетной записи;

– вмешательство в работу или блокирование сервиса для любого пользователя, отличного от компьютера сотрудника (например, реализация «отказа в обслуживании»);

– использование любой программы/сценария/команды или посылка любых сообщений с целью вмешательства или отключения пользовательских терминальных сессий, применяя любые средства, локально или через Интернет/интранет/экстранет;

– передача информации о сотруднике(ах) организации лицами вне организации.

Работа с электронной почтой и средствами связи. Строго запрещаются все без исключения следующие действия:

– посылка незапрашиваемых электронных сообщений, включая материалы рекламного характера, пользователям, которые не просили об этом (спам);

– любые формы преследования по электронной почте или телефону, независимо от языка, частоты или размера сообщений;

– несанкционированное использование или подделка заголовков почтовых сообщений;

– запрос адреса с любого другого почтового адреса, отличного от указанного в качестве отправителя, с целью беспокоить пользователя или собирать ответы;

– создание или пересылка сообщений, использующих схему пирамиды;

– использование незапрашиваемых сообщений, приходящих в интранет организации из Интернета/интранета/экстранета других сервис-провайдеров, от имени или с целью рекламы любых сервисов, предоставляемых организацией или соединение с которыми происходит через интранет организации;

– посылка одинаковых или похожих, не относящихся к бизнесу сообщений в большое число групп новостей.

Ответственность. Любой сотрудник, нарушивший политику, может быть привлечен к дисциплинарному наказанию, вплоть до увольнения с работы.

Определения. Спам – несанкционированная и/или незапрашиваемая массовая рассылка почтовых сообщений.

История пересмотра политики (например, в виде таблицы с датами внесенных изменений и их содержанием).

2. ПОЛИТИКА ИСПОЛЬЗОВАНИЯ ПАРОЛЕЙ

Обзор. Пароль является важным аспектом ОИБ. Это первый рубеж защиты учетных записей пользователей. Плохо выбранный пароль может стать причиной взлома всего интранета организации. Поэтому все сотрудники организации (включая работающих по контракту и партнеров, имеющих доступ к системам организации) являются ответственными за соответствующие шаги, как отмечено ниже, по выбору и защите своих паролей.

Цель политики – установить стандарт по созданию стойких паролей, их защите и частоте смены. Настоящая политика устанавливает требования к порядку выбора, хранения, использова-

ния, периодичности смены и другим вопросам, связанным с применением механизмов парольной аутентификации в интранете организации.

Область действия – для всего персонала, имеющего свою учетную запись или ответственного за нее (или за любую форму доступа, которая поддерживается или требует пароля) в любой системе, находящейся в организации, имеющей доступ к интранету организации или хранящей любую информацию организации, предназначенную не для всеобщего доступа.

Основные положения. Все системные пароли (например, root, NT admin, учетные записи администраторов приложений и т. п.) должны изменяться по крайней мере раз в квартал.

Все системные пароли для продуктов должны храниться в единой базе данных паролей, администрируемой соответствующей организацией (например, InfoSec).

Все пароли пользователей (например, почтовые, Интернета, для настольного компьютера и т. п.) должны изменяться, по крайней мере, каждые шесть месяцев. Рекомендуемая частота смены пароля – каждые четыре месяца.

Учетные записи пользователей, имеющие системные привилегии, заданные с помощью членства в группе или программы типа «sudo», должны иметь уникальный пароль, отличный от других паролей этого пользователя.

Пароли нельзя передавать по электронной почте или другим видам электронных средств связи.

При использовании протокола управления сетью SNMP пароли для «community strings» должны быть отличны от установок по умолчанию «public», «private» и «system» и от паролей, используемых для входа в интерактивный режим. Везде, где это возможно, должен использоваться хеш с ключом (например, SNMPv2).

Все пользовательские и системные пароли должны выбираться в соответствии с нижеприведенным руководством.

Руководство. Общее руководство по выбору паролей. В организации пароли используются с разными целями. Чаще это: пользовательские учетные записи, доступ к Интернету, почтовые пароли, пароли для заставок, пароли для голосовой почты и пароли на локальных маршрутизаторах. Поскольку не везде используются одноразовые (динамические) пароли, нужно знать, как выбрать стойкий пароль.

Слабые пароли обладают следующими свойствами:

– пароль содержит менее восьми символов;

– пароль является словом из словаря какого-либо языка;

– пароль содержит:

– фамилию и имя, кличку животного, имя друга, марку машины, фантастическое имя и т. п.;

– компьютерный термин или имя, команду, узел, наименование организации, название АО или ПО;

– производное от наименования организации;

– дату рождения или другую персональную информацию типа адреса или номера телефона;

– слово или сочетание символов типа aaabbb, qwerty, zyxwvuts, 123321 и т. п.;

– все перечисленное, только в обратном порядке написания;

– любое из перечисленного с цифрой на конце или в начале (например, secretl, lsecret).

Сильный пароль имеет следующие характеристики:

– содержит символы верхнего и нижнего регистра;

– наряду с буквами содержит цифры и знаки препинания ('(2)#$%Л &*( )_+l~ = V {}[]:»;'<>?,./);

– состоит не менее чем из восьми символов;

– не является словом любого языка, сленга, диалекта, жаргона и т. п.;

– не содержит персональной информации, фамилии и т. п.;

– не записан рядом с компьютером или хранится на нем в специально с этой целью созданном файле.

Лучше выбрать пароль, который легко запомнить. Один из способов – взять за основу название песни, пословицы и т. п. Например, на основе фразы «This May Be One Way To Remember» можно создать пароль «TmBlw2R!» или «TmblW>r~».

Стандарты защиты паролей. Все пароли являются конфиденциальной информацией организации.

Для учетных записей в организации и вне нее используйте разные пароли. Внутри организации для различного доступа (к приложениям, к разным ОС и т. п.) также используйте разные пароли.

Не используйте одну учетную запись в организации совместно с кем-либо, включая помощников или секретарей.

Также запрещается:

– говорить кому-либо пароль по телефону;

– писать пароль в почтовом сообщении;

– давать пароль начальнику;

– обсуждать пароль с коллегами;

– намекать на формат пароля (например, «моя фамилия»);

– не писать пароль при опросах;

– не использовать один пароль всеми членами семьи;

– не давать пароль коллегам на время своего отсутствия на работе.

Если кто-либо просит ваш пароль, ссылайтесь на этот документ или просите позвонить в департамент ИБ.

Не используйте опцию приложений «Запомнить пароль» (например, в Microsoft Outlook или Netscape Messenger).

Не храните записанным на бумаге пароль в офисе или на компьютере в незашифрованном файле.

Меняйте пароль не реже раза в полгода (системные пароли нужно менять ежеквартально). Рекомендуемый срок смены паролей – каждые четыре месяца.

Если есть подозрения, что пароль или учетная запись были взломаны, сообщите об инциденте соответствующему уполномоченному лицу и замените все пароли.

Периодически пробуйте взломать или подобрать пароль. Если это удается с применением соответствующих средств, потребуйте от пользователя сменить пароль.

Стандарты для разработки приложений. Разработчики приложений должны создавать программы, имеющие следующие свойства:

– аутентификация отдельных пользователей, а не групп;

– хранение паролей не должно осуществляться в открытом виде или в любой легко читаемой форме;

– управление ролями, исключающее ситуацию, когда один пользователь может получить функции другого без знания его пароля;

– поддержка TACACS+ , RADIUS и/или X.509 с LDAP, где это возможно.

Использование паролей и парольных фраз для удаленного доступа пользователей. Доступ к интранету организации посредством удаленного доступа должен контролироваться на основе одноразовых паролей или ключевой системы со стойкими парольными фразами.

Парольные фразы обычно используются для аутентификации с открытым/личным ключом. Такая система определяет математическое отношение между известным всем открытым ключом и личным ключом, известным только пользователю.

Без парольной фразы, открывающей личный ключ, пользователь не может получить доступ.

Парольные фразы – это не то же самое, что пароли. Парольная фраза – это более длинная и поэтому более защищенная версия пароля. Обычно она состоит из нескольких слов. Кроме того, такая фраза более защищена от атак по словарю.

Правильно составленная парольная фраза достаточно длинная и содержит комбинации символов, цифр и знаков препинания на верхнем и нижнем регистрах. Например, «The*?#>* @ TrafficOn- Thel01Was*&#!# ThisMorning». Все правила выбора паролей применимы и к парольным фразам.

Ответственность. Любой сотрудник, нарушивший политику, может быть привлечен к дисциплинарному наказанию, вплоть до увольнения с работы.

Определение. Учетная запись администратора приложения – любая учетная запись, предназначенная для администрирования приложения (например, администратора базы данных Oracle и т. п.).

3. ПОЛИТИКА ИСПОЛЬЗОВАНИЯ АЛГОРИТМОВ ШИФРОВАНИЯ

Цель политики – определить условия и способы использования алгоритмов шифрования, известных в настоящее время в обществе и доказавших свою эффективную работу. Также данная политика создает условия для гарантированного соблюдения федеральных законов и определяет полномочные органы по распространению и использованию алгоритмов шифрования вне страны, в которой находится организация.

Область действия. Политика применяется ко всем сотрудникам и партнерам организации.

Основные положения. Стандартные алгоритмы шифрования типа DES, Blowfish, RSA, RC5 и IDEA (в России – ГОСТ

2814789) должны использоваться в качестве основы для шифрования. Эти алгоритмы представляют фактический шифр, используемый для одобренного применения. Например, Pretty Good Privacy (PGP) использует комбинацию IDEA и RSA или Диффи – Хеллмана, а Secure Socket Layer (SSL) использует RSA. Для симметричной криптосистемы длина ключа должна быть не менее 56 бит. Для асимметричных криптосистем ключи должны иметь длину, обеспечивающую эквивалентную стойкость. Для организации требования к длине ключа будут пересматриваться ежегодно и обновляться, насколько это позволяют технологии.

Использование собственных алгоритмов шифрования не разрешается ни в каких целях, пока не будет получено заключение квалифицированных экспертов не из числа заинтересованных лиц и одобрено соответствующим полномочным органом страны, где находится организация. Это не должно противоречить экспортным ограничениям на алгоритмы шифрования страны.

Ответственность. Любой сотрудник, нарушивший политику, может быть привлечен к дисциплинарному наказанию, вплоть до увольнения с работы.

Определения. Собственный алгоритм шифрования – алгоритм, который не был обнародован и/или не представлялся на исследование общественности. Разработчиком алгоритма может быть организация, индивидуум или правительство. Симметричная криптосистема – метод шифрования, в котором один ключ используется как для зашифрования, так и расшифрования данных. Асимметричная криптосистема – метод шифрования, в котором используются два различных ключа: один – для зашифрования, другой для расшифрования данных.

4. ПОЛИТИКА АНТИВИРУСНОЙ ЗАЩИТЫ

Цель – определить требования, обеспечивающие эффективное обнаружение и предотвращение вирусов, которые должны выполняться для всех компьютеров, соединенных с интранетом организации.

Область действия. Данная политика применяется для всех компьютеров организации, представляющих собой персональные компьютеры (ПК) или участвующих в совместном использовании файлов. Это включает (но не ограничивается) настольные компьютеры, ноутбуки, серверы file/ftp/tftp/proxy и любые устройства на основе ПК, генерирующие трафик.

Основные положения. Настоящий документ определяет систему защитных мер, предпринимаемых отделом ИТ, направленных на защиту компьютеров, входящих в состав интранета организации, от компьютерных вирусов, троянских программ и прочих деструктив ных программных кодов, а также устанавливает требования к конфигурации комплексной системы антивирусной защиты интранета и мероприятия, обеспечивающие поддержание этой системы в работоспособном состоянии. Антивирусная политика также определяет структуру и компоненты комплексной системы антивирусной защиты интранета, распределение административных ролей по управлению системой антивирусной защиты и соответствующие полномочия администраторов антивирусной защиты.

Все компьютеры организации на основе ПК должны иметь стандартное, поддерживаемое организацией, антивирусное ПО, установленное и проводящее проверку по расписанию с заданным интервалом.

Само ПО и энциклопедия обнаруживаемых вирусов должны поддерживаться в актуальном состоянии.

Зараженные вирусами компьютеры должны отключаться от интранета до уничтожения вирусов.

Системные администраторы являются ответственными за разработку процедур, согласно которым антивирусное ПО работает на постоянной основе и все компьютеры проверяются на отсутствие вирусов.

В соответствии с политикой принятого использования все действия по созданию и/или распространению деструктивных программ в интранете организации (например, вирусов, червей, «троянских коней», почтовых бомб и т. п.) запрещены.

Пользуйтесь следующими рекомендациями для предотвращения заражения вирусами:

Всегда применяйте только стандартное ПО, обновляемое через портал интранет организации. Используйте последнюю версию ПО. Обновляйте ПО по мере выпуска для него новых версий.

Никогда не открывайте файлы или макросы, присоединенные к почтовым сообщениям, пришедшим от неизвестных отправителей. Немедленно уничтожьте эти вложения и очистите корзину почтовых сообщений.

Уничтожайте спам и другую бесполезную почту без ее пересылки по другим адресам в интранете организации в соответствии с принятой политикой допустимого использования электронной почты.

Никогда не загружайте файлы с неизвестных и непроверенных источников.

Избегайте прямого совместного использования дисков с доступом на чтение/запись не особой надобности.

Всегда сканируйте дискеты/диски, не являющиеся вашими собственными, на отсутствие вирусов перед их использованием.

Регулярно делайте резервные копии важной информации и системных настроек и храните данные в защищенном месте.

Если используемое в работе бизнес-приложение конфликтует с антивирусным ПО, завершите его работу; убедитесь, что

компьютер не заражен, запустив антивирус; временно заблокируйте работу антивируса и снова запустите бизнес-приложение. После окончания его работы разблокируйте антивирус. Пока антивирус не работает, не запускайте приложения, которые могут передавать вирусы, например, электронную почту или совместное использование файлов.

Новые вирусы обнаруживаются практически каждый день. Регулярно пересматривайте антивирусную политику и данные рекомендации.

Также определяются структура и состав средств антивирусной защиты, требования к конфигурации этих средств, контроль их функционирования.

Ответственность. Любой сотрудник, нарушивший политику, может быть привлечен к дисциплинарному наказанию, вплоть до увольнения с работы.

Определение. Важная информация – незаменимая и необходимая для деятельности организации информация, ошибочное изменение или подделка которой приносит большой ущерб, а восстановление после уничтожения невозможно либо очень трудоемко и связано с большими затратами.

5. ПОЛИТИКА ОЦЕНКИ РИСКОВ ИБ

Цель – уполномочить соответствующих лиц периодически выполнять оценку рисков ИБ с целью определения уязвимостей и их последующего устранения.

Область действия. Оценка рисков ИБ может проводиться любым уполномоченным лицом в пределах организации или любым внешним уполномоченным лицом, которое подписало соглашение с третьими лицами организации. Оценка рисков ИБ может проводиться для любой ИС и интранет в целом, включая приложения, серверы, подсети, а также любой процесс или про-

цедуру, с помощью которых эта система управляется и/или поддерживается.

Основные положения. За разработку, развитие и реализацию программ устранения обнаруженных уязвимостей несут совместную ответственность уполномоченные лица и отдел – владелец оцениваемой системы. Ожидается, что сотрудники будут помогать оценке рисков ИБ, проводимой для систем, за которые они ответственны. Также ожидается, что сотрудники будут работать с уполномоченной группой оценки рисков ИБ по развитию плана устранения уязвимостей.

Процесс оценки рисков ИБ. Дается описание процесса или приводится ссылка на источник информации, содержащий такое описание.

Ответственность. Любой сотрудник, нарушивший политику, может быть привлечен к дисциплинарному наказанию, вплоть до увольнения с работы.

Определение. Уполномоченное лицо – любой сотрудник, отдел, группа лиц или третье лицо внутри или вне организации, ответственное за поддержание активов организации.

6. ПОЛИТИКА АУДИТА ИБ

Цель – создать основу для проведения аудита ИБ любой системы или интранета организации уполномоченными лицами.

Цели проведения аудита ИБ:

– обеспечить целостность, конфиденциальность и доступность информации и ресурсов систем и интранета;

– обнаружить возможные проблемы с ОИБ и несоответствия ПолИБ организации;

– провести при необходимости мониторинг активности пользователей или систем.

Область действия. Данная политика распространяется на все компьютеры и средства связи, которыми владеет или пользуется организация, а также на те, которые размещаются на ее территории, но не являются ее собственностью или не используются ею.

Основные положения. Настоящая политика определяет:

– нормативную базу для деятельности внутренних и внешних аудиторов ИБ;

– полномочия внешних и внутренних аудиторов ИБ;

– ответственность аудиторов за ОИБ и нормальный режим функционирования ИС и интранета организации;

– порядок и условия проведения аудита ИБ и анализа рисков ИБ.

При запросе или с целью проведения планового аудита ИБ всем уполномоченным лицам должен быть предоставлен в организации требуемый доступ. Он может включать:

– пользовательский и/или системный доступ к любому средству связи;

– доступ к информации (электронной, бумажной и т. п.), которая порождается, передается или хранится на оборудовании организации или на ее территории;

– доступ в рабочие помещения (лаборатории, офисы, хранилища и т. п.);

– доступ для интерактивного мониторинга и контроля трафика в интранете организации.

Ответственность. Любой сотрудник, нарушивший политику, может быть привлечен к дисциплинарному наказанию, вплоть до увольнения с работы.

7. ПОЛИТИКА ДЛЯ ПОГРАНИЧНЫХ МАРШРУТИЗАТОРОВ ИНТРАНЕТА

Цель – определить минимальные требования по защищенному конфигурированию всех пограничных маршрутизаторов и коммутаторов, соединенных с интранетом или используемых в производственных целях самой организацией или от ее имени.

Область действия. Политика распространяется на все пограничные маршрутизаторы и коммутаторы, соединенные с интранетом организации. На маршрутизаторы и коммутаторы внутри интранета политика не распространяется. Для маршрутизаторов и коммутаторов внутри демилитаризованной зоны (ДМЗ) применяется политика для оборудования ДМЗ.

Основные положения. Конфигурация каждого маршрутизатора должна соответствовать общепринятым стандартам.

На маршрутизаторе не должно быть сконфигурировано никаких локальных учетных записей. Для аутентификации всех пользователей должен использоваться протокол TACACS+ или RADIUS (в зависимости от требуемого функционала).

Пароль на вход в привилегированный режим маршрутизатора должен храниться в зашифрованном виде. В качестве пароля привилегированный режим маршрутизатора должен использовать текущий пароль, выданный организацией, осуществляющей поддержку маршрутизатора. Запретить следующее:

– направленный широковещательный IP-трафик (IP-directed broadcasts);

– входящие на маршрутизатор пакеты, направленные с ложных адресов, например, перечисленных в RFC1918; TCP и UDP small services;

– все типы маршрутизации от источника;

– все веб-сервисы, запущенные на маршрутизаторе.

Использовать стандартные для организации «SNMP community strings». Правила доступа должны добавляться по мере необходимости.

Маршрутизатор должен быть включен в корпоративную систему управления с заранее определенным контактным лицом.

На каждом маршрутизаторе должна присутствовать надпись:

«Несанкционированный доступ к данному сетевому оборудованию запрещен. На доступ и конфигурирование устройства необходимо соответствующее разрешение. Все действия, выполняемые на этом устройстве, регистрируются. Нарушение данной политики повлечет за собой дисциплинарные взыскания или даже преследования в соответствии с законом. Никто не имеет права на сохранность информации, вводимой в сеансе удаленного доступа к данному устройству».

Ответственность. Любой сотрудник, нарушивший политику, может быть привлечен к дисциплинарному наказанию, вплоть до увольнения с работы.

8. ПОЛИТИКА УДАЛЕННОГО ДОСТУПА К ИНТРАНЕТУ

Цель – определить стандарты подключения к интранету организации любого хоста. Они предназначены для минимизации потенциального ущерба организации от угроз ИБ, которые может создать несанкционированное использование ресурсов организации. Это включает угрозы потери конфиденциальности данных, интеллектуальной собственности, имиджу, важным внутренним системам организации и т. п.

Область действия. Политика применяется ко всем сотрудникам, контрактным рабочим, поставщикам и агентам, имеющим собственные или предоставленные организацией компьютеры или рабочие станции, подключенные к интранету организации. Политика применяется к удаленным соединениям, исполь-

зуемым для выполнения работы по заказу организации, включая чтение и отправку электронной почты, и просмотр веб-ресурсов интранета.

Основные положения. Сотрудники, контрактные рабочие, поставщики и агенты организации, имеющие привилегии удаленного доступа (УД) к ее интранету, должны гарантировать, что их удаленное подключение является локальным соединением пользователя с организацией.

Доступ с персональных компьютеров к Интернету в личных целях всеми членами семьи через интранет организации запрещен для сотрудников, платящих за наем жилья. Они несут ответственность за то, чтобы члены их семьи не нарушали политики организации, не предпринимали никаких противоправных действий и не использовали доступ ни в каких других целях, кроме рабочих. Также они несут полную ответственность за всю последовательность действий, повлекшую злоупотребление доступом.

Применяются все политики, регламентирующие защиту информации при доступе к интранету посредством удаленных подключений (например, политика шифрования, политика построения ВЧС, политика беспроводного доступа), а также политика допустимого использования компьютеров интранета организации.

Требования. Защищенный УД должен тщательно контролироваться. Контроль осуществляется посредством аутентификации на основе одноразовых паролей или открытых/личных ключей со стойкими парольными фразами (см. политику использования паролей).

Сотрудник организации не должен сообщать свой идентификатор и почтовый пароль никогда и никому, даже членам семьи.

Сотрудники и контрактные рабочие организации, имеющие привилегированный УД, должны гарантировать, что имеющиеся

у них собственные или предоставленные им организацией компьютер / рабочая станция, удаленно подключенные к интранету организации, в то же время не соединены ни с какой другой сетью, за исключением персональных сетей, находящихся под полным контролем пользователя.

Для выполнения своей работы в интересах организации сотрудники и контрактные рабочие, имеющие привилегированный УД, не должны использовать почтовые ящики, не принадлежащие организации (например, Hotmail, Yahoo, AOL), или другие внешние ресурсы, тем самым гарантируя, что личный бизнес нс смешивается с официальной работой.

Маршрутизаторы для выделенных каналов связи (например, ISDN), сконфигурированные для доступа к интранету организации, должны соответствовать минимальным требованиям аутентификации принятого протокола (например, CHAP).

Никогда не разрешается реконфигурация домашнего оборудования пользователя с целью его одновременного подключения к множественным каналам связи, включая виртуальные.

На конфигурирование нестандартного АО для УД требуется разрешение соответствующих служб организации, которые должны утвердить защищенные настройки для доступа к этому обеспечению.

Все хосты, включая ПК, соединенные с внешними по отношению к интранету организации сетями с применением технологий УД, должны использовать самое современное антивирусное ПО. Подключения третьих лиц должны соответствовать требованиям, зафиксированным в подписанном с ними соглашении.

Личное оборудование, используемое для подключения к интранету организации, должно соответствовать требованиям для оборудования УД, принадлежащего организации.

Организации или частные лица, которые хотят использовать нестандартные решения для УД к интранету организации, должны получить особое разрешение от соответствующих служб организации.

Ответственность. Любой сотрудник, нарушивший политику, может быть привлечен к дисциплинарному наказанию, вплоть до увольнения с работы.

Определения. Хост – устройство, имеющее уникальный адрес. Под УД к интранету организации понимаются все виды доступа, осуществляемые по внешним каналам связи (через контролируемые сети или устройства) и с использованием устройств доступа, расположенных за пределами охраняемой зоны и не контролируемых организацией. Основными видами УД являются:

– доступ к интранету по коммутируемым каналам связи с использованием модемов и телефонной сети, который предоставляется сотрудникам организации, находящимся в отпуске, в командировке или в деловых поездках, а также представителям партнеров, проводящим работы в интранете/экстранете организации;

– доступ мобильных пользователей к интранету с использованием VPN-каналов связи типа «компьютер – сеть» через Интернет, предоставляемый сотрудникам организации, находящимся в отпуске, в командировке или в деловых поездках, а также представителям партнеров, проводящим работы в интранете/экстранете организации;

– подключения удаленных подразделений организации к интранету с использованием VPN-каналов типа «сеть – сеть» через Интернет. Реализации УД, рассматриваемые в данной политике, включают (но не ограничиваются): подключения на основе Frame Relay/ISDN/X.25, подключения через сервер УД (по про-

токолам SLIP, PPP); доступ по протоколу Telnet из Интернета; доступ по телефонной линии на основе обычного модема (например, на основе DSL); доступ посредством кабельного модема; прямое подключение (например, на основе SSH), подключение к ВЧС и т. п.

CHAP (Challenge Handshake Authentication Protocol) – основанный на однонаправленной хеш-функции протокол, используемый для аутентификации.

9. ПОЛИТИКА ПОСТРОЕНИЯ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

Цель – определить руководящие принципы для VPN-соединений с интранетом организации с применением УД на основе протоколов IP Sec или L2TP.

Область действия. Политика применяется ко всем сотрудникам, временным рабочим, консультантам, внештатным сотрудникам и другим работникам организации, включая всех третьих лиц, использующих VPN-доступ к интранету организации. Данная политика распространяется на те реализации VPN, в которых используются концентраторы IP Sec.

Основные положения. Имеющие на это разрешение сотрудники и третьи лица организации (например, клиенты, поставщики и т. п.) могут пользоваться VPN-доступом, который считается сервисом, управляемым пользователем. Это означает, что сам пользователь отвечает за выбор сервис-провайдера Интернета (Internet Service Provider, ISP), руководит настройкой, устанавливает требуемое ПО и платит арендную плату (детали изложены в политике УД). Дополнительно к этому:

– сотрудник, имеющий разрешение на VPN-доступ, должен гарантировать, что неуполномоченные пользователи не получают доступа к интранету организации;

– использование VPN контролируется либо на основе аутентификации с одноразовыми паролями (типа токенов), либо системами с открытым/личным ключом со стойкими парольными фразами;

– при активном подключении к интранету VPN направляют весь трафик от и к ПК по VPN-туннелю; весь остальной трафик отбрасывается;

– одновременное соединение с несколькими VPN не разрешается;

– VPN-шлюзы устанавливаются и управляются соответствующей рабочей группой организации;

– на всех компьютерах, включая ПК, соединенных с интранетом организации посредством VPN или любой другой технологии, должно быть установлено стандартное для организации современное антивирусное ПО;

– пользователь VPN будет автоматически отключаться от интранета организации после 30 мин неактивности; после этого пользователь должен снова войти в систему для восстановления подключения; пингование (pings) или другие искусственные сетевые процессы не должны использоваться для поддержания соединения в открытом состоянии;

– время работы VPN-концентратора ограничивается 24 ч соединения; пользователи компьютеров, не являющихся оборудованием организации, должны сконфигурировать их таким образом, чтобы они соответствовали политикам организации для ВЧС и интранета;

– можно использовать только разрешенные организацией VPN-клиенты;

– при использовании VPN-технологии на персональном оборудовании пользователи должны осознавать, что их компьютеры являются фактически расширением интранета организации и по-

этому они подчиняются тем же правилам и положениям, которые применяются к собственному оборудованию организации.

Ответственность. Любой сотрудник, нарушивший политику, может быть привлечен к дисциплинарному наказанию, вплоть до увольнения с работы.

Определения. Концентратор IPSec – устройство, в котором заканчиваются виртуальные каналы.

10. ПОЛИТИКА ДЛЯ ЭКСТРАНЕТА

Цель – определить политику соединения с интранетом организации третьих лиц для осуществления бизнеса в интересах организации.

Область действия. Политика регламентирует соединения между третьими лицами, которые требуют доступа к непредназначенным для широкого доступа ресурсам организации, независимо от того, какой вид соединений применяется – телекоммуникационный (типа Frame Relay или ISDN) или VPN-технология. Политика не распространяется на третьих лиц типа сервис-провайдеров Интернета (ISP), обеспечивающих доступ организации к Интернету или к телефонным сетям общего пользования (Public Switched Telephone Network).

Основные положения

Предварительные условия. Рассмотрение запросов для экстранет-подключения. Все запросы на новые соединения с экстранетом должны быть тщательно рассмотрены департаментом ИБ, о чем выдается соответствующее заключение. Это гарантирует то, что они не противоречат требованиям бизнеса и при этом соблюдается принцип минимального доступа.

Соглашение о соединении с третьими лицами. Все запросы на подключение между третьими лицами и организацией требуют, чтобы представители третьих лиц и организации были упол-

номочены и готовы подписать соответствующее соглашение. Это соглашение должно быть подписано как минимум заместителем руководителя спонсорского подразделения и уполномоченным представителем третьих лиц. Подписанный документ должен храниться в группе поддержки экстранета и в том подразделении, к чьим ресурсам подключаются третьи лица.

Вступление в действие. Все подключения к экстранету для ведения бизнеса должны сопровождаться соответствующим обоснованием в письменном виде, утвержденным руководителем проекта в группе поддержки экстранета. Подключения к конкретным ресурсам организации должны быть одобрены владельцами этих ресурсов и их администраторами ИБ.

Контактные лица. Спонсорское подразделение должно выделить сотрудника, который будет являться контактным лицом по всем вопросам экстранет-подключения. Это лицо действует от имени спонсорского подразделения и несет ответственность за все пункты, имеющие отношение к политике и соглашению. В случае смены контактного лица требуется немедленно известить об этом группу поддержки экстранета.

Установление соединения. Спонсорское подразделение внутри организации, в интересах которого устанавливается подключение к третьим лицам, обращается с запросом к соответствующей группе поддержки экстранета. Эта группа привлекает департамент ИБ для рассмотрения вопросов, связанных с ИБ в проекте. Если запрашиваемое подключение заканчивается в спонсорском подразделении, последнее должно привлечь своего администратора ИБ. Спонсорское подразделение должно представить департаменту ИБ и группе поддержки экстранета для рассмотрения полную и исчерпывающую информацию о виде запрашиваемого доступа.

В соответствии с утвержденными бизнес-требованиями и заключением об ИБ все устанавливаемые подключения должны

удовлетворять принципу минимального доступа. Ни при каких обстоятельствах организация не может положиться на третьих лиц в отношении защиты своих ресурсов и интранета.

Модификация или изменения соединения и доступа. Все изменения доступа должны сопровождаться соответствующим обоснованием и являться предметом рассмотрения для выдачи заключения об ИБ. Изменения осуществляются в соответствии с утвержденным организацией процессом управления изменениями. Спонсорское подразделение несет ответственность за уведомление группы управления экстранетом и/или департамента ИБ об изменении первоначально представленной информации, что позволит своевременно сохранить защищенность и само подключение.

Прекращение доступа. Когда доступ больше не требуется, спонсорское подразделение внутри организации должно уведомить группу поддержки экстранета, осуществляющую подключение. Она ликвидирует подключение. Это может означать либо модификацию существующих разрешений, либо полное прекращение доступа. Группа поддержки экстранета и спонсорское подразделение должны ежегодно проводить аудит ИБ своих экстранет-подключений, что гарантирует актуальность существующих соединений и соответствие им предоставляемого доступа. Обнаруженные ненужные или давно не используемые для бизнеса организации соединения должны быть немедленно отключены. О таких случаях и о случаях нарушения ИБ департамент ИБ или группа поддержки экстранета должны информировать контактное лицо или спонсорское подразделение с целью принятия ими соответствующих мер.

Ответственность. Любой сотрудник, нарушивший политику, может быть привлечен к дисциплинарному наказанию, вплоть до увольнения с работы.

Определения. Третьи лица – люди или организации, не являющиеся официальными или вспомогательными частями организации.

Спонсорское подразделение – подразделение внутри организации, представившее запрос на экстранет-подключение третьих лиц.

11. ПОЛИТИКА ДЛЯ ОБОРУДОВАНИЯ ПОГРАНИЧНОЙ ДЕМИЛИТАРИЗОВАННОЙ ЗОНЫ

Цель – определить стандарты, которым должно отвечать все собственное и/или используемое организацией оборудование, находящееся за пределами МЭ, отделяющего внутренний интранет организации от внешних по отношению к нему сетей. Эти стандарты предназначены для снижения потенциального ущерба организации от потери важной или конфиденциальной информации, интеллектуальной собственности или ее имиджа, что может явиться следствием несанкционированного использования ресурсов организации.

Объект политики – оборудование, установленное на границе с другими сетями за МЭ организации, как часть пограничной демилитаризованной зоны (ДМЗ). Это оборудование (сетевое и хосты) является потенциально уязвимым к атакам, исходящим из внешних сетей (типа Интернета).

Политика определяет следующие стандарты:

– ответственность владельцев;

– требования защищенного конфигурирования;

– требования к работе;

– требования к изменению управления.

Область действия. Все оборудование или устройства, расположенные в ДМЗ, являющиеся собственностью или используемые организацией (включая хосты, маршрутизаторы, коммутаторы

и т. п.) и/или зарегистрированные в принадлежащем ей домене (Domain Name System, DNS), должны соответствовать данной политике. Эта политика также распространяется на любой хост, которым управляет или владеет внешний сервис-провайдер или третье лицо, если это оборудование находится в домене организации или будет принадлежать ей. Все новое оборудование, которое подпадает под действие данной политики, должно быть сконфигурировано в соответствии с ее требованиями. Все существующее и позднее закупленное оборудование, размещаемое в недоверенных сетях организации, должно также соответствовать данной политике.

Основные положения

Владение и ответственность. Оборудование и приложения, являющиеся объектами данной политики, должны администрироваться группой поддержки, утвержденной департаментом ИБ для управления ДМЗ, приложениями и/или сетями.

Оборудование должно быть зарегистрировано в корпоративной системе управления. Для этого как минимум требуется следующая информация:

– местонахождение хоста и контактное лицо;

– аппаратная платформа и ОС с версией;

– основные функции и приложения;

– парольные группы с привилегированными правами.

Сетевые интерфейсы должны иметь соответствующие записи на DNS-сервере (минимально A и PTR-записи).

Парольные группы должны поддерживаться в соответствии с корпоративной системой / процессами управления паролями.

Всем членам департамента ИБ по требованию (см. политику аудита ИБ) должен предоставляться немедленный доступ к оборудованию и системным журналам.

Об изменениях в текущем оборудовании и появлении нового оборудования требуется немедленно уведомить соответствую-

щих лиц с целью изменения корпоративных процессов / процедур управления.

Для проверки соблюдения данной политики департамент ИБ будет периодически проводить аудит оборудования ДМЗ (см. политику аудита ИБ).

Общая политика конфигурирования. Все оборудование должно соответствовать следующей конфигурационной политике: АО, ОС, сервисы и приложения (должны быть одобрены департаментом ИБ на этапе предварительного анализа).

Настройки ОС должны соответствовать стандартам инсталляции и конфигурирования для защищенных хостов и маршрутизаторов (ссылка на стандарт).

Вес обновления, рекомендуемые производителями или департаментом ИБ, должны быть установлены. Это относится ко всем инсталлированным сервисам, даже если они временно или постоянно отключены. Административная группа должна проверять это.

Сервисы и приложения, не удовлетворяющие требованиям бизнеса, должны быть отключены.

Доверительные отношения между системами должны использоваться только по требованиям бизнеса, быть задокументированы и одобрены департаментом ИБ.

Сервисы и приложения не для общего доступа должны быть внесены в соответствующие контрольные списки.

Незащищенные сервисы или протоколы (по определению департамента ИБ) должны быть заменены на более защищенные аналоги, если таковые существуют.

Удаленное администрирование должно осуществляться по защищенным каналам (например, шифрованным сетевым соединениям, использующим протоколы SSH или IPSec) или через консольный доступ, независимый от ДМЗ. Если средства защи-

ты каналов не применимы, для всех уровней доступа должны использоваться одноразовые пароли.

Все обновления контента (содержимого) хостов должны осуществляться по защищенным каналам.

Все имеющие отношение к ИБ события должны регистрироваться и сохраняться в утвержденных департаментом ИБ журналах для последующего аудита ИБ. Эти события включают (но не ограничиваются) следующее:

– попытку неудачного входа пользователя;

– отказ в получении привилегированного доступа;

– нарушения политики доступа.

Департамент ИБ рассматривает запросы на отказ в предоставлении доступа в порядке поступления и удовлетворяет их, если на то есть основания.

Установка нового оборудования и изменение процедур управления. Все новые установки и изменения конфигурации существующего оборудования и приложений должны соответствовать следующим процедурам/политике:

– все новые установки должны осуществляться по разработанной процедуре размещения оборудования в ДМЗ;

– изменения конфигурации должны соответствовать процедурам корпоративного управления изменениями;

– для осуществления аудита ИБ систем/приложений, заменяемых новыми сервисами, должен приглашаться департамент ИБ;

– в одобрении размещения нового оборудования и изменения каких-либо конфигураций департамент ИБ должен участвовать непосредственно или через систему управления изменениями.

Оборудование, управляемое внешними сервис-провайдерами. Ответственность за защиту оборудования, устанавливаемого внешними сервис-провайдерами, должна быть оговорена в кон-

тракте с ними и контактными лицами, отвечающими за ИБ. Подписавшие контракт со стороны организации несут ответственность за следование политике третьих лиц.

Ответственность. Любой сотрудник, нарушивший политику, может быть привлечен к дисциплинарному наказанию, вплоть до увольнения с работы. Внешние сервис-провайдеры, уличенные в несоблюдении данной политики, будут обязаны выплатить штрафы, вплоть до прерывания действия контракта.

Определения. ДМЗ – любая недоверенная сеть, соединенная с интранетом организации, но отделенная от нее МЭ, используемая для внешнего (Интернет/экстранет и т. п.) доступа из организации или представляющая информацию внешним пользователям.

Недоверенная сеть – любая сеть, отделенная от интранета МЭ с целью избежать повреждения ресурсов от незаконного сетевого трафика, НСД (сети партеров, Интернет и т. п.) или чего-то еще, идентифицируемого как потенциальная угроза ИБ для таких ресурсов.

12. ПОЛИТИКА ПОДКЛЮЧЕНИЯ ПОДРАЗДЕЛЕНИЙ К ИНТРАНЕТУ

Цель – определить требования ИБ для подразделений организации, гарантирующие, что конфиденциальная информация и технологии не будут скомпрометированы и что сервисы и интересы организации будут защищены от работы подразделений.

Применение. Политика распространяется на все связанные внутри организации подразделения, служащих организации и третьих лиц, имеющих доступ к ее подразделениям. Все существующее оборудование и то, которое будет установлено в будущем, к которому применима данная политика, должно быть сконфигурировано в соответствии с ней. ДМЗ подчиняется отдельной политике.

Основные положения

Владение и ответственность. Организация назначает администраторов подразделений, контактных лиц и представителей в администрации организации, с которыми работают эти лица. В случае смены этих лиц руководители подразделений обязаны представлять новую информацию в департамент ИБ и администрации организации. Администраторы подразделений должны быть постоянно на связи для информирования в случае необходимости, в противном случае решается вопрос об их обязанностях.

Администраторы подразделений несут ответственность:

– за защиту своих подразделений и их влияние на интранет или любые другие сети;

– следование данной политике и установленным в соответствии с ней процедурам. Если что-то не определено в политике и процедурах, они должны приложить все усилия для защиты организации от уязвимостей;

– соответствие работы подразделения ПолИБ организации. Особенно важно соблюдать политику использования паролей для сетевых устройств и хостов, политику беспроводного доступа, антивирусную политику и физическую защиту;

– контроль доступа в подразделении. Доступ к подразделению предоставляется его администратором или назначенным должностным лицом тем пользователям, которые имеют такую производственную необходимость, на короткое или длительное время. Это подразумевает постоянный мониторинг списков доступа, что гарантирует своевременную отмену доступа для тех, кому он больше не нужен.

Группа поддержки сети обязана осуществлять управление МСЭ между интранетом организации и сетями подразделений.

Эта группа и/или департамент ИБ оставляют за собой право отключить подключение подразделения в случае его негативного воздействия на интранет или создания угрозы для ее ИБ.

Эта группа должна иметь IP-адреса всех подразделений, входящих в интранет организации, в единой корпоративной базе данных адресов, наряду с текущей контактной информацией подразделения.

Любое подразделение, которому требуется внешнее подключение, должно представить департаменту ИБ схему и документацию с обоснованием причин, спецификацией оборудования и схемой IP-адресации. Департамент ИБ рассмотрит запрос и удовлетворит его, если не нарушаются требования ИБ организации.

Пароли всех пользователей должны соответствовать политике использования паролей организации. В случае если учетная запись на оборудование подразделения уже не требуется, она должна быть уничтожена в срок не позднее трех дней. Групповые пароли для компьютеров подразделения (Unix, Windows и т. п.) должны меняться каждые три месяца. Для любого устройства подразделения при изменении состава группы пароль должен быть изменен в срок не позднее трех дней.

Ни одно подразделение не должно предоставлять эксплуатационных сервисов. Они определяются как ведущие и совместно используемые, критичные для бизнеса сервисы, генерирующие потоки поступлений или обеспечивающие работу клиентов. Они должны находиться в ведении соответствующего департамента.

Департамент ИБ рассматривает запросы на отказ в предоставлении доступа в порядке поступления и удовлетворяет их, если на то есть основания.

Общие конфигурационные требования. Трафик между интранетом и сетями подразделений, а также между сетями отдель-

ных подразделений без необходимости не разрешен, поскольку это может поставить под угрозу их конфиденциальную информацию.

Весь трафик между интранетом и подразделением должен проходить через МЭ, которым управляет группа поддержки интранета. Сетевые устройства подразделения (включая беспроводные) не должны иметь перекрестные ссылки между подразделением и интранетом.

Оригинальные настройки МСЭ и любые изменения в них должны быть предварительно проанализированы и одобрены департаментом ИБ, который при необходимости может потребовать пересмотра требований ИБ.

Департамент ИБ оставляет за собой право в любое время проводить аудит ИБ всей информации и административных процедур подразделения, включая (но не ограничиваясь) входящие и исходящие пакеты, МЭ и сетевую периферию.

Подразделениям запрещается проводить сканирование портов, изучение сети, «наводнение» трафика и другие подобные действия, которые негативно влияют на интранет организации и другие сети. Такие действия должны быть запрещены.

Принадлежащие подразделению шлюзы должны соответствовать рекомендациям организации и должны удостоверяться корпоративными серверами аутентификации.

Пароль на вход в привилегированный режим для всех шлюзов подразделения должен отличаться от паролей для другого оборудования подразделения. Этот пароль должен соответствовать политике использования паролей организации. Он дается только тем, кто уполномочен администрировать сеть подразделения.

В подразделениях, где неперсонал организации имеет физический доступ (например, в учебных классах), запрещается пря-

мое подключение к интранету организации. Кроме этого, в таких подразделениях ни на каких компьютерах не должна находиться конфиденциальная информация организации. Подключение уполномоченного персонала к интранету из таких подразделений обязательно должно использовать аутентификацию через корпоративный сервер аутентификации, временные списки доступа, SSH, VPN-клиенты или подобные технологии, одобренные департаментом ИБ.

Инфраструктурные устройства (типа IP-телефонов), которым требуется подключение к интранету, должны соответствовать политике для закрытых территорий.

Все запросы на внешние подключения подразделений должны быть рассмотрены и одобрены департаментом ИБ. Аналоговые и ISDN каналы связи должны быть сконфигурированы только на доступ к доверенным номерам. Для аутентификации должны использоваться стойкие пароли.

Все сети подразделений с внешними подключениями не должны соединяться с интранетом организации или любой другой внутренней сетью непосредственно, через беспроводной канал или на основе любого другого вида компьютерного оборудования.

Ответственность. Любой сотрудник, нарушивший политику, может быть привлечен к дисциплинарному наказанию, вплоть до увольнения с работы.

Определения. Внутреннее подразделение – подразделение внутри организации. Группа поддержки сети отвечает за те части интранета организации, которые не принадлежат ни одному подразделению.

Подразделение – непроизводственное отделение организации, занимающееся разработкой, демонстрацией, обучением и/или тестированием продуктов. Внешние подключения (извест-

ные как ДМЗ) включают (но не ограничиваются) сетевые подключения третьих лиц, аналоговые и ISDN каналы связи и любые другие телекоммуникационные (Т1/Е1, Т3/Е3, ОС3, ОС 12, DSL и т. п.) каналы передачи данных. Шлюзы подразделения составляют его собственность и соединяют сеть подразделения с остальным интранетом организации (весь трафик должен проходить через эти шлюзы).

МЭ – устройство, контролирующее доступ между сетями.

ДМЗ – сеть, расположенная за основными корпоративными МЭ, но также находящаяся под административным контролем организации.

13. ПОЛИТИКА ПОДКЛЮЧЕНИЯ К ИНТРАНЕТУ С ПРИМЕНЕНИЕМ МОДЕМА

Цель – защитить информацию организации в электронном виде от непреднамеренной компрометации персоналом, имеющим разрешение на использование модемных подключений.

Область действия. Политика регламентирует разрешенный модемный доступ и его использование авторизированными пользователями организации.

Основные положения. Сотрудники организации и уполномоченные третьи лица (клиенты, поставщики и т. п.) могут использовать модемные подключения для получения доступа к ее интранету. Модемные подключения должны жестко контролироваться с применением аутентификации на основе одноразовых паролей. Запрос на модемное подключение должен осуществляться в соответствии с разработанной для этого процедурой.

Сотрудник, имеющий разрешение на модемное подключение, должен гарантировать, что это подключение не используется людьми, не являющимися сотрудниками организации, с целью получения доступа к ресурсам ее ИС и интранета. Сотруд-

ник должен постоянно помнить, что такое подключение является фактическим расширением интранета организации и поэтому открывает возможный путь к ее конфиденциальной информации. Он и/или третьи лица должны принять все возможные меры по защите ресурсов организации.

Учетные записи, соответствующие модемным подключениям, подлежат аудиту ИБ. Если в течение шести месяцев учетная запись не использовалась, то она удаляется.

Аналоговые мобильные телефоны и телефоны не GSM-стандарта не могут использоваться в этих целях, так как их сигнал может быть легко несанкционированно прослушан или перехвачен. Только телефоны GSM-стандарта рассматриваются как достаточно защищенные для подключения к интранету организации.

Беспроводной доступ к интранету организации регламентируется политикой беспроводного доступа.

Ответственность. Любой сотрудник, нарушивший политику, может быть привлечен к дисциплинарному наказанию, вплоть до увольнения с работы.

14. ПОЛИТИКА РАБОТЫ С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ

Цель – определить, какая информация может представляться несотрудникам организации, а какая не должна выходить за пределы организации без соответствующего на то разрешения. Информация, подпадающая под действие данной политики, включает (но не ограничивается) информацию, хранимую или совместно используемую с применением различных средств. Это – информация в электронном виде, бумажная информация и информация, совместно используемая устно или визуально (например, через телефон или видеоконференцсвязь) на стадиях

обработки, передачи и хранения, защищаемая от модификации или раскрытия.

Все сотрудники должны быть ознакомлены с перечнем информации, регламентируемым данной политикой. Отнесение специфической информации к определенному классу дается администратором ИБ подразделения или организации. Все вопросы, относящиеся к руководству, решает департамент ИБ организации. Сотрудники должны следовать здравому смыслу при защите конфиденциальной информации организации.

Влияние руководства на осуществление ежедневных обязанностей служащих должно быть минимальным.

Область действия. Вся информация организации подразделяется на открытую и конфиденциальную. Открытая информация – это информация, доступ к которой не связан ни с какими потерями.

Конфиденциальная информация – это информация, доступ посторонних к которой для части сотрудников или посторонних лиц нежелателен, так как может вызвать материальные и моральные потери.

Далее приводятся примеры: общая корпоративная информация, промышленные секреты, программы развития, персональные данные служащих, телефонные справочники, информация о третьих лицах и т. п. Категорирование информации по конфиденциальности выполняется субъективно руководством или персоналом в соответствии с выделенными ему полномочиями в зависимости от риска ее разглашения.

Основные положения. Руководство организации детально описывает, как защитить различную конфиденциальную информацию. Оно будет различным для разных организаций, так как отнесение одной и той же информации к тому или иному классу (например, минимальной, средней и максимальной конфиден-

циальности) зависит от многих обстоятельств: от бизнеса организации, условий осуществления бизнеса, ее размера и многого другого.

1. Информацией минимальной конфиденциальности является общая корпоративная информация, некоторая техническая информация и отдельные данные о персонале. Доступ имеют сотрудники организации, контрактные работники, те, кто должен знать эту информацию в соответствии с потребностями бизнеса. Метод распространения в организации – стандартная внутренняя внутриофисная переписка, одобренная электронная почта и методы передачи электронных файлов. Методы распространения за пределами организации – официальные почтовые службы страны или других стран, одобренная электронная почта и методы передачи электронных файлов. Распространение в электронном виде – ограничений нет при условии посылки разрешенным получателям. Хранение – беречь от неуполномоченных людей, защищать от потери, контролировать доступ. Уничтожение – по разработанной процедуре уничтожения бумажных и электронных носителей информации с невозможностью восстановления. Наказания – согласно административному, гражданскому или уголовному праву.

2. Информация средней конфиденциальности – это финансовая и техническая информация, информация о бизнесе и бо´льшая часть персональных данных. Доступ – сотрудники организации и несотрудники, подписавшие соглашение о неразглашении информации, которым она требуется для бизнеса. Метод распространения в организации – стандартная внутренняя внутриофисная переписка, одобренная электронная почта и методы передачи электронных файлов. Методы распространения за пределами организации – официальные курьерские и почтовые службы страны или других стран. Распространение в электронном виде –

ограничений нет при условии посылки разрешенным получателям внутри организации, вне организации обязательно в зашифрованном виде. Хранение – с индивидуальным контролем доступа. Уничтожение – по разработанной процедуре уничтожения бумажных и электронных носителей информации с невозможностью восстановления. Наказания – согласно административному, гражданскому или уголовному праву.

3. Информация максимальной конфиденциальности – это промышленные секреты, маркетинговая, финансовая и техническая информация, информация о функционировании, исходные коды и часть персональных данных. Доступ – только сотрудники организации, имеющие разрешенный доступ и подписавшие соглашение о неразглашении информации. Метод распространения в организации – непосредственная доставка в руки, доставка в конверте со штампом конфиденциальности, одобренные методы передачи электронных файлов. Методы распространения за пределами организации – разрешенная курьерская служба с подписью о вручении. Распространение в электронном виде – ограничений нет при условии посылки разрешенным получателям внутри организации, вне организации обязательно в зашифрованном виде. Хранение – с индивидуальным контролем доступа, с обеспечением физической защиты (включая хранение на компьютере). Уничтожение – по разработанной процедуре уничтожения бумажных и электронных носителей информации с невозможностью восстановления. Наказания – согласно административному, гражданскому или уголовному праву.

Данная политика также должна определять:

– кто может иметь доступ к конфиденциальной информации вообще и при особых обстоятельствах;

– в каких системах может храниться и обрабатываться конфиденциальная информация;

– информация какой степени секретности может быть распечатана на физически незащищенных принтерах;

– как конфиденциальная информация удаляется из систем и запоминающих устройств (например, размагничивание носителей данных, чистка жестких дисков, резка бумажных копий);

– любые установки по умолчанию для файлов и каталогов, определяемые в системных файлах конфигурации, и т. п.

Ответственность. Любой сотрудник, нарушивший политику, может быть привлечен к дисциплинарному наказанию, вплоть до увольнения с работы.

Определение. Определены методы передачи электронных файлов на основе FTP-клиентов и веб-браузеров.

15. ПОЛИТИКА ДЛЯ ВЕБ-СЕРВЕРА

Цель – определить стандарты базовой конфигурации оборудования внутреннего веб-сервера, находящегося во владении и/или используемого организацией. Эффективная реализация данной политики уменьшит НСД к составляющим собственность организации информации и технологиям.

Область действия. Политика распространяется на серверное оборудование, находящееся во владении и/или используемое организацией, и веб-серверы, зарегистрированные в любом внутреннем сетевом домене организации. Политика применяется только к оборудованию интранета организации. Защищенное конфигурирование внешнего оборудования из ДМЗ организации регламентируется политикой для оборудования ДМЗ.

Основные положения

Владение и ответственность. Все размещенные в организации внутренние веб-серверы находятся в собственности рабочей группы, осуществляющей их системное администрирование. Должны существовать и использоваться каждой рабочей группой

руководства по настройке веб-серверов, основанные на потребностях бизнеса и утвержденные соответствующими службами организации. Рабочие группы должны осуществлять мониторинг соответствия конфигурации и предпринимать предписанные действия при выявлении отклонений. Каждая рабочая группа должна определить процесс изменения руководств по настройке, который должен быть рассмотрен и утвержден в установленном порядке.

Веб-сервер должен быть зарегистрирован в корпоративной системе управления. Для определения обратной связи, как минимум, необходима следующая информация:

– местонахождение веб-сервера и контактное лицо для обратной связи;

– аппаратная платформа и ОС с версией;

– основные функции и приложения, если таковые используются. Информация в корпоративной системе управления должна быть актуальной.

За изменениями конфигурации веб-серверов должны быть внесены соответствующие изменения в процедуры управления.

Общее руководство по конфигурированию:

Настойки ОС должны соответствовать утвержденным руководствам. Сервисы и приложения, которые не используются, нужно отключить. Доступ к сервисам должен регистрироваться и/или защищаться методами контроля доступа (типа TCPWrappers), если это возможно.

Самые последние обновления, устраняющие уязвимости системы, должны устанавливаться сразу же после их появления, за исключением тех случаев, когда это помешает выполнению неотложных работ.

Доверительные отношения между системами являются угрозой ИБ, поэтому лучше избегать их использования. Лучше применять другой, более надежный метод связи.

Всегда используйте стандартные принципы ОИБ, требующие наименьшего доступа для выполнения функций.

Когда для работы достаточно привилегий обычного пользователя, не используйте административную учетную запись root.

Если технически доступно и выполнимо защищенное канальное подключение, то привилегированный доступ должен осуществляться на его основе (например, зашифрованное сетевое соединение с использованием протоколов SSH или IPSec).

Веб-вервер должен физически располагаться в среде с контролируемым доступом.

Работа с веб-сервером из неконтролируемого закрытого помещения запрещается.

Мониторинг. Все относящиеся к ИБ события в важных или конфиденциальных системах должны регистрироваться, и в журналах регистрации должна сохраняться следующая информация:

– все записи событий должны сохраняться как минимум неделю;

– ежедневные резервные копии измененной информации должны храниться не меньше месяца;

– еженедельные полные резервные копии журналов событий должны храниться не меньше месяца;

– ежемесячные полные резервные копии должны храниться не меньше двух лет.

Обо всех относящихся к ИБ событиях следует уведомлять соответствующие службы, которым нужно представить для рассмотрения журналы событий и сообщения об инцидентах ИБ в установленной форме. При необходимости они помогут определить корректирующие меры.

Относящиеся к ИБ события включают (но не ограничиваются):

– сканирование портов;

– НСД к привилегированным учетным записям;

– аномальные признаки, не относящиеся к работе приложений хоста, являющегося веб-сервером.

Соглашения. Аудит ИБ веб-сервера должен выполняться регулярно уполномоченными лицами внутри организации.

В соответствии с политикой аудитом ИБ руководит внутренняя группа или уполномоченная внешняя организация. Они отбирают обнаруженные события и при необходимости посылают соответствующие отчеты в правоохранительные органы.

Должно быть сделано все возможное, чтобы аудит ИБ не вызвал сбоев в работе или потерю ресурсов.

Ответственность. Любой сотрудник, нарушивший политику, может быть привлечен к дисциплинарному наказанию, вплоть до увольнения с работы.

Определения. В рамках данной политики веб-сервер – внутренний веб-сервер организации.

Демилитаризованная зона (ДМЗ) – сетевой сегмент, внешний по отношению к интранету организации.

16. ПОЛИТИКА ОТПРАВКИ ЭЛЕКТРОННОЙ ПОЧТЫ ЗА ПРЕДЕЛЫ ИНТРАНЕТА

Цель – предотвратить несанкционированное или случайное раскрытие конфиденциальной информации организации.

Область действия. Политика распространяется на автоматическую отправку электронной почты за пределы интранета организации и связанную с этим случайную передачу конфиденциальной информации сотрудниками, поставщиками и агентами, работающими от имени организации.

Основные положения. Сотрудники должны проявлять особую бдительность при отправке электронной почты из интранета организации во внешнюю сеть. Электронная почта организации не будет автоматически посылаться внешнему получателю,

за исключением той, которая одобрена администратором ИБ подразделения сотрудника. Конфиденциальная информация, как это определено в политике работы с конфиденциальной информацией, в открытом виде не отправляется никакими средствами, поскольку она носит критический для бизнеса характер и должна быть зашифрована в соответствии с политикой шифрования.

Ответственность. Любой сотрудник, нарушивший политику, может быть привлечен к дисциплинарному наказанию, вплоть до увольнения с работы.

Определения. Электронная почта – это электронная передача информации на основе почтового протокола (типа SMTP).

Пересылаемая почта – электронная почта, пересылаемая из интранета к внешнему получателю.

Информация считается конфиденциальной, если она может нанести ущерб финансового характера, репутации или позиции на рынке самой организации или ее клиентам.

Случайное раскрытие – намеренное или ненамеренное открытие запрещенной информации людям, которым не нужно знать эту информацию.

17. ПОЛИТИКА ХРАНЕНИЯ СООБЩЕНИЙ ЭЛЕКТРОННОЙ ПОЧТЫ

Цель – определить, какую отправленную и полученную электронную почту хранить и как долго. Распространяется на информацию, хранимую или совместно используемую посредством электронной почты или других применяемых в настоящее время технологий передачи сообщений. Отнесение информации к классам определяет руководитель подразделения. Вопросы по данному руководству направляются департаменту ИБ.

Применение. Политика распространяется на четыре основных класса почтовой корреспонденции (переписки): админи-

стративную (срок хранения – четыре года), финансовую (четыре года), общую (один год) и однодневную (после прочтения уничтожить).

Основные положения. Административная корреспонденция включает, например, сообщения о политике компании, выходных, поведении, защите интеллектуальной собственности и многое другое, сообщения с пометкой «Только для администрации». Для хранения такой корреспонденции ее копии нужно отправлять в почтовый ящик admin@Домен_организации, администрированием которого занимается департамент ИТ.

Финансовая корреспонденция – это вся информация, относящаяся к доходам и расходам организации. Для ее хранения копии сообщений нужно отправлять на адрес fiscal@Домен_организации, администрированием которого занимается департамент ИТ.

Общая корреспонденция – информация, относящаяся к взаимодействию с клиентами и выполнению бизнес-функций отдельными сотрудниками организации. Они несут ответственность за ее сохранение.

Однодневная корреспонденция – бóльшая часть электронной почты, включающая персональные почтовые сообщения, запросы на получение рекомендаций, разработку продуктов и т. п.

Сообщения текущего почтового клиента могут сохраняться с использованием стандартных встроенных процедур или копироваться в файл и в таком виде храниться. Сообщения клиента административного или финансового характера должны копироваться в электронное сообщение и пересылаться в соответствующий адрес для хранения.

Защищенные средства связи организации должны применяться в случаях, предусмотренных в политике работы с конфиденциальной информацией. В остальных случаях информация должна храниться в незашифрованном виде.

Резервирование работы почтового сервера. Организация создает резервные копии данных с почтового сервера, и раз в квартал соответствующий носитель изымается из ротации и хранится отдельно. Никто не может уничтожать электронную почту с этого носителя.

Ответственность. Любой сотрудник, нарушивший политику, может быть привлечен к дисциплинарному наказанию, вплоть до увольнения с работы.

Определение. Текущий почтовый клиент – разрешенный к использованию в организации клиент для работы с электронной почтой.

18. ПОЛИТИКА ДЛЯ МЕЖСЕТЕВЫХ ЭКРАНОВ

Политика для МЭ описывает, как управляется АО и ПО такого специального средства защиты, как МЭ, и какие при этом изменения в интранете требуются и допустимы (например, в операционной системе того компьютера, получившего название «бастион», где будет установлен МЭ). Эта политика должна определять:

– кто может получить привилегированный доступ к МЭ;

– кому разрешено получать информацию о конфигурации и списках доступа к МЭ;

– процедуры написания запроса на изменение конфигурации МЭ и удовлетворения этого запроса;

– сроки пересмотра конфигурации МЭ и т. д.

19. ПОЛИТИКА ПОДКЛЮЧЕНИЯ НОВЫХ УСТРОЙСТВ К ИНТРАНЕТУ

Политика подключения новых сетевых устройств к интранету организации определяет требования и порядок добавления в интранет новых аппаратных средств. Эта политика особенно

важна для оборудования, которое будет располагаться до средств защиты интранета, например, на стыке интранета с любой другой открытой сетью до МЭ. Также она нужна для того АО, доступ к которому будет открыт сразу для нескольких групп пользователей. Такая политика должна определять, например:

– кто может устанавливать новые ресурсы в интранете;

– какие при этом обоснования и уведомления должны быть выполнены;

– как документируются в интранете любые изменения;

– каковы требования по защите при подключении новых сетевых устройств;

– как будут защищаться устройства, не имеющие встроенных средств защиты, и т. д.

Учебное издание

Минаев Владимир Александрович,
доктор технических наук, профессор

Поликарпов Евгений Сергеевич,
кандидат технических наук

Еременко Владимир Тарасович,
доктор технических наук, профессор

Рытов Михаил Юрьевич,
кандидат технических наук, доцент

Управление информационной безопасностью

Корректор *Табунова Е. А.*
Компьютерная верстка *Гридчина Т. А.*

Московский университет МВД России имени В.Я. Кикотя
117997, г. Москва, ул. Академика Волгина, д. 12

Подписано в печать 20.12.2022	Формат 60×84 1/16	Тираж 106 экз.
Заказ № 35	Цена договорная	1-й завод 85 экз.
		Объем 11,48 уч.-изд. л.
		18,02 усл. печ. л.