В. А. Конявский

ЗАО «ОКБ САПР»

ИЕРАРХИЯ ЗАЩИТЫ ЭЛЕКТРОННЫХ ДОКУ МЕНТОВ

Очевидно, что существуют различные виды электронных документов (ЭлД), как и документов вообще. Естественно, что применять сложные и дорогостоящие технологии защиты для малозначительных ЭлД нецелесообразно (тезис о необходимости и достаточности средств защиты). Для иллюстрации этого факта можно сравнить необходимые уровни защиты информационного письма, банковского платежного документа, ценных бумаг и документов, содержащих сведения, составляющие государственную тайну. В этой связи естественно предложить некоторую иерархию трейлеров безопасности (ТБ) [1] для различных видов документов.

При разработке информационной технологии применяется ряд типов допустимых операций, в том числе: операции доступа, функциональные, вычислительные, запросы на доступ и др.

Введем обозначение O_i, $i=\overline{1, m}$, для множеств операций каждого типа.

Рассмотрим множество всех операций АС как объединение множеств операций различных типов: $O = \bigcup_{i=1}^{m} O,\ O \bigcap O_j = \varnothing,\ i \neq j\ ,\ |O| = |O_1| + \ldots + |O_m| = k$

Опр1. Технологией изготовления (обработки) электронного документа будем называть последовательность операций из множества О. результатом применения которых к исходным сведениям является электронный документ.

Каждой операции $o \in O$ поставим в соответствие трейлер безопасности, т. е. некоторый реквизит, фиксирующий целостность применения технических и программных средств при выполнении функций обработки исходных сведений.

Обозначим трейлеры безопасности T_i, $i = \overline{1, k}$.

Рассмотрим множество всевозможных трейлеров безопасности:

$T = \{T_1\ ,\ \ldots,\ T_k\} = \{T_i\}^{k}_{i=1}\ ,\ |T| = k$

Множество всевозможных подмножеств множества Т обозначим **Т**.

Таким образом, в процессе изготовления электронного документа

формируется последовательность трейлеров безопасности, соответствующих операциям, входящим в технологию изготовления рассматриваемого электронного документа.

Обозначим такую последовательность трейлеров безопасности Т, $Т \in \mathbf{T}$.

Установим связь между технологией изготовления (обработки) ЭлД и последовательностью Т, содержащейся в ЭлД.

Опр2. Электронный документ (ЭлД) – это сведения в электронном виде в совокупности с последовательностью трейлеров безопасности, соответствующей технологии изготовления электронного документа:

$$\text{ЭлД} = \{\textit{Сведения}, \text{Т}\}.$$

Последовательностью трейлеров безопасности фиксируют целостность документа и неизменность технологии на протяжении технологического процесса изготовления (обработки) ЭлД.. Таким образом, трейлеры безопасности являются специфическими элементами, несущими в себе информацию о подлинности рассматриваемого электронного документа.

Данное свойство трейлеров безопасности можно использовать для решения вопроса подлинности ЭлД.

Предположим существование в АС некоторого электронного документа, подлинность которого необходимо установить:

$$\text{ЭлД}^* = \{\textit{Сведения}^*, \text{Т}^*\},$$

где $\text{Т}^* = \{T_1^*, \ldots, T_P^*\},\ T_l^* \in T,\ i = \overline{1, p}$.

Каждый из трейлеров безопасности, входящий в последовательность Т*, соответствует некоторой операции $o \in O$ и является реквизитом, фиксирующим целостность выполнения операции применительно к исходным сведениям.

В процессе создания (обработки) ЭлД на каждом этапе, т. е. при выполнении каждой операции, вычисляется значение трейлера безопасности, соответствующего операции.

Введем обозначение:

$N T_i$ – значение трейлера безопасности $T_i \in T,\ N T_i \in N, i = \overline{1, k}$

Значение трейлера безопасности вычисляется как функция от самого трейлера безопасности (как реквизита, соответствующего некоторой операции о $\in$ О) и от сведений, содержащихся в изготавливаемом (обрабатываемом) электронном документе:

$$N_{T_i} = f(Сведения, T_i).$$

Рассмотрим подробней структуру трейлера безопасности. Будем рассматривать трейлер безопасности как совокупность некоторой описательной части (назовем ее *Заголовок),* содержащей в себе данные об операции, в соответствие которой поставлен трейлер безопасности; функциях, с помощью которых вычисляется трейлер безопасности; и значения трейлера безопасности:

$$T_i = \{Заголовок\ T_i,\ N_{T_i}\},\ T_i \in T,\ \ N_{T_i} \in N,\ i = \overline{1, k}$$

Трейлер безопасности $T_i = [Заголовок\ T_i,\ N_{T_i}\}$ с вычисленным значением N_{T_i} включается в обрабатываемый ЭлД. Тогда рассматриваемый электронный документ может быть представлен в следующем виде:

$$ЭлД^* = \{Сведения^*,\ Т^*\},$$

где $Т^* = \{T_1^*, \ldots, T_P^*\},\ T_1^* \in T,\ i = \overline{1, p}$ и $T_i = \{Заголовок\ T_i,\ N_{T_i}\}$.

Опр3. ЭлД является подлинным тогда и только тогда., когда подтверждена:
неизменность технологии изготовления (обработки) ЭлД;
целостность сведений, входящих в рассматриваемый ЭлД.

Рассмотрим этапы установления подлинности ЭлД.

1. Анализ неизменности (эквивалентности) технологии изготовления (обработки) ЭлД.

Изготовление (обработка) любого электронного документа заключается в последовательном применении некоторого набора операций к исходным сведениям. Некоторые операции (например, чтение) могут быть использованы как однократно, так и несколько раз. Так как каждая произведенная операция фиксируется в информационной технологии путем установки ТБ, то, например, повторное прочтение данных в процессе изготовления (обработки) ЭлД может

трактоваться как некоторое технологическое отличие. Однако в случае, когда повторное использование операции является допустимым, можно говорить об эквивалентности информационных технологий и, соответственно, об эквивалентности изготовленных (обработанных) по ним ЭлД.

Рассмотрим множество информационных ресурсов. Выделим из него множество всевозможных электронных документов.

Обозначим его *D*.

Разобьем множество *D* на подмножества в соответствии с требованиями нормативных документов по защите или требованиями, устанавливаемыми собственником информации.

Обозначим их D_i, $i = \overline{1, l}$, $D = \bigcup_{i=1}^{l} D_i$.

Опр4. Подмножества D_i, $i = \overline{1, l}$ будем называть классами электронных документов.

На практике возможны различные способы изготовления (обработки) ЭлД, принадлежащих классу D_i. Другими словами, возможно существование различных информационных технологий, т. е. приемов, способов и методов применения технических и программных средств при выполнении функций обработки исходной информации, результатом которых будет ЭлД $\in D_i$.

Каждую из технологий для класса D_i обозначим T_j^i, $j = \overline{1, r}$.

Как отмечено выше, каждой технологии изготовления (обработки) соответствует последовательность трейлеров безопасности.

Опр5. Базовой (оптимальной) информационной технологией для класса электронных документов D_i будем называть технологию, которой соответствует последовательность трейлеров безопасности Т наименьшей длины.

Такую последовательность для каждого класса электронных документов D_i, $i = \overline{1, l}$ обозначим Т іб , $i = \overline{1, l}$.

Далее для каждого класса D_i, $i = \overline{1, l}$ возникает вопрос об эквивалентности информационных технологий T_j^i, $j = \overline{1, r}$.

Рассмотрим множество трейлеров безопасности *T* как алфавит, т. е. как систему попарно различных знаков, T_i – буквы в алфавите *T*.

Последовательность трейлеров безопасности Т любого ЭлД, т. е. элемент

множества **Т**, является словом в определенном алфавите *Т*.

Согласно [2] преобразование одних слов алфавита в другие осуществляется посредством некоторых допустимых подстановок, которые заданы в виде $R \rightarrow Q$, *где* R *и* Q -слова в заданном алфавите *Т*.

Для рассматриваемого класса электронных документов D_i определим конечную систему допустимых подстановок.

Обозначим ее P_i.

Опр6. Если слово *R* может быть преобразовано в слово *Q* посредством n-кратного применения допустимых подстановок, т. е. существует дедуктивная цепочка, ведущая от слова R к слову Q , то в таком случае слова R и Q называются эквивалентными: $R \; Q$.

Ассоциативным исчислением будем называть совокупность всех слов в алфавите вместе с какой-нибудь конечной системой допустимых подстановок.

В нашем случае, для класса D_i ассоциативное исчисление есть $\{T, P_i\}$.

Как отмечалось выше, T_j^i , $j = \overline{1, r}$. являются словами в алфавите Т.

Опр7. Информационные технологии T_{r1} и T_{r2} , T_{r1}, $T_{r2} \in$ Т, будем называть эквивалентными, если соответствующие им последовательности трейлеров безопасности эквивалентны как слова в алфавите *Т*.

Таким образом, вопрос об эквивалентности информационных технологий будем рассматривать как проблему эквивалентных слов в ассоциативном исчислении $\{T, P_i\}$, т. е. если из слова T_{r1} путем применения допустимых подстановок из P_i, может быть получено слово T_{r2} , то информационные технологии являются эквивалентными.

Учитывая все вышесказанное, предположим, что рассматриваемый ЭлД* принадлежит некоторому классу электронных документов.

Обозначим его $D^* \subset D$.

Последовательность трейлеров безопасности Т* рассматриваемого электронного документа ЭлД* соответствует технологии изготовления (обработки) ЭлД* .

Согласно *опр5* класс электронных документов $D^* \subset D$ связан с базовой

информационной технологией $T^{*б}$

Тогда в случае, если информационные технологии Т* и $T^{*б}$ эквивалентны как слова в алфавите T, будем утверждать, что неизменность технологии изготовления (обработки) Т* электронного документа ЭлД* установлена.

Опр8. Информационную технологию для класса электронных документов D_i будем называть защищенной, если информационные технологии $T_j^{\,i}$, $j = \overline{1, r}$, являются попарно эквивалентными в ассоциативном исчислении $\{T, P_i\}$.

2. Анализ неизменности сведений, содержащихся в ЭлД.

Для каждого трейлера безопасности T^*_j, $j = \overline{1, p}$, входящего в последовательность Т* , необходимо вычислить значение $N_{T1}^{\,*} = f(Сведения^*, T_i^*)$, $j = \overline{1, p}$ (данные о функции f получены из *Заголовка* T_i^* T^*_j) и сравнить полученные значения с уже имеющимися значениями $N_{T1}^{\,i}$, $i = \overline{1, p}$, из набора трейлеров безопасности Т* . В случае, когда

$$N_{T^*_i} = N^*_{T^*_i}, i = \overline{1, p},$$

т. е. в случае совпадения всех вычисленных значений трейлеров с уже имеющимися значениями, можно говорить о целостности сведений, содержащихся в ЭлД*.

Таким образом, иерархия защиты ЭлД связана с установлением соответствия:

классов ЭлД последовательностям $T_i^{\,6}$, $i= \overline{1, l}$ (классификация ЭлД по минимальному множеству трейлеров безопасности, достаточному для защиты этого типа документов);

информационных технологий АС ассоциативным исчислениям $\{T, P_i\}$, $i=\overline{1, l}$ (классификация информационных, технологий по множеству трейлеров безопасности, которые могут устанавливаться на ЭлД, в процессе изготовления (обработки), и допустимым подстановкам, учитывающим возможные расхождения в множествах трейлеров безопасности).

Литература

1. Конявский В. А. Управление защитой информации на базе СЗИ НСД «Аккорд». М., 1999.

2. Трахтенброт Б. А. Алгоритмы и вычислительные автоматы. М., 1974.