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.

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.

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».

О терминологии в современных информационных технологиях

Бурное развитие информационных технологий (ИТ) в 20-м веке явилось причиной появления огромного количества новых слов, а также новой смысловой нагрузки у слов существующих.

Исторически количество терминов, связанных с ИТ, непрерывно и весьма быстро росло. Данный процесс продолжается и по сей день. На рынке появляются новые виды технологий, программного обеспечения, аппаратных устройств. Например, в 1990-х годах появились сервисы мгновенных сообщений, в 2000-х - социальные сети и блоги. Непрерывно увеличивается и номенклатура устройств – в 2007-м году появились нетбуки, в 2009-м - планшеты, а в 2011-м – ультрабуки.

Термины ИТ можно разделить на несколько групп:

- Обозначение компьютерных устройств (базовые составляющие, периферийное оборудование) и ресурсов (подаппаратные, аппаратные, программно-аппаратные, прикладные).
- Обозначение технологий, работающих на базе ресурсов ИТ (например, облака, социальные сети, сервисы мгновенных сообщений, блоги).
- Обозначение характеристик и свойств, применимых к тем или иным ресурсам, устройствам, технологиям (например, многозадачность, масштабируемость, многопользовательскость, производительность).
- Обозначение методов, применяемых в ИТ (например, экспликация, полиморфизм, наследование).
- Обозначение событий и фактов, происходящих в тех или иных объектах и субъектах ИТ (например, заражение, перегрев).
- Обозначение субъектов ИТ (например, пользователь, администратор, программист).
- Обозначение атомарных составляющих, используемых в тех или иных ИТ (например, сигнатура, список, голова и хвост списка и т.д.).

Немаловажно заметить, что группы терминов тесно взаимосвязаны.

Термины, обозначающие компьютерные устройства и ресурсы

В понятие о ***устройствах*** входят:

1. Виды компьютеров.
2. Составные части оборудования компьютеров.
3. Различные технологические устройства (источники бесперебойного питания, принтеры, плоттеры, хабы, свитчи и т.д.).
4. Составные части технологических устройств.

В понятие «компьютер» включаются следующие виды вычислительной техники: стационарные компьютеры, мобильные, а также встраиваемые в различные виды техники вычислительные системы.

К стационарным относятся мэйнфреймы, мини-ЭВМ и микро-ЭВМ.

К мобильным компьютерам относятся ноутбуки, нетбуки, ультрабуки, планшетные ПК, а также смартфоны и коммуникаторы.

К встраиваемым компьютерам относятся бортовые ЭВМ бытовой техники, самолетов, автомобилей, поездов, судов и т.д.

Составными частями оборудования компьютеров является содержимое системного блока и основные устройства компьютера (материнская плата, процессоры, оперативная и дисковая память, дисплей и т.д.).

Технологическими устройствами являются периферийные устройства (принтеры, плоттеры, сканеры, МФУ и т.д.) и инфраструктурные устройства (источники бесперебойного питания, хабы, свитчи, системы кондиционирования и т.д.).

К составным частям технологических устройств относится элементная база, из которой состоят технологические устройства.

Термины, обозначающие технологии, работающие на базе ресурсов ИТ

Технологии, работающие на базе ресурсов ИТ, очень разнообразны, но, тем не менее, поделим их на инфраструктурные сервисы, а также сервисы обмена информацией и сообщениями.

К инфраструктурным сервисам отнесем технологии облачных вычислений и хранения информации, технологии сотовой и спутниковой связи, геолокации и другие, работающие на основе ИТ.

Сервисы обмена информацией и сообщениями, базирующиеся на ИТ, это сервисы мгновенной передачи сообщений (ICQ, Jabber и т.д.), блоги, социальные сети, которые уже сложно отнести просто к прикладному программному обеспечению – это именно целые технологии обмена информацией и сообщениями.

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