ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 13335-1 — 2006

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Часть 1

Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

ISO/IEC 13335-1 : 2004
Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management
(IDT)

Издание официальное

БЗ 2—2006/12

Москва
Стандартинформ
2007

1—179

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «ЛИНС-М» (ООО «Линс-М») на основе собственного аутентичного перевода стандарта, указанного в пункте 4, а также Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФГУ ГНИИИ ПТЗИ ФСТЭК России)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 10 «Перспективные производственные технологии, менеджмент и оценка рисков»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 19 декабря 2006 г. № 317-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 13335-1:2004. «Информационная технология. Методы обеспечения безопасности. Менеджмент безопасности информационных и телекоммуникационных технологий. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» (ISO/IEC 13335-1 : 2004 «Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management»).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2004 (пункт 3.5)

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок – в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомления и тексты размещаются также в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

© Стандартинформ, 2007

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения . . . 1
2 Термины и определения . . . 1
3 Концепции безопасности и взаимосвязи . . . 3
3.1 Принципы безопасности . . . 3
3.2 Активы . . . 3
3.3 Угрозы . . . 3
3.4 Уязвимости . . . 4
3.5 Воздействие . . . 5
3.6 Риск . . . 5
3.7 Защитные меры . . . 5
3.8 Ограничения . . . 6
3.9 Взаимосвязь компонентов безопасности . . . 6
4 Цели, стратегии и политика . . . 8
4.1 Цели и стратегии безопасности информационно-телекоммуникационных технологий . . . 9
4.2 Иерархия политик . . . 10
4.3 Элементы политики безопасности информационно-телекоммуникационных технологий организации . . . 10
5 Организационные аспекты безопасности информационно-телекоммуникационных технологий . . . 12
5.1 Служебные обязанности и ответственность . . . 12
5.2 Организационные принципы . . . 15
6 Функции управления безопасностью информационно-телекоммуникационными технологиями . . . 17
6.1 Общие вопросы . . . 17
6.2 Внешние условия . . . 17
6.3 Управление рисками . . . 17

к ГОСТ Р ИСО/МЭК 13335-1—2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

В каком месте	Напечатано	Должно быть
Первая страница стандарта	Дата введения — **2007—08—01**	Дата введения — **2007—06—01**

(ИУС № 7 2007 г.)

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Часть 1
Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

Information technology. Security techniques. Part 1. Concepts and models for information and communications technology security management

Дата введения — 2007—08—01

1 Область применения

Настоящий стандарт представляет собой руководство по управлению безопасностью информационных и телекоммуникационных технологий (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.

Целью настоящего стандарта является формирование общих понятий и моделей управления безопасностью ИТТ. Приведенные в нем положения носят общий характер и применимы к различным методам управления и организациям. Настоящий стандарт разработан так, что позволяет приспосабливать его положения к потребностям организации и свойственному ей стилю управления. Настоящий стандарт не разрабатывает конкретных подходов к управлению безопасностью.

2 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 17799, ИСО/МЭК 13335-4, а также следующие термины с соответствующими определениями:

2.1 **подотчетность** (accountability): Свойство, обеспечивающее однозначное прослеживание действий любого логического объекта.

[ИСО/МЭК 7498-2]

2.2 **активы** (asset): Все, что имеет ценность для организации.

2.3 **аутентичность** (authenticity): Свойство, гарантирующее, что субъект или ресурс идентичны заявленным.

Примечание — Аутентичность применяется к таким субъектам, как пользователи, к процессам, системам и информации.

2.4 **доступность** (availability): Свойство объекта находиться в состоянии готовности и используемости по запросу авторизованного логического объекта.

[ИСО/МЭК 7498-2]

2.5 **базовые защитные меры** (baseline controls): Минимальный набор защитных мер, установленный для системы или организации.

2.6 **конфиденциальность** (confidentiality): Свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса.

[ИСО/МЭК 7498-2]

Издание официальное

2—179

2.7 **контроль** (control): —

Примечание — В контексте безопасности информационно-телекоммуникационных технологий термин «контроль» может считаться синонимом «защитной меры» (см. 2.24).

2.8 **рекомендации** (guidelines): Описание, поясняющее действия и способы их выполнения, необходимые для достижения установленных целей.

2.9 **воздействие** (impact): Результат нежелательного инцидента информационной безопасности.

2.10 **инцидент информационной безопасности** (information security incident): Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Примечание — Инцидентами информационной безопасности являются:
- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политик или рекомендаций;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

2.11 **безопасность информационно-телекоммуникационных технологий (безопасность ИТТ)** (ICT security): Все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информационно-телекоммуникационных технологий.

2.12 **политика безопасности информационно-телекоммуникационных технологий (политика безопасности ИТТ)** (ICT security policy): Правила, директивы, сложившаяся практика, которые определяют, как в пределах организации и ее информационно-телекоммуникационных технологий управлять, защищать и распределять активы, в том числе критичную информацию.

2.13 **средство(а) обработки информации** (information processing facility(ies)): Любая система обработки информации, сервис или инфраструктура, или их физические места размещения.

2.14 **информационная безопасность** (information security): Все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки.

2.15 **целостность** (integrity): Свойство сохранения правильности и полноты активов.

2.16 **неотказуемость** (non-repudiation): Способность удостоверять имевшее место действие или событие так, чтобы эти события или действия не могли быть позже отвергнуты.

[ИСО/МЭК 13888-1, ИСО/МЭК 7498-2]

2.17 **достоверность** (reliability): Свойство соответствия предусмотренному поведению и результатам.

2.18 **остаточный риск** (residual risk): Риск, остающийся после его обработки.

2.19 **риск** (risk): Потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимостей актива или группы активов.

Примечание — Определяется как сочетание вероятности события и его последствий.

2.20 **анализ риска** (risk analysis): Систематический процесс определения величины риска.

2.21 **оценка риска** (risk assessment): Процесс, объединяющий идентификацию риска, анализ риска и оценивание риска.

2.22 **менеджмент риска** (risk management): Полный процесс идентификации, контроля, устранения или уменьшения последствий опасных событий, которые могут оказать влияние на ресурсы информационно-телекоммуникационных технологий.

2.23 **обработка риска** (risk treatment): Процесс выбора и осуществления мер по модификации риска.

2.24 **защитная мера** (safeguard): Сложившаяся практика, процедура или механизм обработки риска.

Примечание — Следует заметить, что понятие «защитная мера» может считаться синонимом понятию «контроль» (см. 2.7).

2.25 **угроза** (threat): Потенциальная причина инцидента, который может нанести ущерб системе или организации.

2.26 **уязвимость** (vulnerability): Слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами.

3 Концепции безопасности и взаимосвязи

3.1 Принципы безопасности

Для создания эффективной программы безопасности ИТТ фундаментальными являются следующие высокоуровневые принципы безопасности:

- менеджмент риска — активы должны быть защищены путем принятия соответствующих мер. Защитные меры должны выбираться и применяться на основании соответствующей методологии управления рисками, которая, исходя из активов организации, угроз, уязвимостей и различных воздействий угроз, устанавливает допустимые риски и учитывает существующие ограничения;
- обязательства — важны обязательства организации в области безопасности ИТТ и в управлении рисками. Для формирования обязательств следует разъяснить преимущества от реализации безопасности ИТТ;
- служебные обязанности и ответственность — руководство организации несет ответственность за обеспечение безопасности активов. Служебные обязанности и ответственность, связанные с безопасностью ИТТ, должны быть определены и доведены до сведения персонала;
- цели, стратегии и политика — управление рисками, связанными с безопасностью ИТТ, должно осуществляться с учетом целей, стратегий и политики организации.
- управление жизненным циклом — управление безопасностью ИТТ должно быть непрерывным в течение всего их жизненного цикла.

Ниже с позиций фундаментальных принципов безопасности приведено описание основных компонентов безопасности, вовлеченных в процесс управления безопасностью, и их связи. Приведены характеристики каждого компонента и указаны основные сопряженные с ним факторы.

3.2 Активы

Правильное управление активами является важнейшим фактором успешной деятельности организации и основной обязанностью всех уровней руководства. Активы организации могут рассматриваться как ценности организации, которые должны иметь гарантированную защиту. Активы включают в себя (но не ограничиваются):

- материальные активы (например вычислительные средства, средства связи, здания);
- информацию (данные) (например документы, базы данных);
- программное обеспечение;
- способность производить продукт или предоставлять услугу;
- людей;
- нематериальные ресурсы (например престиж фирмы, репутацию).

Невозможно разработать и поддерживать успешную программу по безопасности, если не идентифицированы активы организации. Во многих случаях процесс идентификации активов и установления их ценности может быть проведен на верхнем уровне и не требует дорогостоящей, детальной и длительной процедуры. Степень детализации данной процедуры должна определяться отношением величины временных и финансовых затрат к ценности активов. Во всех случаях степень детализации должна быть установлена, исходя из целей безопасности.

Характеристики активов, которые необходимо рассмотреть, включают в себя следующие величины: ценность, чувствительность активов, и имеющиеся защитные меры. Наличие конкретных угроз уязвимости влияет на требования к защите активов. Внешние условия, социальная и правовая среда, в которых организация осуществляет свою деятельность, могут влиять на активы, их свойства и характеристики. Особенности в упомянутых условиях могут иметь существенное значение для международных организаций и трансконтинентального использования ИТТ.

Основываясь на определении угроз и уязвимостей и их комбинации, можно оценить риск и выбрать защитные меры и, тем самым, повысить безопасность активов. Далее необходимо оценивать остаточный риск для того, чтобы определить, адекватно ли защищены активы.

3.3 Угрозы

Активы подвержены многим видам угроз. Угроза обладает способностью наносить ущерб активам и, следовательно, организации в целом. Этот ущерб может возникать из-за атаки на информацию, обрабатываемую ИТТ, на саму систему или иные ресурсы, приводя, например, к их неавторизованному разруше-

нию, раскрытию, модификации, порче, недоступности или потере. Ущерб активам может быть нанесен только при наличии у них уязвимости. Угрозы могут быть естественного происхождения или связаны с человеческим фактором. В последнем случае угрозы могут быть случайными или целенаправленными. Примеры угроз приведены в таблице 1. Угрозы, как случайные, так и преднамеренные, должны быть идентифицированы, а их уровень и вероятность возникновения должны быть оценены. По многим видам угроз среды собраны статистические данные. Эти данные могут быть использованы организацией при оценке угроз.

Таблица 1 — Примеры угроз

Угрозы, обусловленные человеческим фактором		Угрозы среды
целенаправленные	случайные	
Подслушивание/перехват. Модификация информации. Атака хакера на систему. Злонамеренный код. Хищение	Ошибки и упущения. Удаление файла. Ошибка маршрутизации. Материальные несчастные случаи	Землетрясение. Молния. Наводнение. Пожар

Угрозы могут быть также направлены на отдельные специфические части организации, например, на разрушение вычислительных средств. Некоторые угрозы могут быть общими для всей организации, например ущерб зданиям от урагана или молнии. Угроза может исходить как изнутри организации, например забастовка сотрудников, так и снаружи, например атаки хакеров или промышленный шпионаж. Размер ущерба от угрозы может варьироваться при каждом ее возникновении. Ущерб, наносимый нежелательным инцидентом, может быть временным или постоянным, как в случае разрушения актива.

Угрозы обладают следующими характеристиками, устанавливающими их взаимосвязь с другими компонентами безопасности:

- источник, внутренний или внешний;
- мотивация, например финансовая выгода, конкурентное преимущество;
- частота возникновения;
- правдоподобие;
- вредоносное воздействие.

Некоторые угрозы могут поражать не один вид актива. В этом случае угрозы могут наносить вред в зависимости от того, какие именно активы повреждены. Например, программный вирус на автономной персональной вычислительной машине может нанести ограниченный или локальный вред. Однако тот же программный вирус может оказать на сетевой сервер обширное воздействие.

Окружающие условия и социальная среда, в которых функционирует организация, могут иметь большое значение и существенно влиять на отношение к угрозам и активам. Некоторые угрозы в организациях могут вообще не рассматриваться. Когда речь идет об угрозах, необходимо учитывать влияние внешней среды.

При оценке уровень угрозы в зависимости от результата ее воздействия может быть определен как высокий, средний или низкий.

3.4 Уязвимости

Слабость актива или нескольких видов активов, которые могут быть использованы одной или более угрозами, трактуется как уязвимость. Связанные с активами уязвимости включают в себя слабости физического носителя, организации, процедур, персонала, управления, администрирования, аппаратного/программного обеспечения или информации. Угрозы могут использовать уязвимости для нанесения ущерба ИТТ или целям бизнеса. Уязвимость может существовать и в отсутствие угрозы. Уязвимость сама по себе не причиняет ущерб, но это является только условием или набором условий, позволяющим угрозе воздействовать на активы. Следует рассматривать уязвимости, возникающие из различных источников, например внутренних и внешних по отношению к конкретному активу. Уязвимость может сохраняться, пока сам актив не изменится так, чтобы уязвимость уже не смогла проявиться. Уязвимость необходимо оценивать индивидуально и в совокупности, чтобы рассмотреть сложившуюся ситуацию в целом.

Примером уязвимости является отсутствие контроля доступа, которое может обусловить возникновение угрозы несанкционированного доступа и привести к утрате активов.

В конкретных системе или организации не все уязвимости соответствуют угрозам. В первую очередь следует сосредоточиться на уязвимостях, которым соответствуют угрозы. Но в силу того, что окружающая среда может непредсказуемо меняться, необходимо вести мониторинг всех уязвимостей для того, чтобы вовремя выявлять те из них, которые могут использовать вновь появляющиеся угрозы.

Оценка уязвимостей — это проверка слабостей, которые могут быть использованы существующими угрозами. Эта оценка должна учитывать окружающую среду и существующие защитные меры. Мерой уязвимости конкретной системы или актива по отношению к угрозе является степень того, с какой легкостью системе или активу может быть нанесен ущерб.

При оценке уровень уязвимости может быть определен как высокий, средний или низкий.

3.5 Воздействие

Воздействие — это результат инцидента информационной безопасности, вызванного угрозой и нанесшего ущерб ее активу. Результатом воздействия могут стать разрушение конкретного актива, повреждение ИТТ, нарушение их конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности. Непрямое воздействие может включать в себя финансовые потери, потерю доли рынка или репутации. Контроль за воздействием позволяет достичь равновесия между предполагаемыми последствиями инцидента и стоимостью защитных мер. Следует учитывать вероятность возникновения инцидента. Это особенно важно в тех случаях, когда ущерб при каждом возникновении инцидента невелик, но суммарный эффект накопившихся со временем инцидентов может быть существенным. Оценка воздействия является важным элементом оценки риска и выбора защитных мер.

Количественное и качественное измерение воздействия могут быть проведены:

- определением финансовых потерь;
- использованием эмпирической шкалы серьезности воздействия, например от 1 до 10;
- использованием заранее оговоренных уровней (высокий, средний и низкий).

3.6 Риск

Риск — это способность конкретной угрозы использовать уязвимости одного или нескольких видов активов для нанесения ущерба организации. Одна угроза или группа угроз могут использовать одну уязвимость или группу уязвимостей.

Сценарий риска описывает, как определенная угроза или группа угроз могут использовать уязвимость или группу уязвимостей подверженного угрозе актива. Риск характеризуется комбинацией двух факторов: вероятностью возникновения инцидента и его разрушительным воздействием. Любое изменение активов, угроз, уязвимостей или защитных мер может оказать значительное влияние на риск. Раннее обнаружение или знание обо всех этих изменениях увеличивает возможности по принятию необходимых мер для обработки риска. Обработка риска включает в себя устранение, снижение, перенос и принятие риска.

Следует учитывать, что риск никогда не устраняется полностью. Принятие остаточного риска является частью заключения о соответствии уровня безопасности потребностям организации. Руководство организации должно быть поставлено в известность обо всех остаточных рисках, их опасных последствиях и вероятности возникновения инцидентов. Решение о принятии риска должно приниматься специалистами, имеющими право принимать решение о допустимости опасных последствий при возникновении инцидента и применении дополнительных мер защиты в случае, если уровень остаточного риска неприемлем.

3.7 Защитные меры

Защитные меры — это действия, процедуры и механизмы, способные обеспечить безопасность от возникновения угрозы, уменьшить уязвимость, ограничить воздействие инцидента в системе безопасности, обнаружить инциденты и облегчить восстановление активов. Эффективная безопасность обычно требует комбинации различных защитных мер для обеспечения заданных уровней безопасности при защите активов. Например, механизмы контроля доступа, применяемые к вычислительным средствам, должны подкрепляться аудитом, определенным порядком действий персонала, его обучением, а также физической защитой. Часть защитных мер может быть обеспечена внешними условиями, свойствами актива или может уже существовать в системе или организации.

Порядок выбора защитных мер очень важен для правильного планирования и реализации программы информационной безопасности. Защитная мера может выполнять много функций безопасности и, наоборот, одна функция безопасности может потребовать нескольких защитных мер. Защитные меры могут выполнять одну или несколько из следующих функций:

- предотвращение;
- сдерживание;
- обнаружение;

- ограничение;
- исправление;
- восстановление;
- мониторинг;
- осведомление.

Пример — Области, в которых могут использоваться защитные меры, включают в себя:
- физическую среду;
- техническую среду (аппаратно-программное обеспечение и средства связи);
- персонал;
- администрирование.

Некоторые защитные меры могут характеризовать позицию организации в области информационной безопасности. В связи с этим важно выбирать специфические защитные меры, не причиняющие ущерба культурной и социальной среде, в которой функционирует организация.

Пример — Такими специфическими защитными мерами являются:
- политики и процедуры;
- механизмы контроля доступа;
- антивирусное программное обеспечение;
- шифрование;
- цифровая подпись;
- инструменты мониторинга и анализа;
- резервный источник питания;
- резервные копии информации.

3.8 Ограничения

Обычно ограничения устанавливает или признает руководство организации, а также определяет среда, в которой действует организация.

Пример — Такие ограничения могут включать в себя:
- организационные;
- коммерческие;
- финансовые;
- по окружающей среде;
- по персоналу;
- временные;
- правовые;
- технические;
- культурные/социальные.

Ограничения, присущие организации, должны учитываться при выборе и реализации защитных мер. Необходимо периодически пересматривать существующие и учитывать новые ограничения. Следует отметить, что ограничения могут со временем изменяться в зависимости от положения организации и изменения внешней среды. Внешняя среда, в которой действует организация, имеет отношение к нескольким компонентам безопасности, в частности к угрозам, рискам и защитным мерам.

3.9 Взаимосвязь компонентов безопасности

Безопасность ИТТ — это многоплановая организация процессов защиты, которую можно рассматривать с различных точек зрения. Взаимосвязь компонентов безопасности, показывающая, как активы могут подвергаться воздействию нескольких угроз, одна из которых является основой для модели, представлена на рисунке 1. Набор угроз постоянно меняется и, как правило, известен только частично. Также со временем меняется и окружающая среда, и эти изменения способны повлиять на природу угроз и вероятность их возникновения.

Модель безопасности отображает:

- окружающую среду, содержащую ограничения и угрозы, которые постоянно меняются и известны лишь частично;
- активы организации;
- уязвимости, присущие данным активам;
- меры для защиты активов;
- приемлемые для организации остаточные риски.

На основе анализа взаимосвязи компонентов безопасности, представленной на рисунке 1, модель безопасности может быть представлена пятью возможными сценариями. Эти сценарии включают в себя:

- сценарий 1 — защитная мера *S* может быть эффективна для снижения рисков *R*, связанных с угрозой *T*, способной использовать уязвимость актива *V*. Угроза может достичь цели, только если активы уязвимы для данной угрозы;

- сценарий 2 — защитная мера может быть эффективной для снижения риска, связанного с угрозой, использующей группу уязвимостей актива;

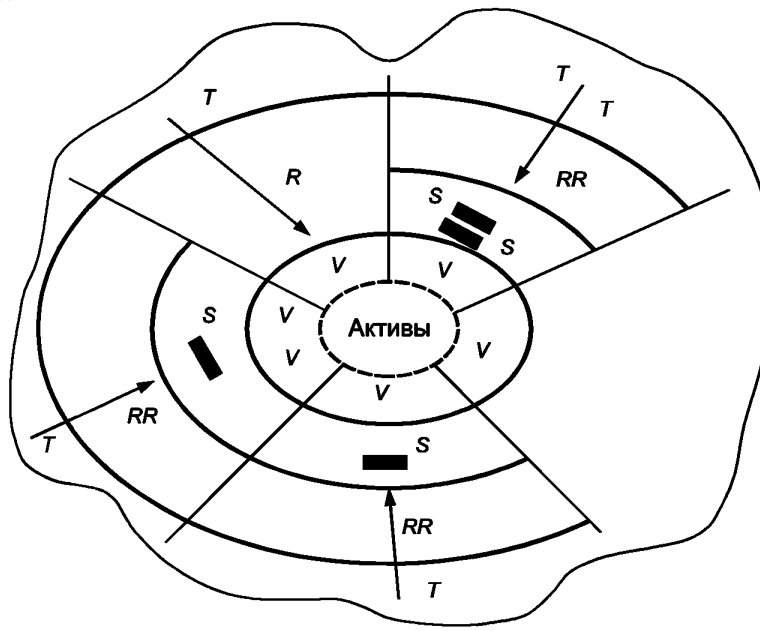
- сценарий 3 — группа защитных мер может быть эффективна в снижении рисков, связанных с группой угроз, использующих уязвимость актива. Иногда требуется несколько защитных мер для снижения риска до приемлемого уровня для получения допустимого остаточного риска *RR*;

- сценарий 4 — риск считают приемлемым и никакие меры не реализуются даже в присутствии угроз и при наличии уязвимостей актива;

- сценарий 5 — существует уязвимость актива, но не известны угрозы, которые могли бы ее использовать.

В качестве защитной меры может быть использован мониторинг угроз для того, чтобы убедиться, что угрозы, способные использовать уязвимость актива, не появились. Ограничения влияют на выбор защитных мер.

Ограничения



R — риск; *RR* — остаточный риск; *S* — защитная мера; *T* — угроза; *V* — уязвимость актива

Рисунок 1 — Взаимосвязь компонентов безопасности

Любая ИТТ включает в себя активы (в первую очередь информацию, а также технические средства, программное обеспечение, связь и т. д.), важные для успешной деятельности организации. Эти активы представляют для организации ценность, которая обычно определяется по их влиянию на бизнес-операции неавторизованного раскрытия информации, ее модификации или отказа от авторства, а также недоступностью или разрушением информации или услуг. Для того, чтобы точнее оценить реальное значение воздействия, вначале его определяют вне зависимости от угроз, которые могут его вызвать. Затем отвечают на вопрос о том, какие угрозы могут возникнуть и вызвать подобное воздействие, какова вероятность их появления и могут ли активы подвергаться нескольким угрозам. Далее изучают вопрос о том, какие уязвимости активов могут быть использованы угрозами для того, чтобы вызвать воздействие, т. е. могут ли угрозы использовать уязвимости, чтобы воздействовать на активы. Каждый из этих компонентов (ценности активов, угрозы и уязвимости) может создать риск. От оценки риска далее зависят общие требования безопасности, которые выполняются или достигаются реализацией защитных мер. В дальнейшем применение защитных мер снизит риск, защитит от воздействия угроз и уменьшит уязвимость активов.

Взаимосвязь защитных мер и риска, показывающая эффективность некоторых защитных мер в снижении риска, представлена на рисунке 2. Часто требуется применение нескольких защитных мер для

снижения риска до приемлемого уровня. Если риск считается приемлемым, то реализация защитных мер не требуется.

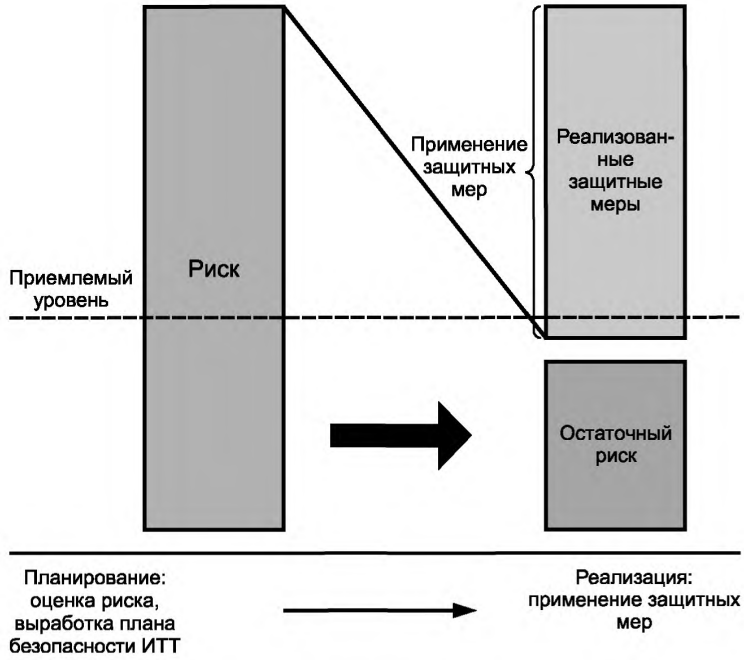


Рисунок 2 — Взаимосвязь защитных мер и риска

4 Цели, стратегии и политика

В качестве основы действенной безопасности ИТТ организации должны быть сформулированы цели, стратегии и политика безопасности организации. Они содействуют деятельности организации и обеспечивают согласованность всех защитных мер. Для того, чтобы обеспечить подобную согласованность, особенно важно, чтобы цели, стратегия и политика безопасности были интегрированы в программы обучения и повышения квалификации в области безопасности.

Цели (чего необходимо достичь), стратегии (способы достижения цели), политика (правила, которые следует соблюдать при реализации стратегий) и процедуры (методы осуществления политики) могут быть определены и раскрыты в соответствующих подразделениях и на соответствующих уровнях организации. Руководящие документы должны отражать организационные требования и учитывать организационные ограничения. Поскольку многие угрозы (например атаки хакеров, удаление файлов, пожар) являются распространенными, важна согласованность между соответствующими документами.

Более того, общие цели, стратегии и политика должны быть отражены и уточнены в детальных и специфических целях, политике и процедурах во всех сферах интереса организации, таких как управление финансами, персоналом и безопасностью. Далее безопасность подразделяют на составляющие (связанную с персоналом, физическую, информационную, ИТТ безопасность и т. д.). Иерархия документации должна поддерживаться и актуализироваться по результатам периодического анализа безопасности (например по результатам оценки рисков, внешнего и внутреннего аудита безопасности) и в связи с изменениями целей деятельности организации.

Цели, стратегии, политика и методы безопасности ИТТ должны отображать то, что ожидается от ИТТ в сфере безопасности. Как правило, их излагают на общепринятом языке, однако в некоторых случаях может возникнуть и потребность изложить их более формально с использованием специфической терминологии. Цели, стратегия, политика определяют уровень безопасности для организации и порог приемлемого риска.

4.1 Цели и стратегии безопасности информационно-телекоммуникационных технологий

После установления целей безопасности ИТТ организации должны быть разработаны стратегии безопасности ИТТ, являющиеся фундаментом развития политики безопасности ИТТ организации. Развитие безопасности ИТТ необходимо для того, чтобы гарантировать достоверность и эффективность результатов процесса управления рисками. Для развития и успешной реализации политики безопасности ИТТ в организации требуется обеспечить ее всестороннее управление. Важно, чтобы политика безопасности ИТТ учитывала цели и особенности данной организации. Политика безопасности ИТТ должна объединяться с политикой безопасности и бизнес-политикой организации. Такое объединение поможет достичь наиболее эффективного использования ресурсов и обеспечить согласованный подход к безопасности в различных условиях окружающей среды.

Может оказаться необходимым развивать отдельные специфические аспекты политики безопасности для каждой или нескольких ИТТ. Эти направления должны базироваться на оценке риска и согласовываться с политикой безопасности ИТТ, тем самым учитывая рекомендации по безопасности для тех систем, с которыми они связаны.

В качестве первого шага к процессу управления безопасностью ИТТ можно рассмотреть вопрос о том, насколько широки границы уровня риска, приемлемого для организации. Тщательное определение приемлемых рисков и, следовательно, соответствующего уровня безопасности — это ключ к успешному управлению безопасностью.

Необходимость задания широких границ допустимого риска безопасности диктуется задачами безопасности ИТТ, которые должна выполнить организация. Для решения задач обеспечения безопасности нужно идентифицировать активы организации и провести оценку их ценности. При идентификации и оценке ценности активов необходимо учитывать роль, которую они играют в поддержании деятельности организации. ИТТ является лишь частью активов организации.

Чтобы оценить, в какой мере бизнес организации зависит от ИТТ, необходимо рассмотреть вопросы о том:

- какие важные составляющие бизнеса не могут осуществляться без ИТТ;
- какие задачи могут быть решены только при помощи ИТТ;
- какие важные решения зависят от конфиденциальности, целостности, доступности, неотказуемости, подотчетности и аутентичности информации, хранимой или обрабатываемой ИТТ, или от того, насколько эта информация актуальна;
- какая хранимая или обрабатываемая информация должна защищаться;
- каковы для организации последствия инцидента безопасности?

Ответы на эти вопросы позволят установить задачи безопасности ИТТ организации. Если, например, некоторые важные или очень важные составляющие деятельности организации зависят от точности или актуальности информации, то одной из задач безопасности организации может стать обеспечение целостности и обновляемости информации в процессе ее хранения и обработки ИТТ. Определяя задачи безопасности ИТТ, необходимо также рассмотреть задачи бизнеса и их связь с безопасностью.

В зависимости от целей безопасности ИТТ необходимо согласовать стратегию достижения этих целей. Выбранная стратегия должна соответствовать ценности защищаемых активов. Если, например, ответ на один или более вопросов, рассмотренных выше, выявляет сильную зависимость от ИТТ, то организация, скорее всего, должна предъявлять высокие требования к безопасности ИТТ, и целесообразно выбирать стратегию, достаточную для выполнения этих требований.

Основные положения стратегии безопасности ИТТ сводятся к тому, как организация будет достигать своих целей в области безопасности ИТТ. Вопросы, к которым должна обращаться стратегия, будут зависеть от числа, вида и важности этих целей. Для организации обычно важно применять типовые решения этих вопросов. Характер вопросов может быть как очень конкретным, так и общим.

Примеры

1 Конкретный вопрос: организация (в силу специфики своей деятельности) может иметь первоочередной целью безопасности ИТТ обеспечение постоянной доступности всех своих систем. В этом случае одна из составляющих стратегии может быть направлена на уменьшение вероятности заражения вирусами путем установки антивирусного программного обеспечения.

2 Общий вопрос: организация, осуществляющая продажу своих информационно-телекоммуникационных услуг, может поставить целью безопасности ИТТ доказать потенциальным клиентам, что ее собственные системы организации защищены. В этом случае частью стратегии будет аттестация системы по требованиям безопасности информации, проведенная уполномоченной сторонней организацией.

Другими возможными аспектами стратегии безопасности ИТТ, в силу специфических задач или их комбинаций, могут быть:

- стратегия оценки риска и методы, адаптируемые в рамках организации;
- комплексная политика безопасности ИТТ для каждой системы;
- организационные методы безопасности для каждой системы;
- схема классификации ИТТ систем;
- осознание необходимости безопасности и повышение квалификации в области безопасности;
- условия безопасности соединений, которые должны выполняться и проверяться перед осуществлением соединения с другими устройствами;
- стандартные схемы управления инцидентами информационной безопасности в рамках всей организации.

После определения стратегия безопасности и ее составляющие должны быть включены в политику безопасности ИТТ организации.

4.2 Иерархия политик

Политика безопасности организации может состоять из принципов безопасности и директив для организации в целом. Политика безопасности организации должна отражать более широкий круг аспектов политики организации, включая аспекты, которые касаются прав личности, законодательных требований и стандартов.

Политика информационной безопасности может содержать принципы и директивы, специфичные для защиты чувствительной и ценной или иной важной для организации информации. Содержащиеся в ней принципы строятся на основе принципов политики безопасности и, таким образом, согласованы с ними.

Политика безопасности ИТТ организации должна отражать существенные принципы безопасности ИТТ и директивы, применимые к политике безопасности и политике информационной безопасности, и порядок использования ИТТ в организации.

Политика безопасности ИТТ должна отражать принципы безопасности и директивы, содержащиеся в политике безопасности ИТТ организации. Она должна также содержать детали особых требований безопасности и защитных мер, подлежащих реализации, и процедуры правильного использования защитных мер для обеспечения адекватной безопасности. Во всех случаях важно, чтобы принятый подход был эффективен в отношении потребностей бизнеса организации.

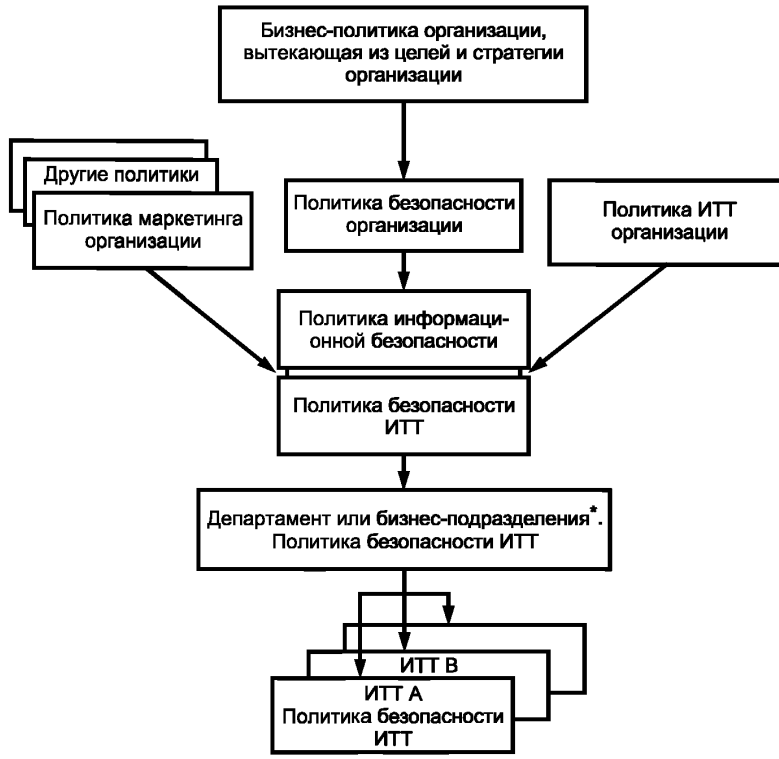
В некоторых случаях политика безопасности ИТТ может быть включена в состав технической и управленческой политики организации, которые вместе составляют основу политики ИТТ. Эта политика должна содержать несколько убедительных положений важности безопасности, если она необходима для соблюдения данной политики. Пример иерархических отношений, которые могут возникать между политиками, показан на рисунке 3. Вне зависимости от организационной структуры или документации, принятой в организации, важно, чтобы учитывались различные стороны политики и поддерживалась их согласованность.

Другие более детальные политики безопасности требуются для специфических систем и услуг или групп ИТТ и услуг. Эти политики обычно известны как политики безопасности ИТТ. С позиций управления очень важно, чтобы их предмет и границы были ясны и базировались одновременно на бизнес-требованиях и технических требованиях.

4.3 Элементы политики безопасности информационно-телекоммуникационных технологий организации

Политика безопасности ИТТ должна формироваться, исходя из согласованных целей и стратегий безопасности ИТТ организации. Необходимо выработать и сохранять политику безопасности ИТТ, соответствующую законодательству, требованиям регулирующих органов, политике в области бизнеса, безопасности и политике ИТТ.

Чем более организация полагается на ИТТ, тем важнее ее безопасность, которая обеспечивает выполнение бизнес-задач. При формировании политики безопасности ИТТ следует помнить об особенностях культуры, окружающей среды организации, поскольку они влияют на подход к безопасности, например на защитные меры, которые могут быть легко приняты в одной среде и быть абсолютно неприемлемы в другой. Деятельность в области безопасности, изложенная в политике безопасности ИТТ, может основываться на организационных целях и стратегиях, результатах предыдущих исследований по оценке и управлению риском, результатах мероприятий по сопровождению создаваемых защитных мер, мониторинге, аудите и анализе безопасности ИТТ в процессе текущей деятельности и отчетах об инцидентах безопасности. Любая серьезная угроза или уязвимость, замеченная в ходе данных мероприятий, должна быть соотнесена с



* Глубина иерархии (число слов) зависит от нескольких факторов (например размера организации).

Рисунок 3 — Иерархия политик

политикой организации, описывающей общий подход к решению этих проблем безопасности. Детальные действия излагаются в различных политиках безопасности ИТТ или других вспомогательных документах, например в организационных методах безопасности.

В разработке политики безопасности ИТТ организации должны принимать участие представители направлений, связанных с:

- аудитом;
- правом;
- финансами;
- информационными системами (специалисты и пользователи);
- коммунальными службами/инфраструктурой (лица, отвечающие за здания, размещение, электроснабжение и кондиционирование);
- персоналом;
- безопасностью;
- руководством.

В соответствии с целями безопасности и стратегией, принятой организацией для достижения этих целей, определяется надлежащий уровень детализации политики безопасности ИТТ организации. Политика безопасности ИТТ должна распространяться на:

- предмет и задачи безопасности;
- цели безопасности с учетом правовых и регулирующих обязательств, а также с учетом бизнес-целей;
- требования безопасности ИТТ к обеспечению конфиденциальности, целостности, доступности, безотказности, подотчетности и аутентичности информации и средств ее обработки;
- ссылки на стандарты, лежащие в основе данной политики;

- администрирование информационной безопасности, охватывающее организационные и индивидуальные ответственности и полномочия;
- подход к управлению риском, принятый в организации;
- метод определения приоритетов реализации защитных мер;
- уровень безопасности и остаточный риск, определяемый руководством организации;
- общие правила контроля доступа (логический контроль доступа, а также контроль физического доступа в здания, помещения, к системам и информации);
- подходы к осведомленности о безопасности и повышение квалификации в области безопасности в рамках организации;
- процедуры проверки и поддержания безопасности;
- общие вопросы защиты персонала;
- способы, которыми политика безопасности будет доведена до сведения всех заинтересованных лиц;
- условия анализа или аудита политики безопасности;
- метод контроля изменений в политике безопасности.

Организации должны оценить свои требования, окружающую среду и уровень развития и определить наиболее отвечающую им специфическую проблему безопасности. Эта проблема включает в себя:

- требования безопасности ИТТ, например требования конфиденциальности, целостности, доступности, неотказуемости, аутентичности и достоверности, особенно с учетом мнений владельцев активов;
- организационную инфраструктуру и распределение обязанностей;
- интеграцию безопасности при совершенствовании системы и закупках;
- определение методов и уровней классификации информации;
- стратегию управления рисками;
- планирование непрерывности бизнеса;
- вопросы, связанные с персоналом (особое внимание должно быть уделено персоналу, занимающему ответственные должности, такому как технический персонал и системные администраторы);
- осведомленность и обучение персонала;
- правовые и регулирующие обязательства;
- менеджмент, осуществляемый независимым экспертом;
- управление инцидентами информационной безопасности.

Как отмечено выше, результаты исследований по оценке риска, проверок соответствия безопасности и инцидентов безопасности могут оказывать влияние на политику безопасности ИТТ организации. Это, в свою очередь, может потребовать пересмотра или совершенствования ранее определенной стратегии или политики безопасности.

Для обеспечения адекватной поддержки всех связанных с безопасностью мер политика безопасности ИТТ должна быть одобрена руководством организации.

На основе политики безопасности ИТТ должны быть подготовлены директивные указания, обязательные для всех руководителей и сотрудников организации. Это может потребовать подписания каждым сотрудником документа, подтверждающего его обязанности в рамках безопасности данной организации. Далее следует развивать и осуществлять программу осведомленности о безопасности, разъясняющую эти обязанности.

Должен быть назначен ответственный за политику безопасности ИТТ, который должен обеспечивать соответствие политики требованиям и актуальному статусу данной организации. Обычно им является сотрудник службы безопасности, который несет ответственность за следующие действия: проверку соответствия безопасности, ревизию, аудит, обработку инцидентов, выявление слабых мест в безопасности и внесение изменений в политику безопасности ИТТ организации, которые могут потребоваться по результатам подобных действий.

5 Организационные аспекты безопасности информационно-телекоммуникационных технологий

5.1 Служебные обязанности и ответственность

5.1.1 Служебные обязанности, подотчетность и ответственность в организации

Эффективная безопасность требует подотчетности, исчерпывающего определения и признания обязанностей в сфере безопасности. Руководство должно отвечать за все аспекты управления безопасно-

тью, включая принятие решений по управлению рисками. Отдельные ее факторы, такие как тип, форма регистрации, размер и структура организации, повлияют на то, на каком уровне будут определены эти обязанности. Безопасность ИТТ — это междисциплинарная тема, относящаяся к каждому проекту ИТТ и ко всем пользователям внутри организации. Надлежащее определение и разграничение подотчетности, специфических служебных обязанностей и ответственности должно обеспечивать эффективное и квалифицированное выполнение всех важных задач. В малых организациях их руководство может исполнять обязанности, связанные с безопасностью, либо другие сотрудники могут выполнять две и более функций безопасности. В подобных случаях для исключения конфликта интересов и обеспечения необходимого разделения служебных обязанностей нужны независимые ревизии.

Хотя эта цель может быть достигнута при помощи различных организационных схем, зависящих от размера и структуры организации, в каждой организации должны присутствовать следующие служебные обязанности:

- совет по безопасности ИТТ, который обычно решает междисциплинарные вопросы, дает консультации и рекомендует стратегии, одобряет политики и процедуры;
- администратор безопасности ИТТ, который связывает воедино все аспекты безопасности внутри организации.

Совет по безопасности и администратор безопасности должны иметь строго определенные и четко сформулированные обязанности и достаточные полномочия для обеспечения выполнения политики безопасности ИТТ. Организация обязана предоставить администратору безопасности четкие механизмы взаимодействия, обязанности и полномочия, а его обязанности должны быть одобрены советом по безопасности ИТТ. Выполнение этих функций может быть дополнено привлечением внешних консультантов.

Пример отношений между администратором безопасности ИТТ, советом по безопасности ИТТ и представителями других структур в рамках организации, таких как пользователи и персонал ИТТ, показан на рисунке 4. Эти отношения могут носить управленческий или функциональный характер. В представленном на рисунке 4 примере организации безопасности ИТТ показаны три организационных уровня. Они в целом вытекают из классической организационной структуры, такой как корпорация/департамент или центр/бизнес-подразделение, но могут быть легко адаптированы применительно к любой организации увеличением или уменьшением числа уровней в соответствии с потребностями организации. Малые или средние организации могут возложить на администратора безопасности ИТТ все обязанности, связанные с безопасностью. Когда обязанности объединяются, важно обеспечить сохранение соответствующего контроля и баланса, чтобы избежать концентрации в одних руках слишком большой ответственности без возможности оказывать влияние или осуществлять контроль обязанностей.

5.1.2 Совет по безопасности информационно-телекоммуникационных технологий

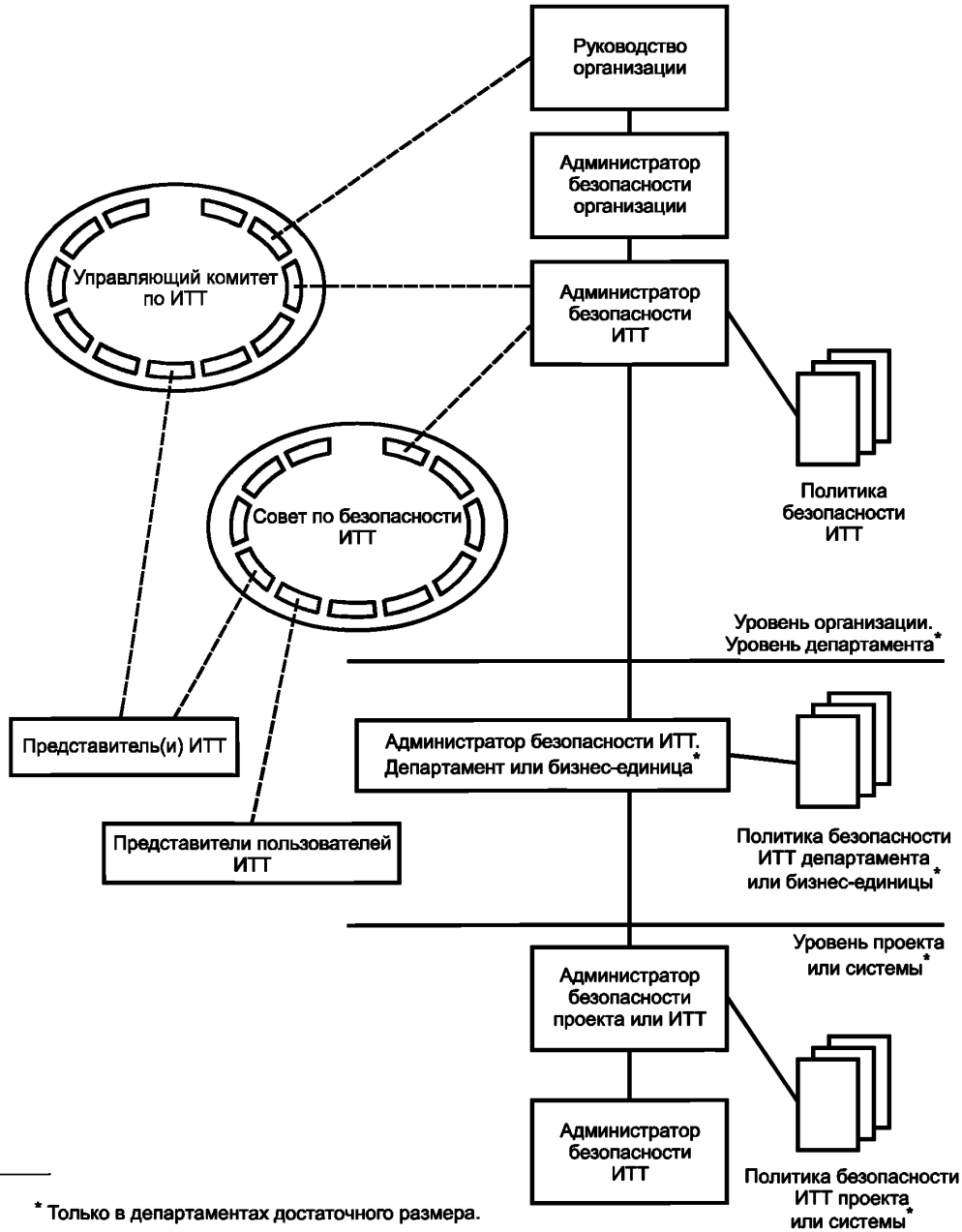
В совет по безопасности ИТТ должны входить люди, обладающие достаточной квалификацией, чтобы давать консультации и рекомендации в отношении стратегий, определять требования, формулировать политику, разрабатывать программу безопасности, проверять их выполнение и руководить администратором безопасности ИТТ. Совет может уже существовать в рамках организации или, что предпочтительнее, может быть создан отдельный совет по безопасности ИТТ. В обязанности такого совета или комитета входит:

- консультирование управляющего комитета ИТТ по вопросам стратегического планирования в сфере безопасности;
- формулирование политики безопасности ИТТ в поддержку стратегии ИТТ и согласование с управляющим комитетом по ИТТ (если существует);
- транслирование политики безопасности в программу безопасности ИТТ;
- мониторинг реализации программы безопасности ИТТ;
- анализ эффективности политики безопасности ИТТ;
- повышение осведомленности о вопросах безопасности ИТТ;
- консультирование относительно ресурсов (людских, денежных, научных и т. д.) для поддержания процесса планирования и реализации программы безопасности ИТТ;
- решение межотраслевых проблем.

Для большей эффективности совет должен включать в свой состав членов, имеющих подготовку в области безопасности и технических аспектов ИТТ, а также представителей провайдеров и пользователей ИТТ. Знания и опыт в этих сферах необходимы для разработки политики безопасности ИТТ.

5.1.3 Администратор безопасности информационно-телекоммуникационных технологий

Ответственность за безопасность ИТТ должна быть возложена на конкретного администратора. Администратор безопасности ИТТ должен играть роль центра для всех направлений безопасности ИТТ в рамках организации; тем не менее, администратор безопасности ИТТ может делегировть другому сотруднику некоторые свои полномочия. Такой сотрудник может взять на себя дополнительно обязанности администратора безопасности ИТТ, хотя в средних и крупных организациях рекомендуется организовывать спе-



* Только в департаментах достаточного размера.

– – – – – - служебные обязанности;

——— - организационный уровень

Рисунок 4 — Пример организации безопасности информационно-телекоммуникационной системы

циальную должность. В крупных организациях может существовать сеть администраторов для подразделений, департаментов и т. д. В качестве администраторов безопасности ИТТ и администраторов безопасности ИТТ для департаментов/подразделений предпочтительно отбирать людей с образованием в области безопасности и ИТТ. В обязанности администратора безопасности ИТТ входит:

- наблюдение за реализацией программы безопасности ИТТ;
- поддержание контакта с советом по безопасности ИТТ и администратором безопасности ИТТ и предоставление им отчетов;
- опубликование и поддержка политики безопасности ИТТ и директив;
- координация расследования инцидентов;
- управление программой осведомленности о безопасности в рамках организации;
- установление целей и критериев безопасности ИТТ, исходя из политик;
- анализ, аудит и мониторинг эффективности контроля безопасности;
- анализ, аудит и мониторинг строгого соблюдения процедур безопасности ИТТ в организации.

Служебные обязанности могут быть разделены с учетом размера организации, сложности системы безопасности и других ее значимых особенностей (см. 5.1.1).

Примеры — Делегируемые функции могут быть следующими:

а) администратор безопасности проекта ИТТ.

Отдельные проекты или системы должны иметь лиц, ответственных за безопасность, которых иногда называют администраторами безопасности проекта ИТТ. В ряде случаев такие обязанности могут быть дополнительной нагрузкой. Руководство такими администраторами должен осуществлять администратор безопасности ИТТ. Администратор безопасности ИТТ является центром всех связанных с безопасностью аспектов проекта, системы или группы систем.

Обязанности администратора безопасности проекта ИТТ включают в себя:

- поддержание контакта с администратором безопасности ИТТ и предоставление ему отчетов,

- выработку и реализацию плана безопасности для конкретного проекта,

- текущий мониторинг реализации и использования защитных мер в сфере ИТТ,

- первоначальное расследование и содействие в расследовании инцидентов;

в) администратор безопасности ИТТ.

В средних и крупных организациях, как правило, существуют функции для делегированного управления, включающие в себя:

- исполнение и применение процедур безопасности ИТТ,

- администрирование безопасности систем и сети,

- обновление специфических программ безопасности (например антивирусных программ, версий программного обеспечения), программного обеспечения,

- администрирование специфических методов контроля безопасности, например резервных копий, списка контроля доступа и т. д.

Администраторы безопасности должны иметь соответствующую подготовку для проведения специальных мероприятий и применения специальных средств защиты.

5.1.4 Пользователи информационно-телекоммуникационных технологий

Пользователи ИТТ отвечают за:

- использование ИТТ-ресурсов в соответствии с политикой, директивами и процедурами;
- защиту бизнес-активов в соответствии с политикой, директивами и процедурами безопасности ИТТ.

5.2 Организационные принципы

5.2.1 Обязательства

Для обеспечения безопасности активов организации должны существовать обязательства руководства организации в отношении обеспечения безопасности ИТТ. Любой фактически существующий или осознаваемый недостаток таких обязательств будет подрывать доверие к администратору безопасности ИТТ и значительно ослаблять защиту против угроз. Результатом поддержки сверху должна стать официально согласованная и документированная политика безопасности ИТТ, вытекающая из политики безопасности организации. Существующая конкретная политика и ее ключевые элементы должны регулярно доводиться до сведения работающих в организации на постоянной основе и по контракту и (где уместно) подчеркивать заинтересованность и поддержку руководством политики безопасности ИТТ.

Обязательства руководства организации в отношении задач безопасности включают в себя:

- понимание общих потребностей организации;
- понимание потребности в безопасности ИТТ в рамках организации;
- демонстрацию обязательств в отношении безопасности ИТТ;
- необходимость обращения к потребностям безопасности ИТТ;
- необходимость выделения ресурсов для безопасности ИТТ;
- осведомленность на самом высоком уровне о том, что является средствами безопасности ИТТ и в чем она заключается (возможности, ограничения).

Следует пропагандировать цели безопасности во всей организации. Каждый сотрудник, работающий на постоянной основе или по контракту, должен знать о своих обязанностях, ответственности, о вкладе в безопасность ИТТ и ему должны быть предоставлены полномочия для их достижения.

5.2.2 Последовательный подход

Необходим последовательный подход ко всей деятельности по планированию, реализации и управлению безопасностью ИТТ. Безопасность должна быть обеспечена на протяжении всего жизненного цикла информации и ИТТ — от планирования до приобретения, тестирования и эксплуатации.

Организационная структура, показанная на рисунке 4, может содействовать гармонизированному подходу к безопасности ИТТ во всей организации. Структура должна быть основана на требованиях и положениях международных, национальных, региональных, отраслевых стандартов и правил, и стандартов организации, применяемых в соответствии с потребностями ИТТ организации. Технические нормы должны дополняться правилами и рекомендациями по их реализации и использованию.

Использование стандартов обеспечивает:

- интегрированную безопасность;
- функциональную совместимость;
- согласованность;
- мобильность;
- экономию средств;
- межсетевое взаимодействие.

5.2.3 Интегрирование безопасности информационно-телекоммуникационных технологий

Деятельность по безопасности более эффективна, если в рамках организации она осуществляется единообразно и с начала жизненного цикла системы ИТТ. Процесс безопасности ИТТ сам по себе является последовательностью множества периодических действий и должен интегрироваться во все фазы жизненного цикла системы ИТТ. Несмотря на то, что безопасность наиболее эффективна в случае интеграции в новую систему с самого начала, интеграция безопасности окажет положительное воздействие на уже работающие системы и бизнес-деятельность на любом этапе.

Жизненный цикл системы ИТТ может быть разделен на четыре основные фазы. Каждая из этих фаз связана с безопасностью ИТТ следующим образом:

- планирование — потребности безопасности ИТТ должны быть учтены при планировании и в процессе принятия решений;
- приобретение — требования безопасности ИТТ должны быть включены в процессы конструирования, разработки, закупки, модернизации систем ИТТ. Интеграция требований безопасности в указанную деятельность гарантирует, что рентабельные средства и меры, относящиеся к сфере безопасности, будут своевременно реализованы в данной системе;
- тестирование — тестирование системы ИТТ должно включать в себя тестирование компонентов, свойств и обслуживания безопасности ИТТ. Новые или измененные компоненты безопасности должны тестироваться отдельно с тем, чтобы подтвердить, что они функционируют должным образом, а далее, в операционном окружении, — для подтверждения того, что их интеграция в систему ИТТ не нарушит характеристик качества или свойств безопасности. В течение всех стадий жизненного цикла системы должно быть запланировано ее периодическое тестирование;
- эксплуатация — безопасность ИТТ должна быть интегрирована в операционную среду. Поскольку систему ИТТ используют для выполнения определенных функций, она должна поддерживаться в рабочем состоянии и, как правило, подвергаться серии модернизаций, включающих в себя закупку новых компонентов технических средств, а также модификации или дополнению программного обеспечения. К тому же она подвержена частым изменениям операционной среды. Эти изменения могут создать новые уязвимости системы, которые должны быть проанализированы и оценены и либо снижены, либо приняты. Столь же важны безопасная замена или переподчинение систем.

Обеспечение безопасности ИТТ — постоянный процесс с множеством обратных связей внутри и между фазами жизненного цикла системы ИТТ. В большинстве случаев существует обратная связь между и внутри всех основных составляющих процесса обеспечения безопасности ИТТ. Связь должна обеспечивать непрерывный поток информации об уязвимостях, угрозах и защитных мерах в системе безопасности ИТТ на протяжении всех фаз жизненного цикла системы ИТТ.

Каждое направление бизнеса организации может также определять уникальные требования безопасности ИТТ. Такие направления должны взаимно поддерживать друг друга: общий процесс безопасности ИТТ должен обеспечивать обмен информацией об аспектах безопасности в целях ее использования для процесса принятия решения руководством.

6 Функции управления безопасностью информационно-телекоммуникационными технологиями

6.1 Общие вопросы

Для успешного управления безопасностью ИТТ требуется применение видов деятельности, некоторые из которых осуществляют в соответствии со следующим циклом:

а) планирование:

1) определение организацией требований по безопасности ИТТ,

2) определение организацией целей, стратегий и политик безопасности ИТТ,

3) установление обязанностей и ответственности в рамках организации,

4) разработка плана по безопасности ИТТ,

5) оценка рисков,

6) решение об обработке риска и выборе защитных мер,

7) планирование непрерывности бизнеса;

б) реализация:

1) создание защитных мер,

2) одобрение ИТТ,

3) разработка и выполнение программы осведомленности персонала о безопасности,

4) аудит-функционирование защитных мер;

в) эксплуатация и поддержка:

1) контроль конфигурации и управление изменениями,

2) управление непрерывностью бизнеса,

3) анализ, аудит и мониторинг, а также проверка соответствия безопасности заявленным требованиям,

4) управление инцидентами безопасности информации.

6.2 Внешние условия

При управлении функциональной деятельностью в области безопасности необходимо учитывать внешнюю среду, в которой действует организация, поскольку она может оказывать значительное влияние на общий подход к организации информационной безопасности. В некоторых случаях обеспечение информационной безопасности является прерогативой государства, которое определяет обязанности и ответственность путем принятия и ввода в действие законов. В других случаях ответственность возлагается на собственника или менеджера. В связи с этим может существенно меняться подход к безопасности ИТТ-организации.

6.3 Управление рисками

Процесс управления рисками должен быть непрерывным. В новых системах и в системах, находящихся на стадии планирования, управление рисками должно быть частью процесса конструирования и разработки. В уже существующих системах управление рисками должно осуществляться в любой подходящий момент. При процессе планирования значительных изменений в системах управление рисками должно быть частью этого процесса и должно учитывать все системы внутри организации, а не применяться только к конкретной изолированной системе.

УДК 004.056:006.354 ОКС 13.110 35.020 Т00

Ключевые слова: информационная и телекоммуникационная технологии, информационная и телекоммуникационная безопасность, риск, угроза, уязвимость

Редактор *В. Н. Копысов*
Технический редактор *Л. А. Гусева*
Корректор *Н. И. Гаврищук*
Компьютерная верстка *З. И. Мартыновой*

Сдано в набор 23.01.2007. Подписано в печать 19.02.2007. Формат 60·84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 2,79. Уч.-изд. л. 2,40. Тираж 334 экз. Зак. 179. С 3732.

ФГУП «Стандартинформ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано и отпечатано в Калужской типографии стандартов, 248021 Калуга, ул. Московская, 256.

gost.e-ecolog.ru