Подходы к онтологизации политик информационной безопасности

А.В. Ревнивых

Тюменский государственный нефтегазовый университет (г. Тюмень)
Институт вычислительных технологий СО РАН (г. Новосибирск)
E-mail: alexchr@mail.ru

Глобальная информатизация постиндустриального общества привела к тому, что важнейшее значение для современных организаций имеет разработка политик (регламентов), связанных с информационной безопасностью (ИБ), а также дальнейшее соблюдение этих регламентов. При анализе рисков нарушения ИБ становится очевидным, что на ИБ организации в конечном счете влияет соблюдение очень широкого спектра различного рода политик, регламентирующих действия сотрудников и контрагентов организации с точки зрения совершенно разных аспектов. Кроме того, в политике ИБ может регламентироваться поведение в различных ситуациях самой информационной системы (ИС) и ее отдельных компонентов в частности.

Риски нарушения ИБ для разных организаций будут отличаться как номенклатурно, так и качественно. Необходимо также отметить, что один и тот же инцидент может по разному трактоваться каждым из субъектов, если к нему имеют то или иное отношение несколько организаций. Относительность толкований проявляется и на больших предприятиях, где существенный ущерб одного из структурных подразделений может и не особо повлиять на деятельность головного предприятия (и, наоборот, для структурного подразделения ущерб может казаться небольшим, но для всего предприятия окажется трагедией).

Важным аспектом при разработке политик ИБ является баланс между затратами на ИБ и возможным ущербом, а также его вероятностью [1].

В информатике термин "онтология" подразумевает формальное представление знаний. Онтологии определяют понятия (концепции), относящиеся к какой-то области, а также задают отношения между этими терминами. Современные онтологии могут содержать десятки и сотни тысяч определений, поэтому они часто имеют формат, удобный для чтения компьютером, а также строгую логическую базу.

Классификация политик информационной безопасности

Ниже представлена классификационная схема политик ИБ, представленная в виде рубрикатора. Такая схема позволяет при необходимости расширять понятия, находящиеся в узлах дерева рубрикатора.

0. Политики ИБ
0.1. Политики технологического обеспечения
0.1.1. Политики инфраструктурного технологического обеспечения
0.1.1.1. Политика обновления инфраструктуры
0.1.1.2. Политика учета инфраструктурных ресурсов
0.1.1.3. Политика мониторинга инфраструктуры
0.1.1.4. Политика предоставления и разграничения доступа к инфраструктурным ресурсам
0.1.1.5. Политика защиты от вторжений
0.1.1.6. Политика обеспечения целостности информации
0.1.1.7. Политика защиты от нарушений доступности
0.1.1.8. Политика резервного копирования

0.1.2. Политики прикладного технологического обеспечения
0.1.2.1. Политика обновления прикладных ресурсов
0.1.2.2. Политика учета пользовательских ресурсов
0.1.2.3. Политика мониторинга пользовательских ресурсов
0.1.2.4. Политика мониторинга прикладных ресурсов
0.1.2.5. Политика предоставления и разграничения доступа к прикладным ресурсам
0.1.2.6. Политика предоставления и разграничения доступа к информационным ресурсам
0.1.2.7. Политика использования средств криптографической защиты
0.1.2.8. Политика обеспечения актуальности информации
0.1.2.9. Политика управления версиями

0.2. Организационные политики
0.2.1. Кадровая политика
0.2.2. Политика обеспечения конфиденциальности служебной информации
0.2.3. Экономическая политика
0.2.4. Политика обновления организационных ресурсов [1]

Для описания области знаний, которая прошла через онтологизацию, хорошо подходит закон Муира: «Когда мы пытаемся вытащить что-то одно, оказывается, что оно связано со всем остальным».

Действительно, при изучении данной предметной области, делаем вывод о том, что политики ИБ имеют очень тесные связи друг с другом. Данный факт необходимо учитывать при формировании документов правоустанавливающей юридической документации о ИС.

Концепция ITSM (IT Service Management, управление услугами ИТ) — подмножество библиотеки ITIL, описывающее процессный подход к предоставлению информационных технологий и обеспечению их использования [2].

Приведенный выше подход к составлению обзора политик информационной безопасности в целом приводит к результатам, которые во многих отношениях коррелируют с тем, на что предлагается обратить внимание при внедрении концепции ITSM. Разница состоит в том, что ITSM рекомендует сосредоточиться на клиенте и его потребностях, на услугах, предоставляемых пользователю информационными технологиями, а не на самих технологиях. Приведенный выше подход напротив в основном сосредоточен на технологиях и, кроме того, имеет весьма четко заявленную направленность на обеспечение, прежде всего, ИБ. В каком-то смысле подходы можно считать и противоположными друг другу, так как в целом внедрение политики ИБ обычно снижает удобство использования ИС для рядовых пользователей [1].

ЛИТЕРАТУРА

[1] Ревнивых А.В., Федотов А.М. Обзор политик информационной безопасности // Вестник НГУ. Сер.: Информационные технологии. - 2012. - Т.10. - № 3. - С.66-79. - ISSN 1818-7900.
[2] Р. Ингланд. Введение в реальный ITSM / Пер. с англ. – Москва. Лайвбук, 2010, 132 стр., ISBN: 978-5-904584-05-4.