ГОСУДАРСТВЕННЫЙ СТАНДАРТ УЗБЕКИСТАНА

Информационная технология

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 1

Концепции и модели управления безопасностью информационно-коммуникационных технологий

(ISO/IEC 13335-1:2004, IDT)

Узбекское агентство стандартизации, метрологии и сертификации
Ташкент

Предисловие

1 ПОДГОТОВЛЕН Государственным унитарным предприятием Центр развития и внедрения компьютерных и информационных технологий UZINFOCOM (ГУП Центр UZINFOCOM)

2 ВНЕСЕН Техническим комитетом по стандартизации в сфере связи и информатизации № 7

3 ПРИНЯТ И ВВЕДЕН В ДЕЙСТВИЕ постановлением Узбекского агентства стандартизации, метрологии и сертификации (агентство «Узстандарт») от 06.11.2009 № 05-169

4 Настоящий стандарт идентичен международному стандарту ISO/IEC 13335-1:2004 «Информационная технология. Методы обеспечения безопасности. Управление безопасностью информационно-коммуникационных технологий. Часть 1. Концепции и модели управления безопасностью информационно-коммуникационных 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»).

В стандарт внесены следующие редакционные изменения:

a) исключен информационный предварительный элемент «Предисловие";

b) из структурного элемента «Введение» исключены сведения о 3 и 4 частях стандарта;

c) **(Исключен, Изм. № 1)**;

d) стандарт оформлен по национальным требованиям Республики Узбекистан.

Степень соответствия – идентичная (IDT)

5 ВВЕДЕН ВПЕРВЫЕ

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории Узбекистана публикуется в указателе, издаваемом агентством «Узстандарт». В случае пересмотра или отмены настоящего стандарта соответствующая информация будет опубликована в информационном указателе, издаваемом агентством «Узстандарт»

Содержание

(Библиография исключена, Изм. № 1)

Введение ISO/IEC

Настоящий стандарт является первым в серии стандартов в области управления планированием, внедрением и функционированием безопасности информационно-коммуникационных технологий (ИКТ), включая техническое обслуживание.

Государственные учреждения и другие организации в значительной степени полагаются на использование информации при ведении своей деятельности. Нарушение конфиденциальности, целостности, доступности, неотказуемости, подотчетности, подлинности и достоверности активов организации может привести к неблагоприятным последствиям. Следовательно, существует острая необходимость в защите информации и в управлении безопасностью систем ИКТ в пределах организаций. Это требование по защите информации особенно важно в современных условиях, поскольку многие организации соединены во внутренние и внешние сети систем ИКТ, которые необязательно контролируются этими организациями. Кроме того, законодательство многих стран требует, чтобы руководство принимало соответствующие меры для уменьшения рисков, связанных с деятельностью организаций и использованием систем ИКТ. Такие законы могут касаться не только обеспечения защиты данных, но также здравоохранения, финансовых рынков и пр.

ISO/IEC 13335-1 «Информационная технология. Методы обеспечения безопасности. Управление безопасностью информационно-коммуникационных технологий. Часть 1. Концепции и модели управления безопасностью информационно-коммуникационных технологий» содержит обзор по управлению безопасностью на высоком уровне. Эта информация подходит для руководителей и для тех, кто несет ответственность за безопасность ИКТ, общую безопасность или безопасность систем ИКТ организации. Часть 1 концентрирует внимание на концепциях и моделях управления планированием, внедрением и функционированием безопасности ИКТ. Эта часть содержит:

- термины и определения, применяемые во всех частях данного стандарта (Раздел 2);
- описание основных компонентов безопасности и их взаимосвязи, которые включены в управление безопасностью ИКТ (Раздел 3);
- цели, стратегии и политики, необходимые для обеспечения эффективной организационной безопасности ИКТ (Раздел 4);
- организация эффективной безопасности ИКТ, модели подотчетности, явное назначение и подтверждение ответственности за безопасность (Раздел 5);
- обзор функций управления безопасностью ИКТ (Раздел 6).

Информация, представленная в ISO/IEC 13335-1 не может быть прямо применена ко всем организациям. В частности, малые предприятия могут не иметь всех ресурсов, необходимых для полного выполнения некоторых описанных функций. В таких случаях важно, чтобы основные концепции и функции рассматривались соответствующим образом в данных организациях. Даже в крупных организациях некоторые из функций, рассматриваемых в этом стандарте, не могут быть выполнены именно так, как они описаны.

ЎЗБЕКИСТОН ДАВЛАТ СТАНДАРТИ

Ахборот технологияси

ХАВФСИЗЛИКНИ ТАЪМИНЛАШ УСУЛЛАРИ АХБОРОТ-КОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИ ХАВФСИЗЛИГИНИ БОШКАРИШ

1-қисм

Ахборот-коммуникация технологиялари хавфсизлигини бошқариш концепциялари ва моделлари

Информационная технология

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 1

Концепции и модели управления безопасностью информационно-коммуникационных технологий*

Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management

Дата введения 2009-11-16
2019-11-16

1 Область применения

Настоящий стандарт представляет собой руководство по управлению безопасностью ИКТ, устанавливает концепции и модели, лежащие в основе базового понимания безопасности ИКТ, и раскрывает общие вопросы управления, которые важны для успешного планирования, реализации и поддержки безопасности ИКТ.

Целью настоящего стандарта является формирование общих понятий и моделей управления безопасностью ИКТ. 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.

* **С изменением № 1, утвержденным постановлением агентства «Узстандарт» от 03.11.2014 № 05-584**

2 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

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

(Новая редакция, Изм. № 1)

2.2 активы (asset): Что-либо, имеющее ценность для организации.

2.3 аутентичность (authenticity): Свойство, гарантирующее, что субъект или ресурс идентичны заявленным. Аутентичность применяется к таким объектам, как пользователи, процессы, системы и информация.

2.4 доступность (availability): Свойство данных или ресурсов быть доступными и пригодными к использованию по запросу авторизованного логического объекта.

(Новая редакция, Изм. № 1)

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

2.6 конфиденциальность (confidentiality): Свойство данных, позволяющее не давать права доступа к информации или не раскрывать ее неавторизованным лицам, процессам или другим логическим объектам.

(Новая редакция, Изм. № 1)

2.7 контроль (control): В контексте безопасности ИКТ термин «контроль» можно считать синонимом термина «мера безопасности» (см. 2.24 «мера безопасности»).

2.8 рекомендации (guidelines): Описание, проясняющее, что и как должно быть сделано для достижения целей, поставленных в политиках.

2.9 воздействие (impact): Результат инцидента информационной безопасности.

2.10 инцидент информационной безопасности (information security incident): Любое непредвиденное или нежелательное событие, которое может негативно воздействовать на деятельность организации или информационную безопасность.

Пример - Инциденты информационной безопасности:

- ущерб оборудованию или устройствам;

- системные сбои и перегрузки;

- ошибки людей;

- несоответствие политик и рекомендаций;

- нарушения мер физической безопасности;

- неконтролируемые системные изменения;

- сбои программных и аппаратных средств;

- нарушение доступа.

2.11 безопасность информационно-коммуникационных технологий (безопасность ИКТ) (ICT security): Все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостно-

сти, доступности, неотказуемости, подотчетности, аутентичности и достоверности ИКТ.

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

2.13 средство(а) обработки информации (information processing facility(ies)): Любые системы, сервисы или инфраструктуры по обработке информации, а также их физическое местонахождение.

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 сохранять точность и полноту активов.

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

(Измененная редакция, Изм. № 1)

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

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

2.19 риск (risk): Потенциальная возможность нанесения ущерба организации посредством использования определенной угрозой уязвимостей актива или группы активов. Риск измеряется как сочетание вероятности того, что событие произойдет и последствий данного события.

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 управление риском (risk management): Общий процесс идентификации, контроля и устранения (или уменьшения) последствий нежелательных событий, которые могут повлиять на ресурсы систем ИКТ.

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

2.24 мера безопасности (safeguard): Сложившаяся практика, процедура или механизм обработки риска. Понятие «мера безопасности» может считаться синонимом понятию «контроль» (см. 2.7 «контроль»).

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

2.26 уязвимость (vulnerability): Слабое место актива или набора активов, которое может быть использовано при реализации одной или более угроз.

3 Концепции безопасности и взаимосвязи

3.1 Принципы безопасности

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

- управление риском - активы должны быть защищены путем принятия соответствующих мер безопасности. Выбор мер безопасности и управление ими должно осуществляться на основании соответствующей методологии управления рисками, которая, исходя из оценки активов организации, угроз, уязвимостей и различных воздействий угроз, устанавливает допустимые риски и учитывает существующие ограничения;

- обязательства - важны обязательства организации в области безопасности ИКТ и в управлении рисками. Для формирования обязательств необходимо определить преимущества от реализации безопасности ИКТ;

- служебные обязанности и ответственность - руководство организации несет ответственность за обеспечение безопасности активов. Служебные обязанности и ответственность, связанные с безопасностью ИКТ, должны быть уточнены и доведены до сведения персонала;

- цели, стратегии и политики - управление рисками, связанными с безопасностью ИКТ, должно осуществляться с учетом целей, стратегий и политик организации;

- управление жизненным циклом - управление безопасностью ИКТ должно быть непрерывным в течение всего жизненного цикла активов ИКТ.

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 необходимым фактором успешной деятельности организации и основной обязанностью всех уровней руководства. Активы организации должны иметь гарантированную защиту, так как они составляют определенную ценность для организации. К активам относятся (но не ограничиваются):

- материальные активы (например, компьютерная техника, средства телекоммуникаций, здания);

- информация и (или) данные (например, документы, базы данных);

- программное обеспечение;

- способность производить продукт или предоставлять услугу;

- люди;

- нематериальные ресурсы (например, престиж, репутация).

С точки зрения безопасности невозможно внедрить и поддерживать успешную программу по безопасности, если не определены активы организации. Во многих случаях процесс определения активов и установления их ценности может быть проведен на верхнем уровне и не требует дорогостоящей, детальной и длительной процедуры. Уровень детализации данной процедуры должен определяться отношением величины временных и финансовых затрат к ценности активов. Во всех случаях уровень детализации должен быть определен на основе целей безопасности.

Атрибуты активов, которые необходимо рассмотреть, включают в себя их ценность и (или) значимость, а также любые присутствующие меры безопасности. Уязвимости, при наличии конкретных угроз, влияют на требования к защите активов. Внешние условия и правовая система, в которых организация осуществляет свою деятельность, могут влиять на активы и их атрибуты. Например, в одной культурной среде защита персональных данных является более приоритетной, чем в другой. Данные особенности окружающей, культурной и законодательной среды могут иметь существенное значение для международных организаций и трансграничного использования систем ИКТ.

Основываясь на оценке угроз и уязвимостей и их совместном воздействии, можно оценить риск и выбрать меры безопасности, соответствующие защите 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. Этот ущерб может возникать из-за атаки на информацию, обрабатываемую системой ИКТ, на саму систему или на другие ресурсы, вызывая, например, их неавторизованное разрушение, раскрытие, модификацию, порчу, недоступность или потерю. Ущерб активам может быть нанесен только при наличии у них уязвимости. Причиной угроз может быть окружающая среда или человеческий фактор. В последнем случае угрозы могут быть случайными или преднамеренными. Угрозы, как случайные, так и преднамеренные, должны быть идентифицированы, а их уровень и вероятность возникновения должны быть оценены. По многим видам угроз окружающей среды собраны статистические данные. Эти данные могут быть использованы организацией при оценке угроз. Примеры угроз приведены в таблице 1.

Таблица 1 - Примеры угроз

Человеческий фактор		Окружающая среда
Преднамеренные	Случайные	
Подслушивание Модификация информации Взлом системы Вредоносный код Кража	Ошибки и бездействие Удаление файла Ошибка маршрутизации Авария	Землетрясение Молния Наводнение Пожар

Угрозы могут воздействовать на отдельные части организации, например, вывод из строя компьютеров. Некоторые угрозы из числа угроз окружающей среды могут быть общими для всех организаций, 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 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;
- воздействие.

Некоторые угрозы могут воздействовать на несколько активов. В этом случае угрозы могут наносить ущерб в зависимости от того, какие именно активы повреждены. Например, программный вирус на автономном персональном компьютере может нанести ограниченный или локальный ущерб. Однако тот же программный вирус может оказать на сетевой файл-сервер обширное воздействие.

Окружающая среда и социальная среда, в которых действует организация, могут иметь большое значение и существенно влиять на отношение к угрозам и активам. Некоторые угрозы могут вообще не рассматриваться в некоторых средах. В отношении угроз необходимо учитывать аспекты внешней и культурной среды.

В зависимости от результата оценки угроз, их уровень может быть определен как высокий, средний или низкий.

3.4 Уязвимости

Слабость актива или группы 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, руководства, администрирования, аппаратно-программного обеспечения или информации. Угрозы могут использовать уязвимости для нанесения ущерба системам ИКТ или целям деятельности организации. Уязвимости могут существовать и в отсутствии угрозы. Уязвимость сама по себе не причиняет ущерб. Она 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. Уязвимости могут сохраняться, пока сам актив не изменится так, чтобы уязвимость уже не смогла проявиться. Уязвимости 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 определенной 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 новые или вновь появляющиеся угрозы.

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

В зависимости от результата оценки уязвимостей, их уровень может быть определен как высокий, средний или низкий.

3.5 Воздействие

Воздействие - это результат инцидента информационной безопасности, вызванного угрозой и нанесшего ущерб активам. Результатом воздействия могут стать разрушение определенных активов, повреждение систем ИКТ, нарушение конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности. Возможное непрямое воздействие может включать в себя финансовые потери и потерю репутации организации. Контроль за воздействием позволяет достичь равновесия между предполагаемыми последствиями инцидента и стоимостью мер безопасности для защиты от инцидентов. Следует учиты-

вать вероятность возникновения инцидента. Это особенно важно в тех случаях, когда ущерб при каждом возникновении инцидента невелик, а суммарный эффект накопившихся со временем инцидентов может быть существенным. Оценка воздействия является важным элементом оценки риска и выбора мер безопасности.

Для количественного и качественного измерения воздействия могут быть применены следующие методы:

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

3.6 Риск

Риск - это способность определенной угрозы использовать уязвимости актива или группы активов для нанесения ущерба организации. Одна или несколько угроз могут использовать одну или несколько 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 воздействием. Любое изменение активов, угроз, уязвимостей или мер безопасности может оказать значительное влияние на риски. Раннее обнаружение или знание о любых изменениях увеличивают возможность принятия необходимых мер для обработки риска. Обработка риска включает в себя устранение, снижение, передачу и принятие риска.

Риск никогда не устраняется полностью. Принятие остаточного риска является частью оценки соответствия уровня безопасности по отношению к потребностям организации. Руководство организации должно быть поставлено в известность обо всех остаточных рисках, их воздействии и вероятности возникновения инцидентов. Решение о принятии риска должно приниматься уполномоченными лицами, имеющими право принимать решение о допустимости последствий при возникновении инцидента и применении дополнительных мер безопасности в случае, если уровень остаточного риска неприемлем.

3.7 Меры безопасности

Меры безопасности - это действия, процедуры и механизмы, способные обеспечить защиту от угроз, уменьшить уязвимость, ограничить воздействие инцидента информационной безопасности, обнаружить инциденты и облегчить восстановление. Эффективная защита обычно требует сочетания различных мер безопасности для обеспечения уровней безопасно-

сти при защите активов. Например, механизмы контроля доступа, применяемые к компьютерам, должны подкрепляться аудитом, определенным порядком действий персонала, его обучением, а также физической защитой. Некоторые меры безопасности могут уже существовать как часть окружающей среды, со свойственными аспектами актива или могут уже существовать в системе организации.

Соответствующий выбор мер безопасности важен для правильной реализации программы безопасности. Мера безопасности может служить различным целям и, наоборот, одна функция безопасности может потребовать нескольких мер безопасности. Меры безопасности обеспечивают выполнение одной или нескольких нижеперечисленных функций:

- предотвращение;
- сдерживание;
- обнаружение;
- ограничение;
- исправление;
- восстановление;
- мониторинг;
- осведомление.

Пример - Области, в которых могут использоваться меры безопасности

- ***физическая среда;***
- ***техническая среда (аппаратно-программное обеспечение и средства связи);***
- ***персонал;***
- ***администрирование.***

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

Пример – Такими мерами безопасности являются:
- политики и процедуры;
- механизмы контроля доступа;
- антивирусное программное обеспечение;
- шифрование;
- электронные цифровые подписи;
- инструменты мониторинга и анализа;
- резервный источник питания;
- резервные копии информации.

3.8 Ограничения

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

Пример – Такие ограничения могут включать в себя:
- организационные;
- коммерческие;
- финансовые;
- по окружающей среде;
- по персоналу;
- временные;
- правовые;
- технические;
- культурные и (или) социальные.

Данные факторы должны учитываться при выборе и реализации мер безопасности. Необходимо периодически пересматривать существующие и учитывать новые ограничения. Следует отметить, что ограничения могут со временем изменяться в зависимости от географического положения, изменений в социальной и культурной среде организации. Окружающая и культурная среда, в которой функционирует организация, имеет отношение к нескольким компонентам безопасности, в частности к угрозам, рискам и мерам безопасности.

3.9 Взаимосвязь компонентов безопасности

Безопасность систем ИКТ - это многоплановая организация процессов защиты, которую можно рассматривать с различных точек зрения. На рисунке 1 показана модель воздействия некоторого количества угроз на активы. Набор угроз постоянно меняется и известен только частично. Изменения, происходящие с течением времени в окружающей среде способны воздействовать на природу угроз и вероятность их возникновения.

Данная модель отображает:

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

На рисунке 1 представлено пять возможных сценариев. Эти сценарии включают в себя:

- сценарий 1 - мера безопасности S может быть эффективна для снижения рисков R, связанных с угрозой T, способной использовать уязвимость V. Угроза может быть эффективной только при условии, что активы уязвимы для неё;
- сценарий 2 - мера безопасности может быть эффективной для снижения риска, связанного с угрозой, использующей множественные уязвимости;

- сценарий 3 - несколько мер безопасности могут быть эффективны в снижении рисков, связанных с несколькими угрозами, использующих уязвимость. Иногда требуется несколько мер безопасности для снижения риска до приемлемого уровня с целью получения допустимого остаточного риска RR;

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

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

Меры безопасности могут быть реализованы для мониторинга угроз, чтобы убедиться, что угрозы, способные использовать уязвимость, не появились. Ограничения влияют на выбор мер безопасности.

Любая система ИКТ включает в себя активы (в частности информацию, а также программно-аппаратное обеспечение, услуги телекоммуникаций и т.д.), важные для успешной деятельности организации. Эти активы представляют ценность для организации, которая обычно выражается в величине воздействия на коммерческую деятельность с целью неавторизованного раскрытия, модификации или отказа от информации, а также недоступностью или уничтожением информации или услуг. Для того чтобы точнее оценить реальную ценность активов, вначале определяют воздействие 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 могут быть использованы угрозами для того, чтобы вызвать воздействие, т.е. могут ли угрозы использовать уязвимости, чтобы воздействовать на активы. Каждый из этих компонентов (ценность активов, угрозы и уязвимости) может повысить риск. От оценки риска зависят общие требования безопасности, которые выполняются или достигаются реализацией мер безопасности. В дальнейшем применение мер безопасности снизит риск, защитит от угроз и уменьшит уязвимости.

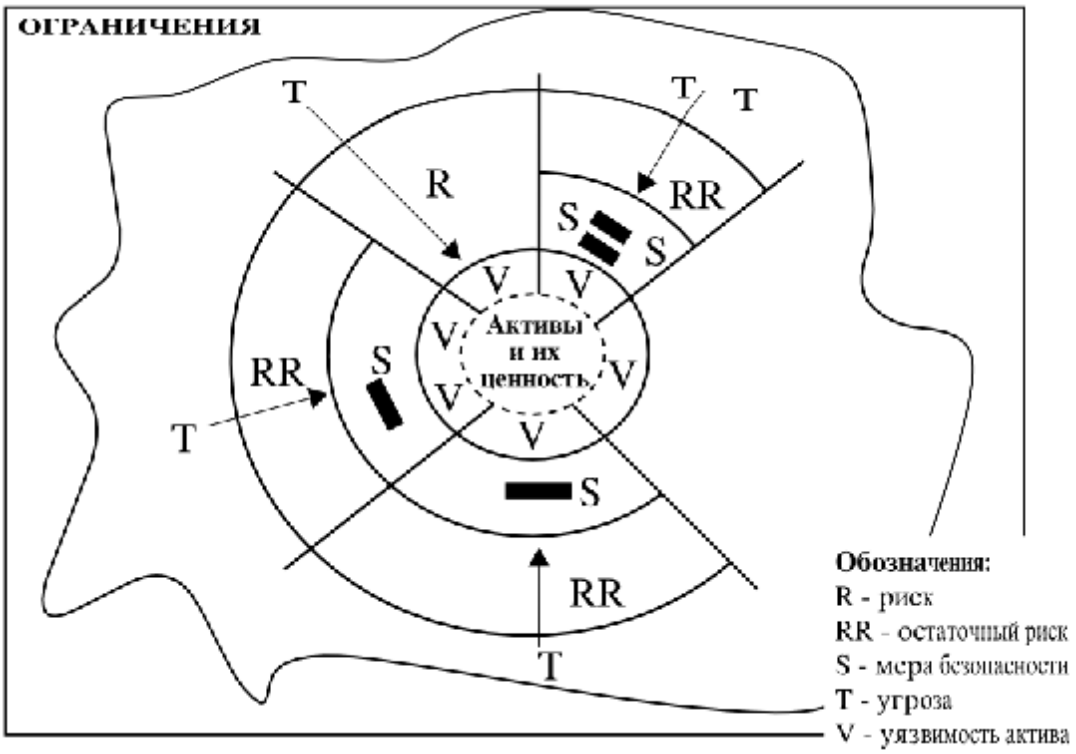


Рисунок 1 – Взаимосвязь элементов безопасности

На рисунке 2 представлена простейшая модель эффективности мер безопасности в целях снижения риска. Часто требуется применение нескольких мер безопасности для снижения риска до приемлемого уровня. Если риск считается приемлемым, то реализация мер безопасности не требуется.

4 Цели, стратегии и политики

В качестве основы эффективной безопасности ИКТ организации, должны быть сформулированы цели, стратегии и политики безопасности организации. Они содействуют деятельности организации и в совокупности обеспечивают согласованность между принятыми мерами безопасности. Важно обеспечить согласованность целей, стратегий и политик для интеграции их в программы обучения, тренинги и программы повышения квалификации персонала в области безопасности.

Цели (чего следует достичь), стратегии (как достичь эти цели), политики (правила, которые должны соблюдаться при осуществлении стратегий) и процедуры (методы осуществления политик) могут быть определены и разработаны начиная от уровня организации и заканчивая уровнем конкретных мероприятий каждого отдела, подразделения или департамента. Руководящие документы должны отражать организационные требования и принимать во внимание любые организационные ограничения. Несмотря на влияние различных точек зрения, важна согласованность между соответствующими документами, а также между различными уровнями организации, поскольку многие угрозы (такие, как взлом системы, удале-

ние файлов и пожары) являются общими проблемами всей организации.

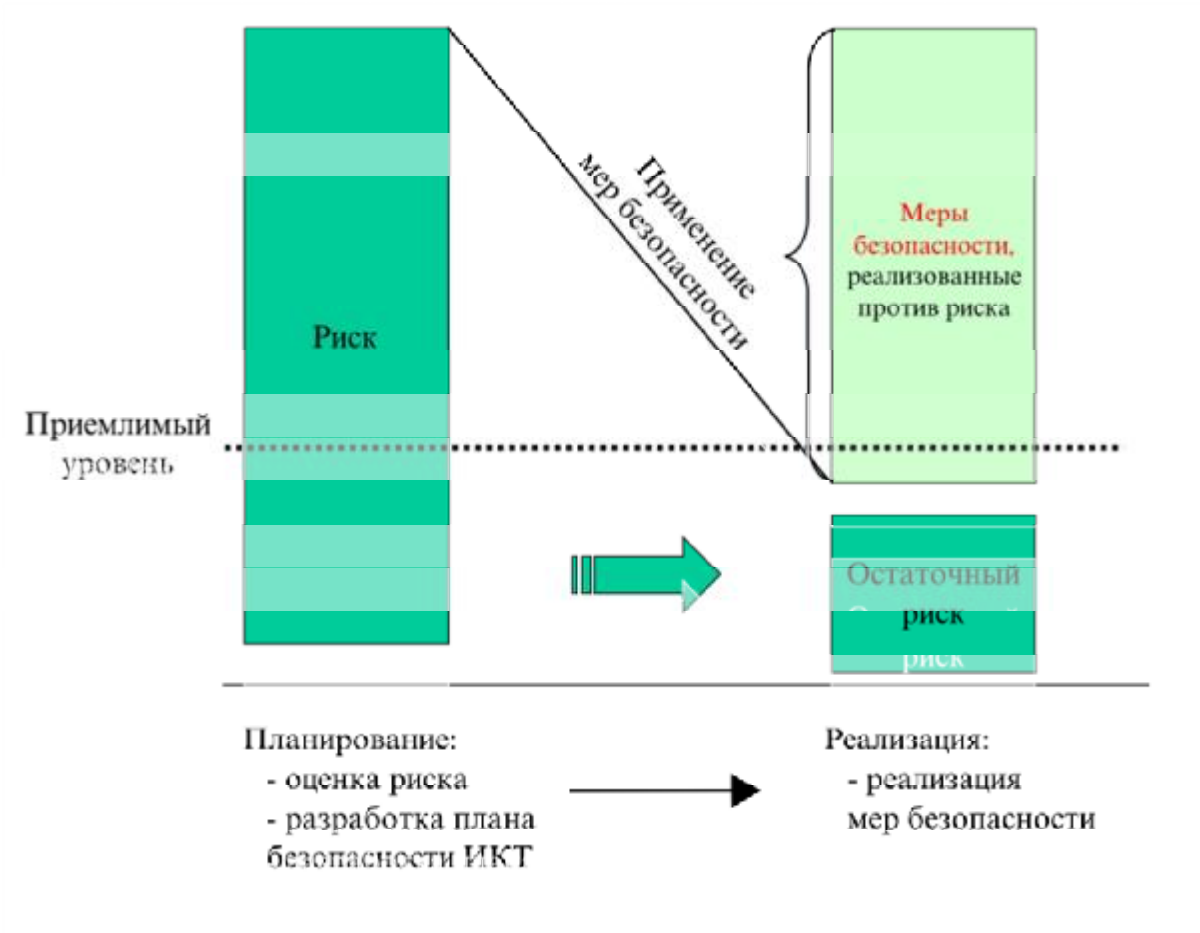


Рисунок 2 – Взаимосвязь мер безопасности и риска

Кроме того, общие цели, стратегии и политики организации должны быть отражены и уточнены в более подробных и конкретных целях, политиках и процедурах, причем во всех областях, представляющих интерес для организации, таких, как управление финансами, персоналом и безопасностью. Безопасность должна быть дополнительно разделена на составные части (безопасность персонала, физическая безопасность, безопасность информации, ИКТ и т.д.). Иерархия документации должна поддерживаться и обновляться на основе результатов периодического анализа безопасности (например, оценки рисков, внутренних и (или) внешних аудитов безопасности) и на основе изменений целей деятельности организации.

Цели, стратегии, политики и процедуры системы ИКТ должны отражать то, что ожидается от данной системы с точки зрения безопасности. Они, как правило, выражаются на общепонятном языке, но возможно будет необходимо описание их более формальным или техническим языком. Цели, стратегии, политики и процедуры устанавливают уровень безопасности для организации и порог приемлемого риска.

4.1 Цели и стратегии безопасности информационно-коммуникационных технологий

После определения целей безопасности ИКТ организации, должна быть разработана стратегия безопасности ИКТ, которая послужит основой для разработки политики безопасности ИКТ организации. Разработка политики безопасности ИКТ организации имеет важное значение для подтверждения того, что результаты процесса управления рисками адекватны и эффективны. Для развития и эффективного внедрения политики, необходима поддержка со стороны всего руководства организации. Крайне важно, чтобы политика безопасности ИКТ организации учитывала цели и конкретные особенности деятельности организации. Она должна соответствовать политике безопасности организации и политике ведения деятельности организации. В таком случае, политика безопасности ИКТ организации будет способствовать достижению наиболее эффективного использования ресурсов, и обеспечивать последовательный подход к безопасности в широком диапазоне условий функционирования систем.

Возможно, потребуется разработка отдельных и конкретных политик безопасности для каждой или некоторых систем ИКТ. Эти политики должны быть основаны на оценке риска и соответствовать политике безопасности ИКТ организации, принимая, таким образом, во внимание указанные в ней рекомендации по безопасности систем, к которым они относятся.

В качестве первого шага в осуществлении процесса управления безопасностью ИКТ, необходимо рассмотреть вопрос о том, насколько широки границы приемлемого для организации риска. Точное определение приемлемых рисков и соответствующего уровня безопасности является ключом к успешному управлению безопасностью. Границы уровня безопасности определяются, исходя из целей безопасности ИКТ, которые организация ожидает достичь. Для того чтобы оценить цели безопасности, необходимо определить активы организации и определить их ценность. При определении необходимо основываться на понимании роли ИКТ в поддержании деятельности организации. Ценность ИКТ как актива организации определяется не только стоимостью самих ИКТ.

Чтобы оценить зависимость деятельности организации от ИКТ необходимо рассмотреть вопросы о том:

– какие важные составляющие деятельности организации не могут осуществляться без ИКТ;

– какие задачи могут быть выполнены только с помощью ИКТ;

– какие основные решения зависят от конфиденциальности, целостности, доступности, неотказуемости, подотчетности и достоверности информации, которая хранится и обрабатывается с помощью ИКТ, или зависят от актуальности этой информации;

– какая конфиденциальная информация, которая хранится или обрабатывается, нуждается в защите;

– каковы последствия инцидента информационной безопасности для организации?

Ответы на эти вопросы могут помочь в оценке целей безопасности ИКТ организации. Если, например, некоторые важные или очень важные составляющие деятельности организации зависят от точности или актуальности информации, то одной из целей безопасности ИКТ этой организации может быть обеспечение целостности и своевременности получения информации в процессе её хранения и обработки в ИКТ-системах. Кроме того, при оценке целей безопасности ИКТ необходимо учитывать цели деятельности самой организации и их связь с безопасностью.

В зависимости от целей безопасности ИКТ, следует согласовать стратегию достижения этих целей. Выбранная стратегия должна соответствовать ценности защищаемых активов. Если, например, ответы на один или несколько из вышеуказанных вопросов показывают сильную зависимость от ИКТ, то вполне вероятно, что эта организация обладает высокими требованиями к безопасности ИКТ, и желательно, чтобы была выбрана стратегия, достаточная для выполнения этих требований.

Стратегия обеспечения безопасности ИКТ в общих чертах излагает процесс достижения организацией своих целей безопасности ИКТ. Рассматриваемые в стратегии вопросы будут зависеть от количества, типа и важности этих целей, и, как правило, это те темы, которые данная организация считает необходимым рассмотреть. Вопросы могут быть как очень конкретными, так и очень общими по своему характеру.

Примеры

1 Конкретный вопрос: организация, в силу специфики своей деятельности, может иметь первостепенную цель безопасности ИКТ, которая заключается в том, что все её системы должны быть постоянно доступны. В этом случае, одним из вопросов, рассматриваемых в стратегии, может быть сведение к минимуму заражения вирусами посредством установки антивирусного программного обеспечения в рамках всей организации.

2 Общий вопрос: одна из целей безопасности ИКТ организации, продающей ИКТ-услуги, может заключаться в том, что ей следует доказать потенциальным клиентам безопасность своих собственных систем. В этом случае в стратегии может быть обозначена необходимость подтверждения уровня безопасности систем этой организации другой, уполномоченной на это, стороной.

Другие возможные вопросы, рассматриваемые в стратегии безопасности ИКТ, в силу конкретных задач или их комбинации, могут включать:

– стратегию и методы проведения процесса оценки рисков, которые должны быть приняты в рамках всей организации;
– политику безопасности ИКТ для каждой системы;
– процедуры обеспечения безопасности каждой системы;
– схему классификации информации во всей организации;
– осведомленность и обучение в области безопасности;

– безопасность соединений, которые необходимо установить и проверить, прежде чем будут подключены сторонние организации;

– единую схему управления инцидентами информационной безопасности в рамках всей организации.

После определения стратегии безопасности, рассматриваемые в ней вопросы, должны быть включены в политику безопасности ИКТ организации.

4.2 Иерархия политик

Политика безопасности организации может состоять из набора принципов и предписаний по безопасности для организации в целом. Политики безопасности организации должны отражать более широкие политики данной организации, в том числе те, которые касаются прав личности, правовых требований и стандартов.

Политика информационной безопасности может содержать принципы и конкретные предписания для защиты критичной, ценной и любой другой информации, имеющей важное значение для организации. Принципы, содержащиеся в ней, берутся и следуют из принципов политики безопасности организации.

Политика безопасности ИКТ организации должна отражать основные принципы и предписания по безопасности ИКТ, применимые к политике безопасности и политике информационной безопасности организации, а также к порядку использования систем ИКТ в организации.

Политика безопасности систем ИКТ должна отражать принципы и предписания, содержащиеся в политике безопасности ИКТ организации. Она должна содержать подробную информацию о конкретных требованиях и мерах безопасности, которые будут внедряться, а также процедуры правильного осуществления мер безопасности для обеспечения надлежащего уровня защиты. Во всех случаях важно, чтобы выбранный подход был эффективным по отношению к потребностям организации в процессе осуществления её деятельности.

Там, где это возможно, политика безопасности ИКТ организации может быть включена в состав технических и управленческих политик, которые составляют основу политики ИКТ организации. Эта политика должна включать несколько убедительных положений о важности обеспечения безопасности, особенно если безопасность необходима для соблюдения этой политики. Рисунок 3 показывает пример возможной иерархии политик организации. Независимо от организационной структуры или документации, принятой в организации, важно, чтобы поддерживалась согласованность различных частей политик.

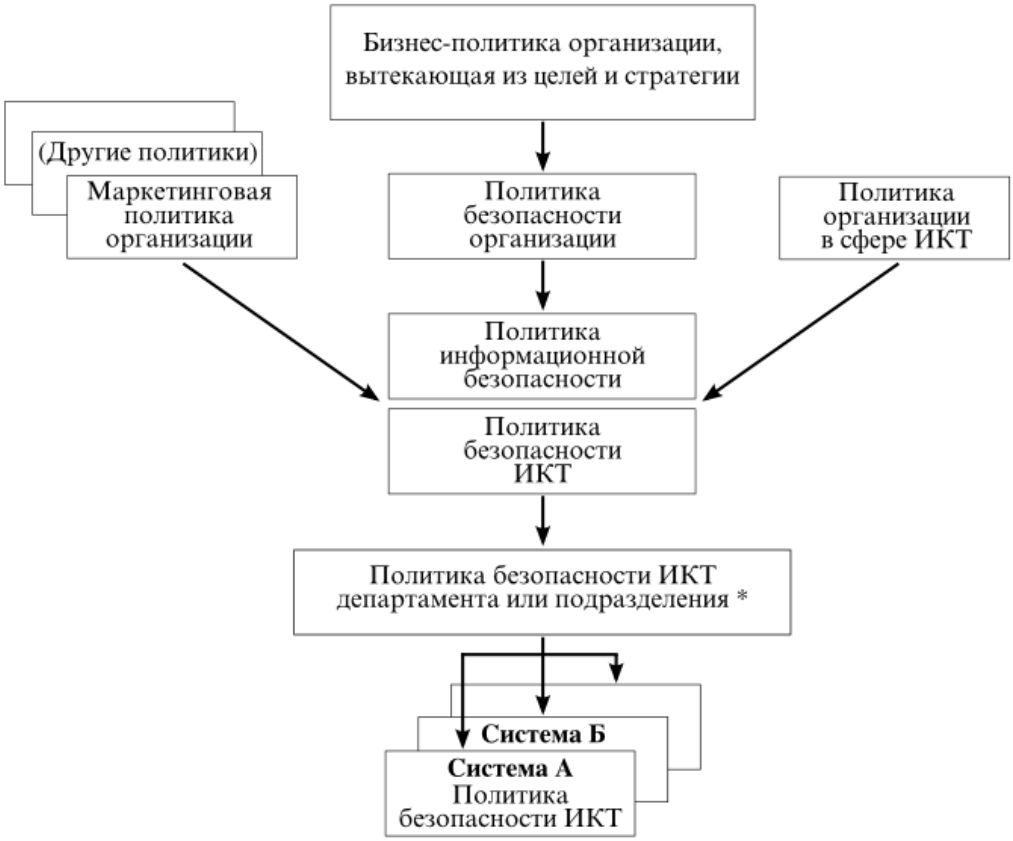
Для конкретных систем и сервисов или для группы таких систем необходимы более подробные политики - политики безопасности систем ИКТ. Важным аспектом управления является то, что масштабы и границы этих политик четко определены, а также основываются как на коммерческих, так и на технических требованиях.

4.3 Элементы политики безопасности информационно-коммуникационных технологий

Политика безопасности ИКТ организации должна основываться на согласованных целях и стратегиях организации в области безопасности ИКТ. Политика безопасности ИКТ организации должна создаваться и поддерживаться в соответствии с законодательством, требованиями регулирующих органов, деятельностью данной организации, безопасностью и политиками в сфере ИКТ.

Чем больше организация опирается на ИКТ, тем важнее обеспечить их безопасность, чтобы гарантировать достижение организацией целей своей деятельности. При написании политики безопасности ИКТ организации, следует принимать во внимание культурные, экологические и организационные особенности, поскольку они могут влиять на подход к безопасности, например некоторые меры безопасности, которые могут быть легко использованы в одной среде, могут быть совершенно неприемлемыми в другой.

Мероприятия по безопасности, изложенные в политике безопасности ИКТ, могут основываться на целях и стратегии организации, результатах предыдущей оценки рисков и управленческих отчетах, результатах последующих действий (таких, как проверка внедрения мер безопасности, мониторинга, аудита безопасности ИКТ в повседневном использовании, проверка отчетов об инцидентах безопасности). Любую серьезную угрозу или уязвимость, обнаруженную в ходе этой деятельности, необходимо соотнести с политикой безопасности ИКТ, описывающей общий подход к решению этих проблем в области безопасности. Более подробные мероприятия описываются в политиках безопасности различных систем ИКТ или в других вспомогательных документах, например, в процедурах обеспечения безопасности.



* Глубина иерархии зависит от разных факторов, например, от размера организации

Рисунок 3 - Иерархия политик

В разработке политики безопасности ИКТ организации должны принимать участие специалисты, связанные с:

- аудитом;
- правом;
- финансами;
- информационными системами (специалисты и пользователи);
- инфраструктурой и общими вопросами (т. е. лица, ответственные за здания, электроснабжение и кондиционирование);
- персоналом;
- безопасностью;
- руководством организацией.

В соответствии с целями безопасности и стратегией, принятых в организации, для их достижения определяется надлежащий уровень детализации политики безопасности ИКТ организации. Политика безопасности ИКТ организации должна описывать:

- ее масштабы и цели;
- цели безопасности с учетом соблюдения нормативно-правовых обязательств и с учетом целей ведения деятельности организации;

– требования безопасности ИКТ с точки зрения конфиденциальности, целостности, доступности, неотказуемости, подотчетности и достоверности информации;

– ссылки на стандарты, на которых основывается политика;

– администрирование информационной безопасности, охватывающее организационные и индивидуальные обязанности и полномочия;

– принятый в организации подход к управлению рисками;

– методы и средства определения приоритетов в реализации мер безопасности;

– уровень безопасности и остаточного риска, установленный руководством организации;

– любые общие правила для контроля доступа (логического доступа, физического доступа в здания, помещения, системы и доступа к информации);

– подход к повышению осведомленности в области безопасности и обучению персонала в рамках организации;

– общие процедуры обеспечения и проверки безопасности;

– общие вопросы безопасности персонала;

– способы, с помощью которых содержание политики будет доведено до сведения всех заинтересованных лиц;

– обстоятельства, при которых политика должна быть проверена или пересмотрена;

– метод контроля изменений в политике.

Организациям следует оценить свои требования, окружающую среду и уровень развития, с тем, чтобы определить конкретные положения, наиболее отвечающие их условиям. Такими положениями могут быть:

– требования к безопасности ИКТ, например, с точки зрения конфиденциальности, целостности, доступности, неотказуемости, подотчетности, подлинности и надежности, особенно с учетом мнений владельцев активов;

– организационная инфраструктура и распределение обязанностей;

– интеграция безопасности в систему развития и закупок;

– определение методов и уровней классификации информации;

– стратегии управления рисками;

– планирование непрерывности ведения деятельности;

– кадровые вопросы (особое внимание следует уделить персоналу, занимающему ответственные должности, например, техническому персоналу и системным администраторам);

– информированность и профессиональная подготовка;

– правовые и нормативные обязательства;

– независимое внешнее (аутсорсинг) управление;

– управление инцидентами информационной безопасности.

Как было отмечено выше, результаты оценки рисков, проверки соблюдения правил безопасности и инциденты информационной безопасности могут оказывать влияние на политику безопасности ИКТ организации.

Это, в свою очередь, может потребовать пересмотра или усовершенствования утвержденной ранее стратегии или политики.

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

Должно быть издано распоряжение, основанное на политике безопасности ИКТ организации, которое было бы обязательным для всех руководителей и сотрудников. Оно может требовать подписи каждого работника на документе, который устанавливает обязанности сотрудника по обеспечению безопасности в организации. Кроме того, для разъяснения этих обязанностей должна быть разработана и внедрена программа по информированию и подготовке персонала в области безопасности.

Для того чтобы политика безопасности ИКТ организации отражала потребности и текущее положение организации, должно быть установлено лицо, ответственное за данную политику. Таким лицом, как правило, является администратор безопасности ИКТ, который несёт ответственность за следующие мероприятия: проверку соблюдения требований безопасности, аудиты, обработку инцидентов и слабых мест безопасности, а также внесение любых изменений в политику безопасности ИКТ организации, которые могут потребоваться по результатам вышеуказанных действий.

5 Организационные аспекты безопасности информационно-коммуникационных технологий

5.1 Служебные обязанности и ответственность

5.1.1 Служебные обязанности, подотчетность и ответственность

Эффективная безопасность требует подотчетности и явного определения и признания обязанностей в этой области. Руководство должно отвечать за все аспекты управления безопасностью, в том числе за решения по управлению рисками. Уровень, на котором будут распределены обязанности, зависит от ряда факторов, таких, как тип, характер деятельности, размер и структура организации. Безопасность ИКТ является междисциплинарным вопросом, относящимся к каждому проекту ИКТ, системе и к каждому пользователю ИКТ в организации. Соответствующее назначение и разграничение подотчетности, а также конкретных функций и обязанностей должны обеспечивать выполнение всех важных задач эффективным и действенным способом. В небольших организациях руководство может исполнять обязанности по обеспечению безопасности, либо другие сотрудники могут выполнять две или более функций безопасности. В таких случаях, во избежание конфликта интересов и для обеспечения надлежащего разделения обязанностей, важное значение имеет независимый обзор функций безопасности.

Хотя эта цель может быть достигнута с помощью различных органи-

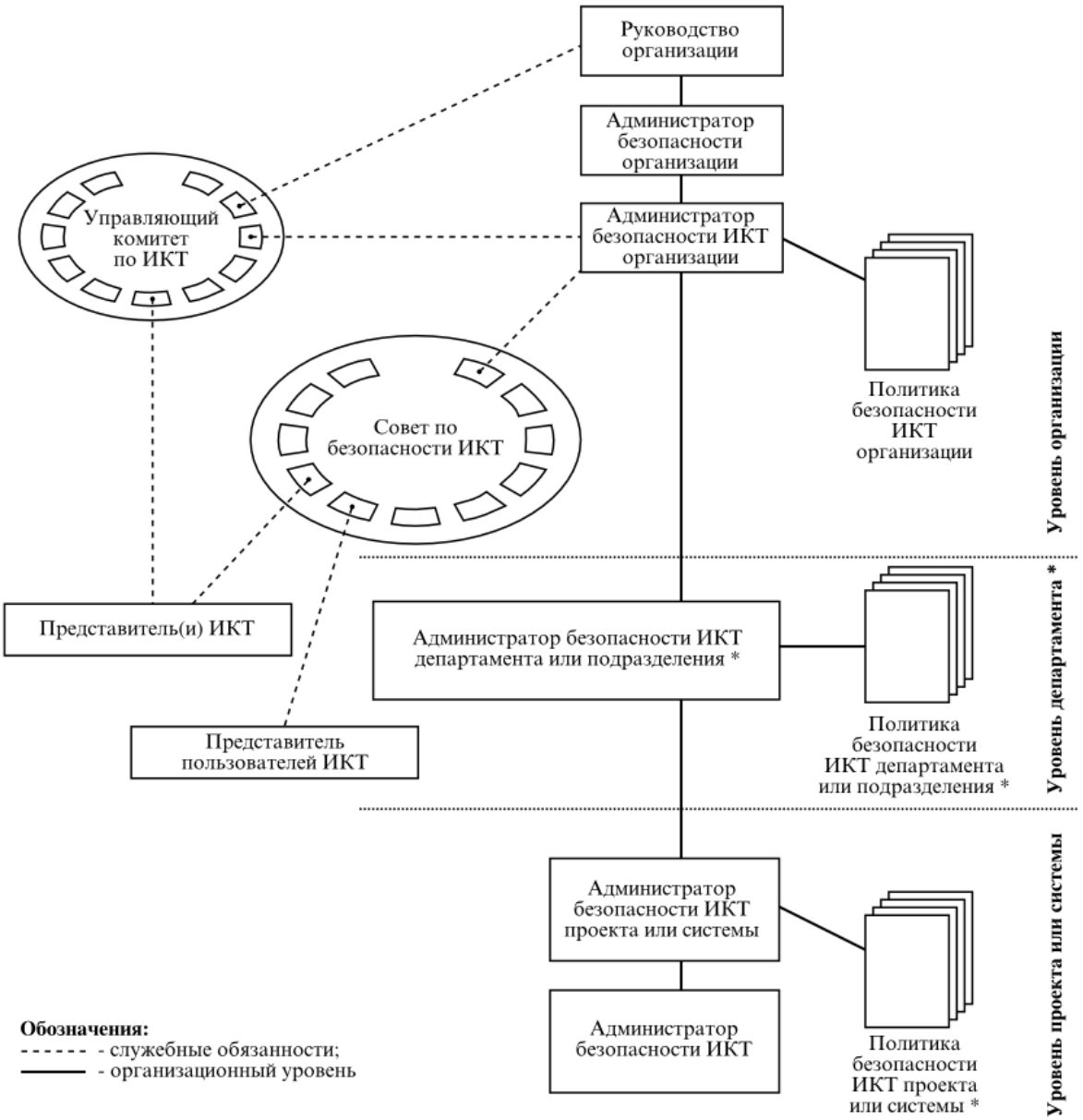
зационных схем, зависящих от размера и структуры организации, следующие обязанности должны быть установлены в каждой организации:

– совет безопасности ИКТ, который решает междисциплинарные вопросы, консультирует и рекомендует стратегию, утверждает политику и процедуры;

– администратор по безопасности ИКТ организации, который связывает воедино все аспекты безопасности ИКТ в рамках организации.

Совет безопасности ИКТ и администратор по безопасности ИКТ должны иметь определённые и четко сформулированные обязанности, а также достаточно высокие полномочия для обеспечения обязательств по исполнению политики безопасности ИКТ организации. Организация должна предоставить администратору по безопасности ИКТ четкие механизмы взаимодействия, ответственности и полномочий, а его обязанности должны быть утверждены советом по безопасности ИКТ. Выполнение этих обязанностей может быть дополнено, в том числе за счет привлечения внешних консультантов.

Рисунок 4 показывает пример организации отношений между администратором по безопасности ИКТ, советом безопасности ИКТ и другими представителями, например, представителями пользователей ИКТ и технического персонала. Эти отношения могут носить управленческий или функциональный характер. Пример организации безопасности ИКТ, описанный на рисунке 4, использует три организационных уровня. Они основываются на классических организационных структурах, таких как корпорация (департамент) или корпоративный центр (бизнес-подразделение), но описанный подход может быть легко адаптирован к любой организации за счет добавления или исключения уровней в соответствии с потребностями организации. Малые и средние организации могут сделать администратора по безопасности ИКТ ответственным за все обязанности и функции в области безопасности. Когда функции безопасности объединены, важно обеспечить соответствующий контроль и баланс, чтобы избежать сосредоточения слишком большой ответственности в руках одного лица, без возможности повлиять на него или контролировать его деятельность.



* Глубина иерархии зависит от разных факторов, например, от размера организации

Рисунок 4 - Пример организации безопасности информационно-коммуникационной системы

5.1.2 Совет по безопасности информационно-коммуникационных технологий

В совет должны входить люди, обладающие необходимыми навыками по консультированию и выдаче рекомендаций по стратегиям, определению требований, формулированию политик, составлению программы обеспечения безопасности, проверке достижений и управлению деятельностью администратора по безопасности ИКТ. Совет может существовать в организации или, что предпочтительнее, может быть создан отдельный совет безопасности ИКТ. В обязанности такого совета или комитета входит:

– консультирование управляющего комитета ИКТ по вопросам стратегического планирования в области безопасности;

– разработка политики безопасности ИКТ, основанной на стратегии организации в области ИКТ и согласование её с управляющим комитетом по ИКТ, если таковой существует;

– перевод политики безопасности ИКТ в программу обеспечения безопасности ИКТ;

– контроль за осуществлением программы обеспечения безопасности ИКТ;

– анализ эффективности политики безопасности ИКТ организации;

– повышение осведомленности в вопросах безопасности ИКТ;

– консультирование относительно ресурсов (людских, денежных, научных и т.д.), необходимых для поддержания процесса планирования и реализации программы обеспечения безопасности ИКТ;

– решение междисциплинарных вопросов.

Для большей эффективности совет должен включать членов, имеющих опыт в области безопасности и в технических аспектах систем ИКТ, а также представителей пользователей систем ИКТ и представителей провайдеров услуг систем ИКТ. Знания и навыки во всех этих областях необходимы для разработки действенной политики безопасности ИКТ организации.

5.1.3 Администратор безопасности информационно-коммуникационных технологий

Ответственность за безопасность ИКТ должна быть возложена на конкретное лицо. Администратор безопасности ИКТ организации выступает как специалист, связывающий воедино все аспекты безопасности ИКТ в рамках организации, хотя администратор безопасности ИКТ может делегировать некоторые свои функции другим лицам. Возможно, в организации окажется подходящий сотрудник, который может взять на себя дополнительные обязанности администратора безопасности ИКТ, но в средних и крупных организациях рекомендуется создать специальную должность. Крупные организации могут иметь сеть администраторов безопасности ИКТ для подразделений, департаментов, занимающихся коммерческой деятельностью и т.д. Желательно, чтобы администратор безопасности ИКТ организации и администраторы безопасности ИКТ департамента имели соответствующий опыт в сфере безопасности. В обязанности администратора по безопасности ИКТ организации входит:

– надзор за осуществлением программы обеспечения безопасности ИКТ;

– связь с советом безопасности ИКТ организации и предоставление ему отчетов;

– утверждение и поддержка политики безопасности ИКТ организации и соответствующих предписаний;

– координация расследования инцидентов;

– управление программой осведомленности в области безопасности в рамках организации;

– установка целей безопасности ИКТ и критериев, исходя из политик;

– пересмотр, аудит и мониторинг эффективности мер безопасности;

– пересмотр, аудит и мониторинг соблюдения процедур безопасности ИКТ во всей организации.

Служебные обязанности могут быть разделены, учитывая размер организации, сложность систем безопасности и другие важные особенности (5.1.1).

Пример - Возможное делегирование функций:

а) администратор безопасности ИКТ-проекта

Отдельные проекты или системы должны иметь ответственных за безопасность лиц, которых иногда называют администраторами безопасности ИКТ-проекта. В некоторых случаях функция администратора безопасности ИКТ-проекта может быть дополнительной обязанностью сотрудника. Руководство деятельностью таких сотрудников должно быть возложено на администратора безопасности ИКТ организации. Администратор безопасности ИКТ-проекта выступает в качестве координационного центра для обеспечения всех аспектов безопасности проекта, системы или группы систем. Его обязанности включают в себя:

– ***связь с администратором безопасности ИКТ организации и отчетность перед ним;***

– ***разработка и реализация плана обеспечения безопасности проекта;***

– ***повседневный мониторинг внедрения и использования мер безопасности ИКТ;***

– ***инициирование и содействие расследованию инцидентов.***

в) технический администратор безопасности ИКТ

В средних и крупных организациях есть обязанности по делегированному управлению. Они включают в себя:

– ***исполнение процедур безопасности ИКТ;***

– ***администрирование безопасности сети и систем;***

– ***обновление специфичных программ по безопасности, например, антивирусов, версий программного обеспечения, установка программных исправлений;***

– ***управление конкретными мерами безопасности, например, резервированием, списками контроля доступа и т.д.***

Технические администраторы безопасности должны иметь соответствующую подготовку для управления конкретными инструментами и мероприятиями.

5.1.4 Пользователи информационно-коммуникационных технологий

Пользователи несут ответственность за:

- использование ИКТ-ресурсов в соответствии с установленной политикой безопасности ИКТ, указаниями и процедурами;
- защиту активов ИКТ в соответствии с установленной политикой.

5.2 Организационные принципы

5.2.1 Обязательства

Для обеспечения безопасности активов организации существуют обязательства руководства организации в отношении обеспечения безопасности ИКТ. Любая фактическая или осознаваемая нехватка таких обязательств будет подрывать доверие к администратору безопасности ИКТ и значительно ослаблять защиту организации от угроз. Результатом видимой поддержки руководства должна стать официально согласованная и документированная политика безопасности ИКТ, вытекающая из политики безопасности организации. Данные политики и их ключевые элементы должны регулярно доводиться до сведения сотрудников, работающих в организации на постоянной основе и по контракту, и подчеркивать заинтересованность и поддержку руководства.

Руководство организации берет на себя следующие обязательства в отношении целей безопасности:

- понимание общих потребностей организации;
- понимание потребности в безопасности ИКТ в рамках организации;
- демонстрацию обязательств в отношении безопасности ИКТ;
- готовность обратиться к потребностям безопасности ИКТ;
- готовность выделить ресурсы для безопасности ИКТ;
- осведомленность на самом высоком уровне о том, что является безопасностью ИКТ и в чем она заключается (область действия, распространение).

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 ИКТ и ему должны быть предоставлены полномочия для их достижения.

5.2.2 Последовательный подход

Последовательный подход к безопасности ИКТ необходимо применять ко всем мероприятиям по планированию, реализации и управлению. Защита должна быть обеспечена на протяжении всего жизненного цикла информации и ИКТ — от планирования до приобретения, тестирования и эксплуатации.

Организационная структура, показанная на рисунке 4, может содействовать гармонизированному подходу к безопасности ИКТ во всей организации. Это усиливает необходимость применения требований стандартов. Стандарты могут быть международными, государственными, отраслевыми или стандартами организации. Технические стандарты должны быть дополнены правилами и руководствами в момент их внедрения и использования.

Использование стандартов обеспечивает:

- интегрированную безопасность;
- функциональную совместимость;
- согласованность;
- переносимость;
- экономию средств;
- взаимодействие между организациями.

5.2.3 Интеграция безопасности информационно-телекоммуникационных технологий

Деятельность по безопасности ИКТ более эффективна, если в рамках организации она осуществляется единообразно и с начала жизненного цикла ИКТ. Процесс безопасности ИКТ сам по себе является циклом действий и должен интегрироваться во все фазы жизненного цикла ИКТ. 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 деловую активность на любом этапе.

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

- планирование - потребности безопасности ИКТ должны быть учтены при планировании и в процессе принятия решений;

- приобретение - требования безопасности ИКТ должны быть включены в процессы конструирования, разработки, закупки, модернизации. Интеграция требований безопасности в указанную деятельность гарантирует, что рентабельные средства и меры, относящиеся к сфере безопасности, будут своевременно реализованы в данной системе;

- тестирование - тестирование ИКТ должно включать в себя тестирование компонентов, свойств и служб безопасности ИКТ. Новые или изме-

ненные 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 ИКТ не будет воздействовать на характеристики и свойства безопасности. В течение всех стадий жизненного цикла системы должно быть запланировано ее периодическое тестирование;

- эксплуатация - безопасность ИКТ должна быть интегрирована в операционную среду. Поскольку ИКТ используют для выполнения определенных функций, они должны 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 операционная среда подвержена частым изменениям. Эти изменения могут создать новые уязвимости системы, которые должны быть проанализированы и оценены и либо уменьшены, либо приняты. Столь же важны безопасная замена или переназначение систем.

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

Каждая область деятельности организации может также определять уникальные требования безопасности ИКТ. Эти области должны взаимно поддерживать друг друга и весь процесс безопасности ИКТ методом обмена информацией об аспектах безопасности в целях ее использования для процесса принятия решения руководством.

6 Функции управления безопасностью информационно-коммуникационных технологий

6.1 Общие вопросы

Для успешного управления безопасностью ИКТ требуется выполнение определенного количества мероприятий, некоторые из которых осуществляют в соответствии со следующим циклом:

а) планирование:

1) определение требований по безопасности ИКТ организации;

2) определение целей, стратегий и политик безопасности ИКТ организации;

3) определение должностных обязанностей и ответственности в пределах организации;

4) разработка плана по безопасности ИКТ;

5) оценка рисков;

6) решение об обработке риска и выборе мер безопасности;
7) планирование непрерывности деятельности;

б) внедрение:
1) реализация мер безопасности;
2) утверждение ИКТ;
3) разработка и внедрение программы осведомленности персонала о безопасности;
4) мониторинг реализованных мер безопасности;

в) эксплуатация и обслуживание:
1) контроль конфигурации и управление изменениями;
2) управление непрерывностью деятельности;
3) аудит, мониторинг и проверка соответствия требованиям безопасности;
4) управление инцидентами информационной безопасности;

6.2 Условия окружающей среды

Мероприятия по управлению информационной безопасностью должны учитывать внешние условия окружения, в которых действует организация, поскольку они могут оказывать значительное влияние на общий подход к безопасности. Кроме того, внешние условия окружения могут воздействовать на тех, кто ответственен за защиту отдельных частей организации. В некоторых случаях данную защиту обеспечивает государственная власть, которая определяет ответственность путем принятия и ввода в действие законов. В других случаях ответственность возлагается на собственника или менеджера. В связи с этим данный вопрос имеет значительное влияние на принятый подход к безопасности.

6.3 Управление рисками

Управление рисками - это мероприятия, осуществляемые на постоянной основе. В новых системах и в системах, находящихся на стадии планирования, управление рисками должно быть частью процесса проектирования и разработки. В уже существующих системах управление рисками должно внедряться в любой подходящий момент. В момент планирования значительных изменений в системах управление рисками должно быть частью этого процесса. Управление рисками должно учитывать все системы внутри организации, а не применяться только к одной изолированной системе.

(Библиография исключена, Изм. № 1)

---

*Оригиналы стандартов хранятся в справочно-информационном центре Узбекского агентства стандартизации метрологии и сертификации.

УДК 025.4.002.6+002 ОКС 35.040

Ключевые слова: информационно-коммуникационные технологии, информационная безопасность, риск, угроза, уязвимость.