УДК 004.492.2

АНАЛИЗ МОДЕЛИ ИСПОЛЬЗОВАНИЯ РЕСУРСОВ С ТОЧКИ ЗРЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цымбалова А.А, Губенко Н.Е.
Донецкий национальный технический университет
Кафедра компьютерных систем мониторинга
E-mail: nastya.tsy@gmail.com

Аннотация:

Цымбалова А.А., Губенко Н.Е. Анализ модели использования ресурсов с точки зрения информационной безопасности. *Рассмотрена общая модель защиты информации. Дано понятие ресурсов для информационных систем и описана модель использования ресурсов системы.*

Общая постановка проблемы

Информационный ресурс стал одним из наиболее главных толчков экономического развития в современном мире. С распространением информационных технологий организации становятся все более зависимыми от информационных систем и услуг, а, следовательно, все более уязвимыми по отношению к угрозам безопасности [1]. Поэтому проблема защиты информации в наши дни стоит особо остро. Проблема обеспечения необходимого уровня защиты информации оказалась весьма сложной, требующей для своего решения создания целостной системы организационных мероприятий и применения специфических средств и методов по защите информации. То есть становится актуальна проблема разработки эффективных систем защиты информации[2].

Анализ состояния методов и подходов по данному вопросу показал, что на сегодняшний день существует несколько методик для решения данной проблемы. Можно выделить работы Петренко С.А., Симонова С.В. по построению экономически обоснованных систем обеспечения информационной безопасности, Мельникова А.З. по проблемам анализа защищенности информационных систем и.т.д. Остановимся подробнее на рассмотрении общей модели выбора средств защиты информации, а конкретно модели использования ресурсов системы, предложенной Грездовым Г.Г.

Модель использования ресурсов системы

Цели защиты информации в системе в общем виде могут быть представлены, как организация оптимального функционирования всех ресурсов системы, то есть обеспечить максимальный результат защиты информации при заданных ресурсах. Для выполнения заданной цели, нужно рассмотреть какие ресурсы существуют в системе и как они используются, то есть построить модель использования ресурсов.

Модель использования ресурсов не является отдельной, а является составной частью общей модели защиты информации. Модель использования ресурсов строится на основе модели функционирования системы, в качестве исходных данных для которой выступает система обработки информации, а результатом является формальное описание технологии функционирования системы.

Информацию, аппаратное и программное обеспечение, обслуживающий персонал, а также помещения, в которых размещаются узлы функционирования системы будем рассматривать как ресурсы системы.

Основным ресурсом является информация. Защита информации должна обеспечиваться на всех этапах ее обработки, так как именно информация является предметом посягательства злоумышленников. Информацию, находящуюся на узлах

функционирования системы можно описать как поступающую для обработки, принятую для обработки и поступающую на выход. Формы представления информации могут быть самыми разнообразными. Информация может находиться на съемных носителях, на бумажных носителях, в оперативной памяти ЭВМ, в файлах на жестких дисках, в каналах связи сети передачи данных [3].

Для построения модели использования информации необходимо знать, какая информация и в каком виде находится на указанных участках системы. Модель использования информации можно представить следующим образом:

$$MI = \bigcup_{j=1}^{k} MI_j \tag{1}$$

где MI - модель использования информации системы; k - число участков функционирования системы; MI_j - модель использования информации системы для j-го участка функционирования системы.

Модель использования информационных ресурсов j-ым участком функционирования системы можно представить следующим образом:

$$MI_j = \{In(I)_j; Out(I)_j; P(I)_j\} \tag{2}$$

где MI_j - модель использования информационных ресурсов j-ым участком функционирования системы; $In(I)_j$ - множество состояний, в которых информация поступает на участок функционирования для ее обработки; $Out(I)_j$ - множество состояний, в которых информация поступает на выход участка функционирования после ее обработки; $P(I)_j$ - множество состояний, в которых информация находится на участке функционирования во время ее обработки

Следующий ресурс - это аппаратное обеспечение, в состав которого входят: сервера и рабочие станции пользователей, система передачи данных, устройства для тиражирования и копирования информации. Именно аппаратные средства обеспечивают пресечение разглашения, защиту от утечки и противодействие несанкционированному доступу к источникам конфиденциальной информации [3]. Модель использования аппаратного обеспечения системы можно представить следующим образом:

$$AO = \bigcup_{i=1}^{N} AO_i \tag{3}$$

где AO - модель использования аппаратного обеспечения системы; N - число средств аппаратного обеспечения в системе; AO_i - модель использования i-го аппаратного средства системы.

Модель использования i-го аппаратного средства имеет вид:

$$AO_i = \{P_i; PO_i; I_i; UF_i; U_i\} \tag{4}$$

где P_i - множество помещений, в которых находятся i-ое аппаратное средство; PO_i - множество программных средств, используемых i-ым аппаратным средством; I_i - множество состояний информации, находящейся на i-ом аппаратном средстве; UF_i - множество участков функционирования, в которых задействовано i-ое аппаратное средство; U_i - множество пользователей, имеющих доступ к i- му аппаратному средству.

Следующий ресурс - это помещения. Помещения включают в свой состав системы электропитания, водоснабжения, телефонные линии и т.п. Отдельного внимания заслуживает размещение помещений, тип стройматериалов, используемых при постройке стен, перекрытий, окон, дверей [3].

Модель использования помещений можно представить следующим образом:

$$P = \bigcup_{i=1}^{M} P_i \tag{5}$$

где P - модель использования помещений системы; M - число помещений в системе; P_i - модель использования i-го помещения системы.

Модель использования i-го помещения имеет вид:

$$P_i = \{W_i; S_i; AO_i; I_i; UF_i; U_i\} \tag{6}$$

где W_i - множество перекрытий (стены, потолок, окна, двери и т. д) i-го помещения системы; S_i - множество систем (отопления, электро- и водоснабжения и т. д), обеспечивающих функционирование i-го помещения системы; AO_i - множество средств аппаратного обеспечения, находящихся в i-ом помещении системы; I_i - множество состояний информации, находящейся в i-ом помещении системы; UF_i - множество участков функционирования, находящихся в i-ом помещении системы; U_i - множество пользователей, имеющих доступ в i- ое помещение системы.

Следующий ресурс – это пользователи или персонал, то есть люди, обеспечивающие функционирование.

Модель описания пользователей системы можно представить следующим образом:

$$U = \bigcup_{i=1}^{L} U_i \tag{7}$$

где U - модель описания пользователей системы; L - число пользователей в системе; U_i - модель использования i-го помещения системы.

Модель i-го пользователя будет выглядеть следующим образом:

$$U_i = \{R_i; P_i; AO_i; I_i; UF_i\} \tag{8}$$

где R_i - множество ролей i-го пользователя; P_i - множество помещений, в которые имеет доступ i- ый пользователь; AO_i - множество средств аппаратного обеспечения, к которым имеет доступ i-ый пользователь; UF_i - множество участков функционирования, к которым имеет доступ i-ый пользователь системы [4].

На рисунке 1 схематически представлено взаимодействие описанных выше моделей.

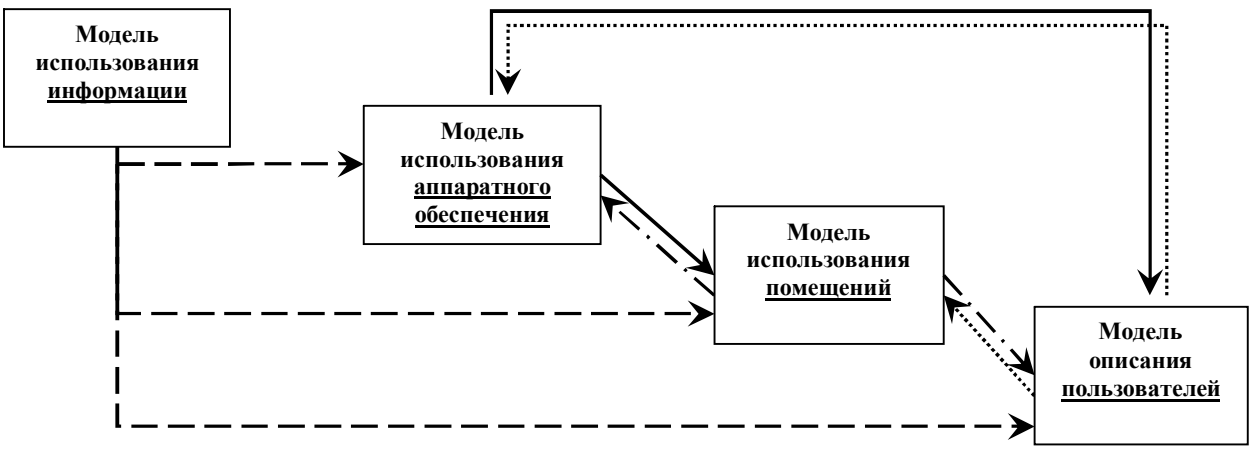

Рис. 1. Взаимодействие составных частей модели использования ресурсов

Модель использования ресурсов строится на основе приведенных выше моделей, но это только в общем случае, так как модель может быть усовершенствованна для конкретного вида предприятия, куда эта модель будет внедряться. Результаты этой модели очень важны, так как они понадобятся для построения моделей угроз информации, модели противника, модели оценки потерь, а также необходимы для адекватной оценки системы, определения функциональных участков системы, классификации обслуживающего персонала, описания правил доступа к информации и т.д. Список возможных форм представления информации на участках функционирования системы понадобятся при формировании модели угроз, а также для получения требований к средствам защиты информации.

Выводы

Как показывает анализ с позиции системного подхода, модель использования ресурсов является эффективной для формирования комплексной, плановой, целенаправленной, активной и надежной системы защиты информации. В данной модели видно четкое взаимодействие каждого из рассмотренных ресурсов системы, а ведь главное в координации деятельности информационной безопасности – это пополнение и распределение этих ресурсов.

Хотелось бы выделить сильные стороны рассмотренной модели:

- для модели использования аппаратного обеспечения учтены такие сведения, как его размещение, использование программных средств и информации, доступ пользователей к данному аппаратному обеспечению.

- для построения модели использования помещений учтены такие сведения, как перекрытия данных помещений, находящиеся в них системы функционирования, аппаратные средства и информация, а также пользователи, имеющие доступ в данные помещения.

- для построения модели описания пользователей учтены множество помещений и аппаратных средств, к которым пользователи имеет доступ в зависимости от их роли.

Но, как и любая модель, модель использования ресурсов имеет некоторые слабые стороны:

- для построения модели использования информации необходимо учесть степень важности информации так, как именно эти знания нужны для сопоставления угроз и возможного ущерба от них применительно к разным условиям или разным зонам защиты.

- для построения модели описания пользователей также необходимо учесть степень важности информации и доступ к ней в зависимости от роли пользователей.

- что касается аппаратных средств, следует четко разработать политику отслеживания устаревших аппаратных средств и внедрения новых, а также отражение этих нововведений в модели.

Литература

1. Малюк А.А., Пазизин С.В, Погожин С.С. Введение в защиту информации в автоматизированных системах. [Текст] – М.: Горячая линия - Телеком, 2001. – С 148 .

2. Защита информации и Информационная безопасность [Electronic resourse] / Интернет-ресурс. – Режим доступа: www/URL: http://www.zashita-informacii.ru/ – Защищенные распределенные системы.

3. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие для вузов. [Текст] – М.: Горячая линия - Телеком, 2004. – С 280.

4. Гроздов Г. Г. Способ решения задачи формирования комплексной системы защиты информации для автоматизированных систем 1 и 2 класса [Текст] / Г. Г. Гроздов // (Препринт/ НАН Украины. Отделение гибридных управляющих систем в энергетике ИПМЭ им. Г. П. Пухова НАН Украины; № 01/2005) – Киев : ЧП Нестреровой, 2005. – С. 66.