МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ТЕХНИЧЕСКОЙ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Н.О. Николаев, Д.В.Мишин (Владимир)

Техническая политика информационной безопасности (ИБ) является концептуальной основой системы защиты информации на предприятии. Что актуализирует задачу автоматизации разработки и сопровождения технической политики ИБ предприятия на всех уровнях. Под технической политикой информационной безопасности понимаются требования к режимам функционирования средств защиты информации (СЗИ), их эталонные конфигурации, регламенты обслуживания, руководства и инструкции по эксплуатации, практические приемы и процедуры, включенные в комплект организационно-распорядительной документации ИБ и утвержденные руководством предприятия.

Техническую политику ИБ безопасности принято разделять на документы верхнего, среднего и нижнего уровня. Документы верхнего уровня (требования к режимам функционирования СЗИ, положения о сервисах ИБ, требования реализации политики ИБ и т.д.) разрабатываются аналитиками или руководством службы ИБ. С документами нижнего уровня (регламенты работ, руководства по администрированию, инструкции по эксплуатации отдельных сервисов информационной безопасности и т.д.) работают технические специалисты ИБ, которые реализуют положения технической политики ИБ. Сотрудники службы ИБ предприятия в соответствии со своими должностными обязанностями работают, как правило, с одним из уровней технической политики ИБ, что затрудняет выявление несоответствий в положениях политики различных уровней.

В работе предлагается модель технической политики информационной безопасности предприятия, позволяющая алгоритмизировать ее разработку и сопровождение. Обобщенная модель представлена на рисунке 1. Основой для описания модели является введение новых сущностей: неформальных правил политики ИБ и профилей настройки СЗИ.

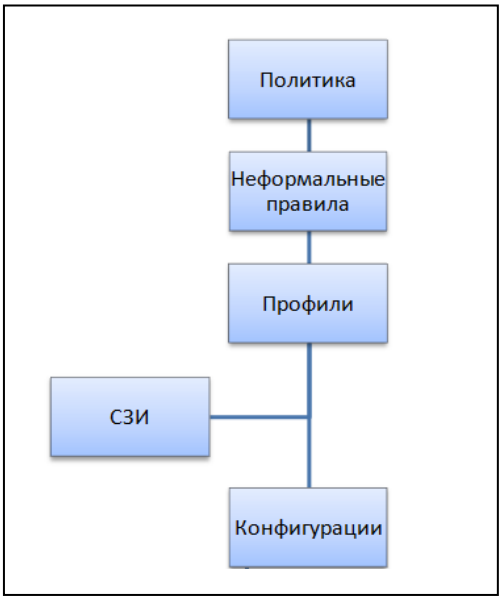

Рис. 1 – Обобщенная модель технической политики ИБ

Представим техническую политику ИБ кортежем (1):

$K = < R, P, F, Q, S >$ (1)

R – Множество неформальных правил технической политики механизма ИБ;

P – Множество конфигурационных параметров СЗИ;

F – Множество профилей СЗИ;

Q – Множество конфигураций (нормативов настройки) СЗИ, реализующих механизм ИБ;

S – Множество СЗИ, реализующих механизмы ИБ.

Механизмы ИБ реализуются множеством СЗИ сети предприятия, которое конечно (2). СЗИ включает в себя набор параметров *P*.

$S = \{s_1, s_2, \dots s_n\}$ (2)

Аналитики или руководитель службы ИБ разрабатывают требования к системе безопасности предприятия. Эти требования не указывают на конкретные СЗИ и их конфигурации. Будем считать, что требования политики ИБ заданного предприятия можно рассматривать, как подмножество требований типового предприятия, разработанных экспертами ИБ. Конечное множество требований политики ИБ назовем неформальными правилами (НП) реализации программно-аппаратной защиты предприятия и обозначим *R* (3).

$R = \{r_1, r_2, \dots r_n\}$ (3)

С точки зрения руководителя службы ЗИ, неформальное правило – требование или группа требований, относящихся к некоторому аспекту программно-аппаратной защиты, написанное на естественном языке. Технический специалист ИБ рассматривает НП, как вектор параметров одного или нескольких СЗИ (4).

$r_1 = \{p_1, p_2, \dots p_n\}$ (4)

$r_2 = \{p_1, p_2, \dots p_n\}$

…

$r_n = \{p_1, p_2, \dots p_n\}$

СЗИ, в рамках модели, рассматривается как вектор конфигурационных параметров, определяющих функции и режим работы СЗИ (5).

$F = \{f_1, f_2, \dots f_n\}$ (5)

Требуемые значения параметров, оформленные в документах технической политики, назовем профилем настройки СЗИ (6).

$f_1 = \{p_1, p_2, \dots p_n\}$ (6)

$f_2 = \{p_1, p_2, \dots p_n\}$

…

$f_n = \{p_1, p_2, \dots p_n\}$

Исходя из (4,5,6), получаем (7):

$r_n \cap f_n = q_n$ (7)

$q_n = \{p_1, p_2, \dots p_n\}$

Требования неформального правила *R* в модели рассматривается как эталонные значения подмножества конфигурационных параметров $P_n \subset P$ СЗИ S_n. В таком случае задача формирования эталонной конфигурации СЗИ S_n сводится к получению максимального количества значений параметров $P_n \subset P$ профиля F из соответствующего множества неформальных правил технической политики ИБ предприятия. Неформальные правила разрабатываются экспертами службы ИБ и соответствуют требованиям предприятия в области ИБ. Множество параметров профиля представлено на рисунке 2.

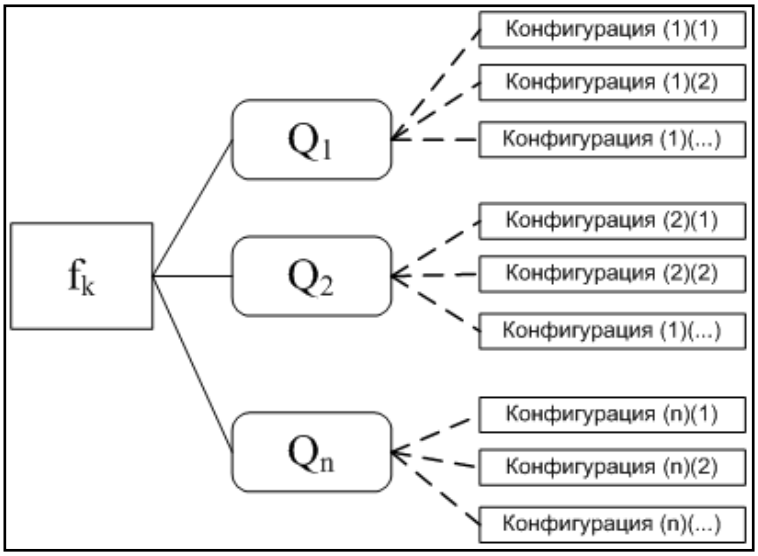

Рис. 2 – множество параметров профиля

Предлагаемая модель позволяет формализовать задачу сформирования профиля СЗИ в соответствии со множеством НП технической политики безопасности предприятия. Следующим этапом работы является разработка программного комплекса, автоматизирующего процесс создания технической политики информационной безопасности предприятия.

Литература

1. 1. Бармен Скотт. Разработка правил информационной безопасности. М.: Вильямс, 2002. — 208с.
2. Петренко С. А., Курбатов В. А. Политики информационной безопасности. — М.: Компания АйТи, 2006. — 400 с
3. *Мишин Д.В., Бегларян А.С.* О политике межсетевого экранирования // Информационные технологии и автоматизация управления Материалы VI Всероссийской научно-практической конференции студентов, аспирантов, работников образования и промышленности (Омск, 27-30 апреля 2015 г.). Ответственный редактор: В. Н. Задорожный, д-р техн. наук, профессор кафедры АСОИУ ОмГТУ Спонсоры конференции: Омский государственный технический университет IT-компания a2disign. Омск, 2015. С. 172-175.
4. *Мишин Д.В., Алексеенко М.С.* Неформальные правила политики туннелирования // Информационные технологии и автоматизация управления Материалы VI Всероссийской научно-практической конференции студентов, аспирантов, работников образования и промышленности (Омск, 27-30 апреля 2015 г.). Ответственный редактор: В. Н. Задорожный, д-р техн. наук, профессор кафедры АСОИУ ОмГТУ Спонсоры конференции: Омский государственный технический университет IT-компания a2disign. Омск, 2015. С. 166-171.
5. *Мишин Д.В., Мошков Н.Е.* О политике идентификации и аутентификации // Информационные технологии и автоматизация управления Материалы VI Всероссийской научно-практической конференции студентов, аспирантов, работников образования и промышленности (Омск, 27-30 апреля 2015 г.). Ответственный редактор: В. Н. Задорожный, д-р техн. наук, профессор кафедры АСОИУ ОмГТУ Спонсоры конференции: Омский государственный технический университет IT-компания a2disign. Омск, 2015. С. 198-200.