ЯЗЫК ОПИСАНИЯ МОДЕЛИ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

К.Е. Израилов, А.Ю. Васильева

Введение

Обеспечение безопасности передаваемой информации в настоящее время является одним из основных условий, предъявляемых к телекоммуникационной сети (далее – ТКС). Это приводит к необходимости постоянной оценки информационной безопасности (далее – ИБ) на всех этапах жизненного цикла ТКС.

Такая оценка производится с применением различных моделей ИБ телекоммуникационной сети (далее – Модель). Для автоматизации процесса моделирования, применяются соответствующие программные средства. При этом, сама Модель и ее операции реализуются в функциональном модуле средства, являясь промежуточным уровнем между информационным (хранящем характеристики объектов Модели) и интерфейсным (предоставляющем пользователю взаимодействие с Моделью).

Анализ средств моделирования и их архитектуры показал, что все они обладают рядом следующих недостатков. Как правило, средства предназначены для статического представления Модели и плохо адаптируемы к изменениям во времени ТКС и его информационного пространства (далее – ИП). Информационный и интерфейсный модули разрабатываются раздельно и оперируют различными сущностями, что приводит к необходимости их постоянного согласования через функциональный. Для всех средств отсутствует единая структуры данных в информационном модуле и концепции графического представления в интерфейсном, что не позволяет сделать моделирование ТКС стандартизованным.

Для устранения указанных недостатков средств моделирования, удачным решением являлась бы разработка специального языка описания Модели, такого что программа на нем была хорошо адаптируема к изменениям ТКС и ИП, а во всех приведенных модулях средств использовались бы единые объекты (а значит обладающие свойствами как ИБ, так и графического отображения). При этом, корректировка вводимых данных ИП будет произведена автоматически. При этом программа может включать код, сгенерированный по базам данных ИБ (например, по открытым таблицам уязвимостей телекоммуникационных устройств).

Язык описания Модели

Предлагаемый язык может быть лаконично назван «Язык описания модели безопасности» (англ. Security Model Description Language, SMDL). Программа на нем описывает элементы безопасности, их характеристики и взаимосвязь. Такой язык относится к активно развивающемуся направлению предметно-ориентированных языков (англ. Domain-Specific Language, DSL), специально разрабатываемых для решения определенного круга задач.

Хотя программа и является линейной (то есть чисто текстовой), но ее визуальное отображение может иметь более сложную структуру, вплоть до целого набора представлений. При этом, каждое представление является разрезом описываемой ТКС с некой точки зрения. Например, одно представление может отображать аппаратные ресурсы согласно зонам безопасности, другое же – риски активов по их принадлежности к различным департаментам оператора ТКС.

Приведем основные требования к языку.

Во-первых, в язык должны быть встроены базовые элементы безопасности ТКС, такие как источник, уязвимость, угроза и т.д.

Во-вторых, язык должен уметь описывать причинно-следственную связь между его элементами. Например, соответствие между источниками угроз, используемыми ими уязвимостями и реализуемыми угрозами.

В-третьих, программист на данном языке должен иметь возможность описания с требуемым уровнем детализации достаточно большого количества частных Моделей реально существующих ТКС. Для этого, язык должен обладать необходимым набором возможностей.

И в-четвертых, идиомы программирования на нем должны быть приспособлены для взаимодействие с визуальным средством. Например, помимо внутренних названий, объекты могут иметь текстовое описание для отображения.

Предлагаемыми синтаксическими элементами языка и соответствующими им объектами (и действиями) в реальных ТКС являются следующие:

- Source – источник угрозы;
- Vulnerability – уязвимость;
- Threat – угроза;
- Zone – зона безопасности (как правило, определяет расположение источников угроз);
- Asset – актив ТКС (то есть то, что подвержено угрозам и должно быть защищено);
- Requirement – требование безопасности, предъявляемое к ТКС;
- Activity – мероприятие, направленное на ликвидацию источника угрозы или уязвимости (проведения которого приводит к удовлетворению соответствующего требования);
- Violation – нарушение, являющееся комплексной оценкой реализации угроз набору активов, приводимое к ущербу;
- Risk – параметр, сочетающий вероятность появления угрозы и ущерба активам от нее;
- View – представление Модели (используется визуальным средством, как описание способа отображения);
- operation «&»,«+», ... – логические действия над элементами (например, процесс использования источником угрозы (Source) уязвимости (Vulnerability) может быть описан с помощью оператора «&»);

- operation «->»– указание причинно-следственных связь между элементами (например, указание, что некий процесс («&») приводит к реализации угрозы (Threat)).

Сфера применения языке предполагает его использование специалистами по безопасности с достаточным уровнем квалификации, поэтому взятие за основу одного из профессиональных языков (таких как C++, Pascal) является более чем оправданным.

Приведем пример текстового представления гипотетической программы example.sdml на предлагаемом языке SDML.

```
Accounts: Asset{
   name = "Учетные записи";
};
UnsafeZone: Zone{
   name = "Небезопасная зона";
};
Hacker: Source{
   name = "Хакер";
   zone = UnsafeZone;
};
BugInSW: Vulnerability{
   name = "Уязвимость в ПО администрирования пользователей";
};
UnauthorizedAccessToAccounts: Threat{
   name = "Угроза несанкционированного доступа";
   asset = Accounts;
};
Hacker & BugInSW -> UnauthorizedAccessToAccounts {
   name = "'Хакер' & 'Уязвимость в ПО администрирования пользователей'\
 -> 'Угроза несанкционированного доступа'";
   description = "Хакера, используя ошибку в ПО администрирования пользователей,\
 создает угрозу несанкционированного доступа к учетным записям";
};
TopView: View{
   type = View.Top;
   description = "Общее представление модели";
};
```

В данном примере программа описывает Модель, в которой присутствует актив в виде учетных записей. При этом хакер, действующей из небезопасной зоны и использующий уязвимость в программном обеспечении, может реализовать угрозу и получить несанкционированный доступ к данному активу. После транслирования программы, она может быть отображена в визуальном

средстве. Пример такого графического представления (описываемого объектом TopView) приведен на Рисунке 1.

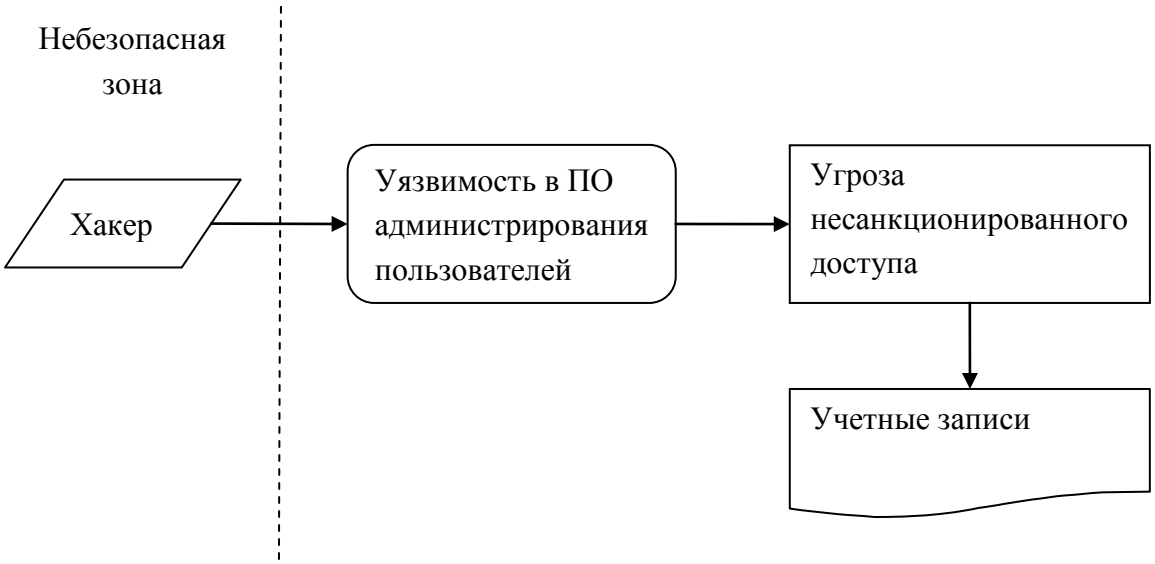

Рисунок 1. – Пример графического представления программы

Вывод

Предлагаемый язык (включая его особенности для визуализации объектов) может быть использован в качестве унифицированного средства для построения Моделей и их графического отображения, что может быть востребовано при разработке системы поддержки принятия решения. Дальнейшим же развитием языка должна стать полноценная поддержка данных и операций над ними, что позволит описывать алгоритмы Модели, такие как оценка, прогнозирование и т.п.