Д. С. Чернявский

ОСОБЕННОСТИ РАЗРАБОТКИ И РЕАЛИЗАЦИИ ПОЛИТИК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Введение

Политика информационной безопасности (ИБ) является одним из основных механизмов управления ИБ и подразумевает различные аспекты обеспечения ИБ. Любые требования, правила, принципы, действия и процедуры, так или иначе связанные с обеспечением ИБ организации, находят свое отражение в соответствующей политике. Кроме того, под политикой ИБ часто подразумевается и ее конкретная реализация в виде конфигурации (настроек) программных и программно-аппаратных средств защиты информации. Таким образом, политика ИБ должна определять точные правила того, кто, как и что должен делать, чтобы обеспечить защищенность информации, будь то межсетевой экран (МЭ) или персонал, обслуживающий серверные помещения.

Очевидно, что политика ИБ — это не один документ, а целый набор документации по различным сферам обеспечения ИБ. Данные документы должны быть так или иначе взаимосвязаны и преследовать одну и ту же конечную цель — защита информационных активов организации. Также ясно, что правила политики ИБ, задаваемые в средствах защиты информации, должны быть реализованы именно на основе документированных политик. Одна из основных проблем при разработке и реализации политик ИБ заключается в том, что на сегодняшний день отсутствует четкая формализация того, как должны быть составлены документы и сколько их должно быть. Более того, задача реализации правил политики в конфигурации средств защиты усложняется тем, что средства защиты различных производителей используют различные способы задания политик. Исходя из этого становятся очевидными трудности переноса положений документированной политики на конкретное средство защиты. Естественно, это приводит к снижению эффективности процессов разработки и реализации политик ИБ.

В данной статье рассматриваются основные требования к политикам ИБ и проблемы их реализации в сетевых средствах защиты (ССЗ), а также возможное решение проблемы путем унификации политик для ССЗ.

Стандарты, содержащие требования к политикам ИБ

Рассмотрим стандарты, которые предъявляют наиболее детальные требования к политикам ИБ. Далее под политикой ИБ будем понимать совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности [1].

Требования к политике ИБ описаны в стандартах ГОСТ ИСО/МЭК 17799 [2], ГОСТ ИСО/МЭК 15408 [1] и ГОСТ Р ИСО/ТО 13569 [3]. Кроме того, требования к политикам ИБ предъявляет Стандарт ЦБ РФ СТО БР ИББС-1.0-2010 [4].

В соответствии с ГОСТ ИСО/МЭК 17799 «Практические правила управления информационной безопасностью» главным документом в области обеспечения безопасности является политика ИБ. Стандарт определяет основные положения, которые должны быть отражены в политике, и предлагает ее структуру. По рекомендациям стандарта, совместно с политикой ИБ должны быть изданы документы, более детально описывающие ее требования. Например, более подробные политики, процедуры в области защиты для конкретных информационных систем или правила защиты, которым должны следовать пользователи [2].

Стандарт ГОСТ ИСО/ТО 13569 «Финансовые услуги. Рекомендации по информационной безопасности» выделяет три уровня документации ИБ: политика, документы практических приемов и документы операционных процедур. В данных документах должны быть охвачены как высокоуровневые цели организации, так и конкретные, относящиеся к безопасности, настройке устройств, реализующих политику. Политика ИБ является наименьшим по объему из данных документов и должна содержать высокоуровневые цели и быть сформулированной как можно более просто и сжато, предоставляя конкретную информацию об активах, нуждающихся в защите, например данные о клиентах, сотрудниках, партнерские соглашения и процессы.

Документы практики ИБ определяют общие требования ИБ, которым должна следовать организация, и отражают намерения и цели, установленные руководством при создании программы ИБ, а также документируют методы реализации политики независимым от технологии способом.

Документы операционных процедур, согласно ГОСТ ИСО/ТО 13569, должны описывать технологию реализации политики ИБ. Документов операционных процедур должно быть необходимое число, они должны быть полными, точными и целесообразными и не противоречить любой другой практике или политике. Данные документы должны содержать требования по реализации политики ИБ для конкретной системы или средства защиты с указанием команд и настроек, которые необходимо произвести [3].

Стандарт Банка России СТО БР ИББС-1.0-2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» рассматривает разработку и реализацию политики ИБ как наиболее эффективный метод снижения рисков ИБ [4]. При этом сама политика должна разрабатываться на основе опыта организации в области обеспечения ИБ, результатов идентификации активов, подлежащих защите, результатов оценки рисков, с учетом особенностей бизнеса и технологий, а также интересов и бизнес-целей конкретной организации. Политика ИБ, согласно стандарту Банка России, должна поддерживаться частными политиками ИБ – документацией, детализирующей положения политики ИБ применительно к одной или нескольким областям, видам и технологиям деятельности организации, а также документами, регламентирующими процедуры выполнения отдельных видов деятельности, связанных с обеспечением ИБ. В целом требования СТО БР ИББС во многом схожи с требованиями ГОСТ ИСО/МЭК 17799 и ГОСТ ИСО/ТО 13569. Это связано в первую очередь с тем, что стандарт Банка России разрабатывался с учетом рекомендаций данных стандартов.

ГОСТ ИСО/МЭК 15408 «Критерии оценки безопасности информационных технологий» («Общие критерии») предназначен для использования в качестве основы при оценке характеристик безопасности продуктов и систем информационных технологий [1]. Согласно данному стандарту, политика ИБ является одним из компонентов среды безопасности. Изложение политики ИБ организации включается в Профиль защиты и Задание по безопасности. В дальнейшем положения политики ИБ используются при формулировании Целей безопасности для объекта оценки и его среды. Политика ИБ рассматривается в Общих критериях как один из основных элементов для разработки информационной системы и ее оценки. Общие критерии не содержат практических рекомендаций по разработке политики ИБ, но позволяют формализовать некоторые ее аспекты [5].

Сетевая политика ИБ

Одним из видов частной политики ИБ является сетевая политика ИБ. Сетевая политика ИБ (англ. network security policy) – это набор формулировок, правил и инструкций, которые разъясняют подход организации к использованию сетевых ресурсов и устанавливают то, как должны защищаться сетевая инфраструктура и сетевые сервисы организации [6]. По сути, сетевая политика ИБ концентрируется на контроле сетевого трафика и его использовании, определяет

сетевые ресурсы и угрозы, использование и возможности сети, а также детальные планы действий при нарушении политики [7].

Как правило, данный тип политики описывает высокоуровневые требования по организации и защите сети, такие как: структура сети, принципы доступа в различные сегменты сети, расположение и назначение ССЗ и т. п. Далее под ССЗ будем понимать программное, программно-аппаратное средство или его компонент, прямо или косвенно используемые для защиты информации, передаваемой по вычислительным сетям.

Более конкретные требования по ИБ содержатся в политиках более низкого уровня по управлению и настройке ССЗ: межсетевых экранов, систем обнаружения/предотвращения вторжений, систем предотвращения утечки данных, криптошлюзов, маршрутизаторов, коммутаторов и т. п. В качестве примера рассмотрим политику безопасности для МЭ.

Политика МЭ отличается от политик ИБ более высоких уровней тем, что она является просто описанием того, как политика будет осуществлена МЭ и связанными с ним механизмами безопасности. Данная политика диктует то, как МЭ должен обращаться с сетевым трафиком, а также то, как МЭ должен управляться и обновляться.

Большинство МЭ используют правила как механизм управления безопасностью. Содержание данных правил определяет фактическую функциональность МЭ, и в зависимости от архитектуры МЭ правила могут содержать разное количество информации.

Для управления конфигурацией МЭ обычно используется один из двух механизмов. Первый из них — интерфейс командной строки, который позволяет администратору настраивать МЭ путем набора команд в командной строке. Эта система подвержена ошибкам, связанным с неправильным набором команд. Однако явным преимуществом является то, что опытный администратор может настраивать МЭ и реагировать на чрезвычайные ситуации значительно быстрее, чем при использовании графического интерфейса.

Вторым механизмом является настройка МЭ через графический пользовательский интерфейс. Данный способ более прост и позволяет администратору настраивать сложные системы за приемлемый промежуток времени. Главная проблема графического интерфейса — степень детализации. Во многих современных МЭ есть настройки, которые недоступны из графического интерфейса. В таких случаях необходимо настраивать конфигурацию с использованием командной строки [8].

Таким образом, правила сетевой политики ИБ реализуются в качестве конфигурации того или иного ССЗ. Далее под конфигурацией ССЗ будем понимать совокупность параметров ССЗ, определяющих его функционирование.

Общие требования к политикам ИБ

На основе требований приведенных выше стандартов и особенностей политик для ССЗ можно сделать вполне очевидное заключение о том, что все типы политик, а также правила, задаваемые в ССЗ, взаимосвязаны между собой. Сетевая политика ИБ происходит из политики ИБ организации и должна быть полностью согласована с ней. В свою очередь, политика для конкретного ССЗ является дополнением сетевой политики ИБ и отражает ее положения для некоторой системы безопасности. Правила, задаваемые в ССЗ, по сути, являются воплощением последней политики на практике. Таким образом, для того, чтобы система управления ИБ была эффективной, она должна включать в себя политики всех уровней.

Кроме того, любая политика и ее правила должны удовлетворять следующим требованиям.

Обоснованность. Как для отдельно взятого правила, так и для всей политики в целом должны быть обоснования их применения. Таким образом, в политике должно быть указано, по какой причине вводится данное правило (политика). При непосредственной реализации правил (в качестве настроек ССЗ) также желательно указание комментариев к ним.

Однозначность и максимальная простота. Любые правила политики должны быть сформулированы таким образом, чтобы их было невозможно трактовать двусмысленно. Кроме того, правила должны быть максимально простыми для понимания. Такому подходу необходимо следовать как при написании любого вида документированных политик, так и при задании правил в ССЗ путем набора соответствующих команд или при использовании графического интерфейса. Выполнение этих требований позволяет сделать политику максимально эффективной и уменьшает вероятность того, что некоторое правило будет проигнорировано, а также вероятность обхода правила. Кроме того, правила (политику), удовлетворяющие этим требованиям, удобно обновлять (дополнять, редактировать) и проверять.

Регулярность тестирования и обновления. Правила (политики) должны регулярно проверяться и обновляться в соответствии с возникающими угрозами ИБ. Выполнение регулярного тестирования и обновления политик позволяет более эффективно управлять ИБ. Для того чтобы этот процесс был максимально эффективным, политика должна соответствовать требованиям, указанным выше. Тестироваться и обновляться должны политики всех уровней: конфигурация ССЗ должна соответствовать требованиям политики для данного конкретного ССЗ, которая, в свою очередь, должна согласовываться с политикой сетевой безопасности.

Проблемы реализации политик ИБ для ССЗ

Несмотря на то что основные требования к политике ИБ и частным политикам ИБ определены в рассмотренных выше стандартах, на финальном этапе реализации политики в качестве конфигурации ССЗ возникает проблема, связанная с отсутствием универсального механизма задания правил, что сказывается на эффективности реализации политик и проверке соответствия им.

Производители ССЗ используют различные интерфейсы для их управления. В случае интерфейса командной строки также различаются их командные языки. Таким образом, несмотря на то что ССЗ разных производителей могут обладать схожими функциональными возможностями и реализовывать одни и те же правила политики ИБ, процесс настройки ССЗ зависит от того, какой интерфейс предоставляет данное ССЗ. Более того, даже в устройствах одного производителя одна и та же функция может реализовываться различными командами. В качестве примера можно привести команды назначения на сетевой интерфейс списков доступа в МЭ и маршрутизаторах Cisco.

Очевидно, что разнообразие пользовательских интерфейсов и языков, применяемых для управления ССЗ, создает трудности при настройке конфигурации ССЗ и последующей ее проверке по требованиям политики ИБ. Правила, описанные на естественном языке в политике нижнего уровня (например, политики МЭ), для каждого конкретного ССЗ необходимо «перевести» в набор команд в случае консольного интерфейса или выполнить последовательность действий в графическом интерфейсе ССЗ. Такой «перевод» занимает значительно больше времени, чем в случае, если бы все ССЗ имели одинаковый пользовательский интерфейс и воспринимали единый для всех набор команд. Кроме того, это может приводить к ошибкам при реализации правил политики ИБ в конфигурации ССЗ, особенно если некоторые правила могут быть трактованы неоднозначно или заданы различными способами. Аналогичная проблема возникает при обратном «переводе» конфигурации ССЗ в правила, необходимом при проверке соответствия требованиям политики, особенно если за настройку ССЗ и его проверку ответственны разные люди (что актуально при проведении внешних аудитов ИБ). Кроме того, в случае замены используемого в организации ССЗ на ССЗ другого производителя предназначенную для него политику необходимо переписывать с учетом особенностей интерфейса и внутреннего устройства последнего, то есть политики ИБ в общем случае непереносимы между ССЗ разных производителей.

Унификация (то есть приведение к единой форме) политик ИБ для ССЗ и метода их реализации (процесса настройки ССЗ) позволила бы решить описанные проблемы и, как

следствие, повысить эффективность разработки и реализации политик. При этом формальный язык для описания политик ИБ должен удовлетворять следующим требованиям [9]:

а) *Наглядность и простота*. Правила политики ИБ, формализованные с помощью языка, должны быть простыми для понимания и исключать возможность некорректной трактовки. Выполнение данного требования позволяет снизить вероятность обхода правила в случае его сложности или его неправильной реализации в случае неверного понимания;

б) *Отсутствие абстрактных понятий в структуре языка*. Правила политики ИБ, формализованные с помощью языка, должны состоять из структурных элементов, описание которых должно быть однозначно сопоставимо с реальными объектами, действиями и процессами. Выполнение данного требования позволяет избежать возможности неоднозначной трактовки правил политики ИБ;

в) *Поддержка широкого спектра правил политики ИБ*. Чем шире этот спектр, тем более универсальным является язык;

г) *Применимость к конкретным системам*. Правила политики ИБ, формализованные с помощью языка, должны быть транслируемы в форматы данных и языки конкретных систем. Выполнение этого требования позволяет решить описанную выше проблему реализации политики ИБ в качестве конфигурации различных систем безопасности;

д) *Расширяемость*. Язык должен быть формализован таким образом, чтобы при добавлении нового типа правил ИБ в спецификацию языка общая структура предложений языка оставалась неизменной. Выполнение данного требования позволяет сделать язык применимым к большему числу типов политик и систем путем его расширения;

е) *Открытость спецификации*. Выполнение данного требования обеспечивает возможность расширения языка и его применения к конкретным системам не только разработчиком языка, но и другими заинтересованными сторонами.

Требования а) и б) согласуются с основными требованиями, предъявляемыми к политикам ИБ различных уровней и описанными ранее. Требования в)-е) способствуют решению проблемы реализации правил политики ИБ в конфигурации ССЗ.

В основу синтаксиса и семантики языка могут быть положены функциональные возможности ССЗ. Тогда с опорой на функции ССЗ язык может быть использован для описания политик ИБ для любых ССЗ независимо от их производителя. В данном случае функция ССЗ эквивалентна понятию функции безопасности, то есть функциональным возможностям части или частей системы, обеспечивающим выполнение подмножества взаимосвязанных правил политики ИБ организации. В то же время правила политики ИБ, формализованные с использованием такого языка, будут являться политикой функции безопасности — политикой ИБ, осуществляемой функцией безопасности [1]. На рис. 1 представлена взаимосвязь политик ИБ согласно модели ГОСТ ИСО/МЭК 15408. При этом под политикой безопасности организации на рис. 1 следует понимать не только политику ИБ самого высокого уровня, но и частные политики ИБ, поскольку, как было упомянуто выше, требования и правила, относящиеся к конкретным системам, обычно указываются в политиках более низкого уровня.

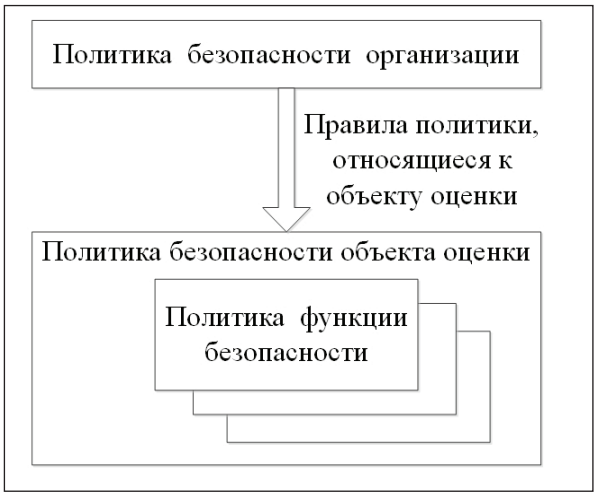

Рис. 1. Взаимосвязь политик ИБ в модели ГОСТ ИСО/МЭК 15408

Трансляция правил политики ИБ в конфигурацию ССЗ

Очевидно, что для реализации в конфигурации ССЗ политик, формализованных описанным выше способом, необходимо использовать транслятор, преобразующий правила политики в последовательность команд и (или) других действий в пользовательском интерфейсе ССЗ.

Рассмотрим применение формального языка, основанного на описании функций ССЗ, для задания и реализации сетевой политики ИБ. Политика ИБ организации описывается в соответствующем документе, который содержит основные цели, задачи и принципы по обеспечению ИБ и ссылки на частные политики ИБ. В сетевой политике ИБ (как одной из частных политик ИБ) описываются требования и правила по организации защиты сети. Сетевая политика ИБ, в свою очередь, содержит ссылки на частные политики ИБ, включающие требования и правила по безопасности для конкретных систем. В политиках, предназначенных для ССЗ, формализуются правила с использованием данного языка. Промежуточных звеньев в виде частных политик ИБ между политикой ИБ организации и политикой, содержащей правила для ССЗ, может быть больше, однако здесь перечислены минимально необходимые элементы для реализации политики. Для выполнения данных правил в конфигурации ССЗ используется система, осуществляющая взаимодействие с ССЗ и преобразующая правила политики ИБ, формализованные с использованием данного языка, в конфигурацию ССЗ. Основой такой системы является транслятор, который, по сути, формирует универсальный пользовательский интерфейс для настройки ССЗ (рис. 2).

В случае замены используемого в организации ССЗ на ССЗ другого производителя новое ССЗ должно выполнять те же функции и соответствовать тем же требованиям (требованиям того же Профиля защиты), если данная замена была вызвана не изменениями в политиках ИБ (например, в случае выхода из строя ССЗ, по истечении срока действия лицензии и т. п.). Политика ИБ для ССЗ, формализованная описанным выше способом, является независимой от конкретного ССЗ и может быть перенесена в конфигурацию нового ССЗ с использованием транслятора.

Рис. 2. Реализация правил политики ИБ в конфигурации ССЗ

Заключение

Базовые требования к политикам ИБ приведены в рассмотренных в статье стандартах, однако пользовательские интерфейсы ССЗ не стандартизованы, что приводит к необходимости учитывать особенности ССЗ при разработке и реализации политик для них. Производители ССЗ используют различные способы задания политик в своих продуктах, и, следовательно, даже если некоторые ССЗ выполняют одинаковые функции, то в общем случае для них необходимо применять различные политики.

Для повышения эффективности процессов разработки и реализации политик ИБ для ССЗ необходимо применять унифицированный подход, позволяющий формализовывать и реализовывать правила политики ИБ, не учитывая особенности пользовательских интерфейсов и внутреннего устройства ССЗ. С этой целью возможно использование формального языка, удовлетворяющего приведенным в статье требованиям, а также транслятора, преобразующего правила политики ИБ в конфигурацию ССЗ. Применение такого подхода позволяет использовать единую политику для всех ССЗ, выполняющих одинаковые функции.

СПИСОК ЛИТЕРАТУРЫ:

1. ГОСТ ИСО/МЭК 15408-2008 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».
2. ГОСТ ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью».
3. ГОСТ Р ИСО/ТО 13569-2007 «Финансовые услуги. Рекомендации по информационной безопасности».
4. Стандарт ЦБ РФ СТО БР ИББС-1.0-2010 «Обеспечение ИБ организаций банковской системы РФ. Общие положения».
5. *Марков А. С., Миронов С. В., Цирлов В. Л.* Разработка политики безопасности организации в свете новейшей нормативной базы // Защита информации. Конфидент. 2004. № 2. С. 2–10.
6. ISO/IEC 18028-2007 "Information technology — Security techniques — IT network security".
7. *Платонов В. В.* Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей. М.: Издательский центр «Академия», 2006.
8. *Wack J., Cutler K., Pole J.* Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800–41, 2002.
9. *Dongliang J., Lianzhong L., Shilong M., Xiaoni W.* Research on Security Policy and Framework // Proceedings of the Second International Symposium on Networking and Network Security (ISNNS10). 2010. Jinggangshan, P. R. China. Academy Publisher. P. 214–217.