28	7	2^{-13}	28	27
32	8	2^{-16}	32	30
36	9	2^{-17}	36	35
40	9	2^{-19}	40	39
44	9	2^{-22}	44	41
48	10	2^{-23}	48	47
52	10	2^{-24}	52	50
56	11	2^{-26}	56	55
60	11	2^{-30}	60	58
64	11	2^{-31}	64	61

Из таблицы видно, что длина ключа, необходимая для того, чтобы шифрсистема была стойкой к линейному методу анализа на заданном числе раундов, равна длине блока открытого текста для всех проведенных экспериментов.

Гипотеза. Пусть $\delta \in (0,1]$. Для любого $n \in \mathbb{N}$ существует алгоритм развертывания ключа блочной шифрсистемы SmallPresent, обеспечивающий ее стойкость к анализу линейным методом при использовании ключа шифрования длины n.

СПИСОК ЛИТЕРАТУРЫ:

1. *Leander G.* Small scale variants of the block cipher PRESENT. Cryptology ePrint Archive, Report 2010/143.
2. *Nakahara J., et al.* Linear (Hull) and Algebraic Cryptanalysis of the Block Cipher PRESENT // Proceedings of CANS'09. Vol. 5888. P. 58–75.
3. *Ozen O., Varici K.* Lightweight block ciphers revisited: Cryptanalysis reduced round PRESENT and HIGHT // Lecture Notes in Computer Science. 2009. Vol. 5594. P. 90–107.

Э. Э. Яндыбаева, И. В. Машкина

ПОЛИТИКА БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ НА ПРЕДПРИЯТИИ

В основе информационной безопасности (ИБ) предприятия лежит комплект документов, включающих в себя концепцию ИБ, модель угроз и нарушителя, политику ИБ, технологические инструкции для сотрудников и т. д. Для обеспечения безопасного использования электронной подписи (ЭП) необходимо создание частной политики безопасности использования ЭП. На рис. 1 показана иерархия документов по ИБ. Ниже приводится текст разработанной политики безопасности использования ЭП.

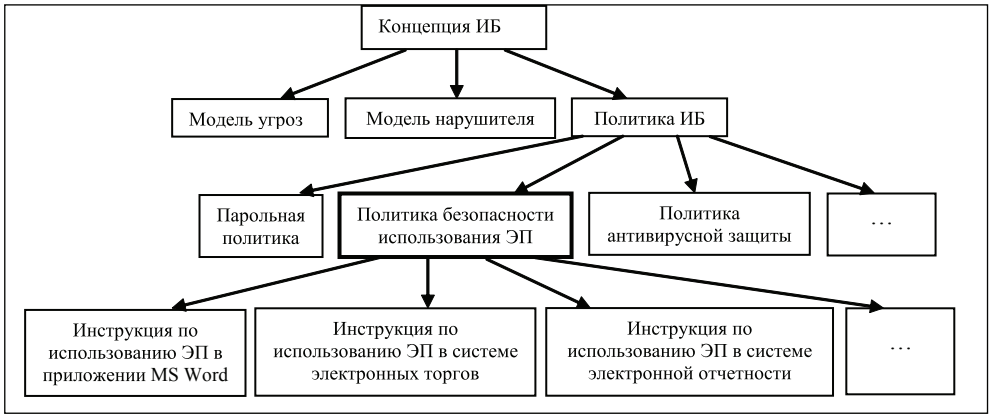

Рис. 1. Иерархия документов по ИБ

ЭП получается в результате криптографического преобразования информации с использованием закрытого ключа электронной подписи. ЭП позволяет определить лицо, подписавшее электронный документ, обнаружить факт внесения изменений в электронный документ после момента его подписания. ЭП создается с использованием средств электронной подписи [1].

Для проверки ЭП используется сертификат открытого ключа электронной подписи. Он принадлежит инфраструктуре открытых ключей (PKI). Сертификат может быть выпущен как внутренним, так и внешним по отношению к предприятию удостоверяющим центром (УЦ).

ЭП может быть использована для внешнего документооборота с контролирующими органами, при совершении гражданско-правовых сделок с российскими организациями, для внешнего документооборота с контрагентами, а также для внутреннего документооборота.

При использовании ЭП должны выполняться следующие требования:

1. В качестве ключевого носителя используется USB-токен со встроенной криптографией. В этом случае закрытый ключ электронной подписи не покидает защищенное устройство и все криптографические операции выполняются непосредственно на USB-токене.

2. На ключевой носитель устанавливается PIN-код. Его значение не является значением, установленным производителем по умолчанию. Значение PIN-кода соответствует парольной политике предприятия.

3. Перед подписанием документ необходимо привести в статичное и безопасное состояние. Для этого необходимо заблокировать содержимое, способное привести к изменениям внешнего вида документа, такое как макросы, мультимедиа, JavaScript [2].

4. Для каждого приложения и для каждой системы электронного документооборота, в которых документы предприятия подписываются электронной подписью, создается инструкция по подписанию документов в данном приложении/системе. Инструкции должны быть пошаговыми, понятными и доступными для сотрудников предприятия.

5. Вместе с подписанным в электронном виде документом сохраняются сертификаты ЭП, необходимые для проверки подлинности подписи. Выполнение данного требования предотвращает угрозу потери юридической значимости документа из-за утраты реестра сертификатов в случае ликвидации УЦ.

6. При необходимости внесения изменения в уже подписанный документ создается и подписывается новый документ с указанием номера корректировки. Таким образом избегаются спорные ситуации, когда одновременно существуют разные варианты одного и того же документа.

7. Закрытые ключи ЭП хранятся в сейфах под ответственность лиц, на то уполномоченных. Доступ неуполномоченных лиц к ключевым носителям исключен.

8. Владельцу закрытого ключа ЭП запрещается передавать его неуполномоченному лицу.

9. При компрометации закрытых ключей ЭП отделом информационной безопасности принимаются меры для прекращения любых операций с использованием этих ключей, для смены закрытых ключей ЭП. По факту компрометации организуется служебное расследование, результаты которого отражаются в акте и доводятся до сведения руководства предприятия.

Таким образом, соблюдение требований разработанной нами политики безопасности позволит существенно снизить риски использования ЭП на предприятии и, как следствие, будет способствовать более широкому применению данной технологии.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».
2. *Buccafurri F.* Digital Signature Trust Vulnerability: A new attack on digital signatures // ISSA Journal, October, 2008. P. 24–28.

ИСПРАВЛЕНИЯ В СТАТЬЮ

В статье А. О. Выборнов, А. П. Курило, В. П. Харламов «РОЛЕВАЯ МОДЕЛЬ СОТРУДНИКОВ БАНКОВСКОЙ ОРГАНИЗАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» опубликованной в 3 номере журнала «Безопасность информайионных технологий» были допущены ошибки в рис.1, рис.2 и рис.3. Правильный вариант рисунков приводится ниже.

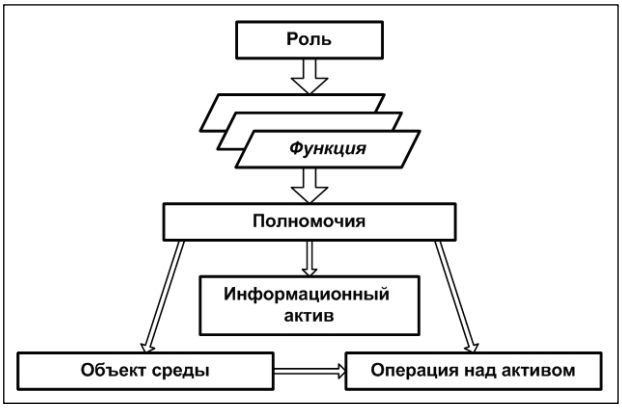

Рис. 1. Структура ролевой модели

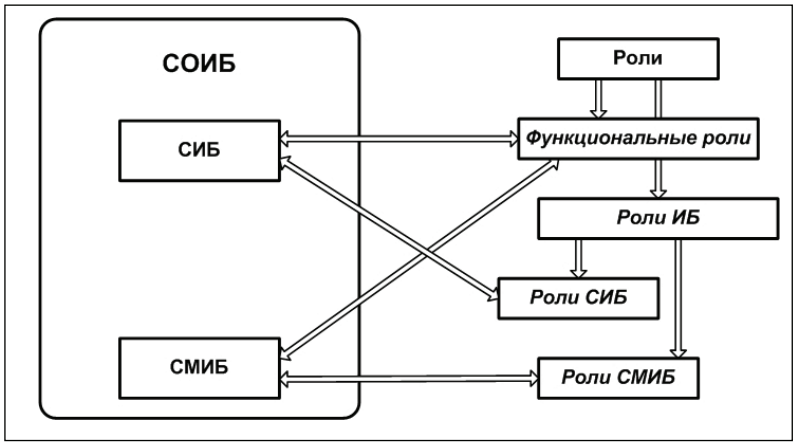

Рис. 2. Категории ролей

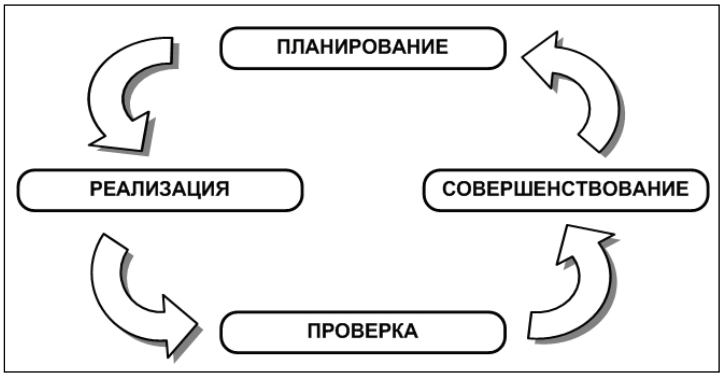

Рис. 3. Модель выделения и назначения функциональных ролей