УДК 004.942

И.А. Офицеров, К.А.Пшеничный
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики
Санкт-Петербург
E-mail bulldozer.spb@gmail.com

ИССЛЕДОВАНИЕ ПРИМЕНИМОСТИ МЕТОДА ДИАГРАММ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ ЗАЩИТЫ ОТ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПЕРЕДАЧЕ ДАННЫХ ПО ОПТОВОЛОКОННЫМ КАНАЛАМ

Аннотация

И.А. Офицеров, К.А. Пшеничный. Исследование применимости метода диаграмм последовательностей для защиты от угроз информационной безопасности при передаче данных по оптоволоконным каналам. *Передача данных по оптоволоконным каналам в настоящее время является одним из основных видов информационного обмена. Вместе с тем, обеспечить контроль сохранности столь разветвленных и протяженных объектов не всегда представляется возможным. При их повреждении неизбежно возникают угрозы информационной безопасности пользователям этих каналов.*

Стоит отметить, что физическая целостность кабеля может быть нарушена (умышленно или случайно) в результате множества причин – например, разрывов снарядов в ходе боевых действий, землетрясения или даже падения метеорита. При этом важно отметить, что данный список заведомо неполон, поскольку невозможно учесть и классифицировать все возможные воздействия внешней среды, включая человеческий фактор. В то же время, было бы крайне желательно и полезно каким-то образом предвидеть все мыслимые угрозы, чтобы разработать универсальные рекомендации по защите от них.

Решение данной проблемы видится в формальном представлении рассматриваемого технического объекта (в данном случае, системы оптоволоконной связи) и возможных угроз его функционированию в виде модели, называемой диаграммой последовательностей.

Введение

Ценность информации зависит не только от её содержания, но и от своевременности её доставки получателю. Несвоевременность доставки информации может не только снизить её стоимость до нуля, но и нанести немалый ущерб. В связи с этим, обеспечение беспрепятственной передачи информации является очень важным аспектом информационной безопасности (далее – ИБ).

Часто причинами сбоев в передаче информации являются такие непреднамеренные угрозы, как обрыв линий связи при прокладке новых инженерных коммуникаций или при ремонте уже существующих[1]. Поэтому важно найти такой метод, который позволил бы увидеть различные возможные сценарии и выбрать определенный план действий при наступлении этой угрозы.

Решение данной проблемы видится в формальном представлении рассматриваемого технического объекта (в данном случае, системы оптоволоконной связи) и возможных угроз его функционированию в виде модели, называемой диаграммой последовательностей[2].

Насколько известно автору, диаграммы последовательностей никогда ранее не применялись для изучения угроз информационной безопасности.

Постановка задачи

Передача данных по оптоволоконным каналам в настоящее время является одним из основных видов информационного обмена[3]. Вместе с тем, обеспечить контроль сохранности столь разветвленных и протяженных объектов не всегда представляется возможным. При их повреждении неизбежно возникают угрозы

информационной безопасности пользователям этих каналов. Так, в ходе прокладки инженерных коммуникаций в посёлке Сертолово Ленинградской области РФ 8 июля 2008 года был неумышленно оборван магистральный волоконно-оптический кабель (по специальной терминологии – транк), принадлежавший провайдерам «Северо-Западный Телеком» и ООО «Икс-Трим». В результате этого без услуг связи остались абоненты этих компаний. Похожая ситуация произошла между городами Бежецк и Удомля Тверской области РФ 29 января 2009 года, когда лишились связи абоненты таких операторов связи, как RETN.net и «Билайн-Бизнес». Не пострадали клиенты тех провайдеров, которые перенаправили трафик на другие каналы, однако абоненты ряда домашних сетей, не имеющих резерва, так и остались без доступа в сеть Интернет[4].

Стоит отметить, что физическая целостность кабеля может быть нарушена (умышленно или случайно) не только при проведении земляных работ, но и в результате множества иных причин – например, разрывов снарядов в ходе боевых действий, землетрясения или даже падения метеорита. При этом важно, что данный список заведомо неполон, поскольку невозможно учесть и классифицировать все возможные воздействия внешней среды, включая человеческий фактор. В то же время, было бы крайне желательно и полезно каким-то образом предвидеть все мыслимые угрозы, чтобы разработать универсальные рекомендации по защите от них.

Моделирование ситуации

Для решения данной задачи необходимо, прежде всего, прибегнуть к словесному описанию ситуации, а затем визуализировать её. Визуализация рассмотренной ранее ситуации с обрывм транка будет проводиться путем построения модели с использованием метода диаграмм последовательностей. В качестве элементной базы модели будут использоваться графические элементы нотации моделирования бизнес-процессов (далее – BPMN)[5].

Реализация угрозы происходит следующим образом.

Экскаваторщик проводит земельные работы. Если зона проведения работ не совпадает с зоной прокладки транка, то транк не может быть поврежден в результате их проведения, следовательно, не может быть нарушена и доступность информации. Если же зона проведения работ совпадает с зоной прокладки транка, то существует вероятность того, что транк будет поврежден в результате их проведения. Например, невнимательность и спешка экскаваторщика могут привести к тому, что он случайно заденет транк ковшом экскаватора, в результате чего произойдет обрыв транка. В этом случае передача информации по транку прерывается. Таким образом, реализовывается угроза доступности информации для пользователей этого транка.

При выполнении работ в непосредственной близости от прокладки транка может быть осуществлен дополнительный контроль за их проведением. Это позволяет вовремя обнаружить пролегающий транк и не допустить его повреждение, и, как следствие, предотвратить реализацию угрозы доступности информации.

Если такой контроль не проводится, и транк повреждается, то доступность информации нарушается. Существует два пути восстановления доступности информации:

1. восстановить поврежденный транк;
2. подключиться к резервному каналу передачи информации.

Реализация первого способа требует гораздо больше времени, чем второго. Так как в течение всего этого времени информация будет оставаться недоступной, уровень негативного влияния последствия реализации угрозы в первом случае будет гораздо выше, чем во втором.

Таким образом, дальнейшее развитие ситуации возможно двумя путями:

1. если пользователь имеет доступ к резервному транку, то он, подключившись к нему, возобновляет доступность информации;
2. если у пользователя нет резервного транка, то

информация для данного пользователя остается недоступной.

При отсутствии у пользователя резервного транка остается единственный способ возобновления её доступности – отремонтировать поврежденный транк. Для этого, прежде всего, необходимо сообщить о проблеме специальной организации, занимающейся ремонтом волоконно-оптических линий связи (ВОЛС), указав в сообщении адрес поврежденного канала связи.

Организация по ремонту ВОЛС, получив сообщение о повреждении транка, прибывает по указанному адресу, проводит поиск места повреждения транка и выполняет ремонт поврежденного участка.

После проведения ремонта поврежденного участка транка доступность информации для пользователей данного транка возобновляется.

Основываясь на приведеном выше словесном описании ситуации, методе построения диаграмм последовательностей и нотации BPM, вербальная модель рассмотренной ситуации с обрывом транка и соответствующая ей субъектно-предикатная модель[6] принимают вид, показанный в приложениях 1 и 2, соответственно.

Данная диаграмма позволяет сделать вывод о том, что предотвратить подобную угрозу практически невозможно в силу случайности характера её возникновения. Однако, можно существенно снизить негативные последствия её реализации при наличии резервного канала передачи информации и своевременного подключения к нему «пострадавшего» клиента. Кроме того, при проведении земляных работ на участках, где вероятность повреждения транка при неосторожных действиях достаточно высокая, целесообразно осуществлять дополнительный контроль за их выполнением. Это позволит вовремя обнаружить пролегающий транк и не допустить его повреждение, и, как следствие, предотвратить реализацию угрозы доступности информации.

Заключение

Результаты моделирования показывают, что диаграмма

последовательностей весьма удобна для визуализации процессов. Благодаря небольшому и, вместе с тем, универсальному набору графических элементов можно легко визуализировать самые различные ситуации. Кроме того, правила применения данных элементов просты, что позволяет быстро и без особых усилий научиться строить подобные диаграммы. Диаграмма легко читается и воспринимается, а её построение не требует много времени.

На построенной модели, словно на карте, можно выделять наиболее уязвимые места, в которых возможно возникновение потенциальных угроз информационной безопасности, определять алгоритм «избегания» возникшего негативного сценария, обеспечив, таким образом, безопасное функционирование технического объекта. Это позволяет не только минимизировать негативный эффект от уже возникшей угрозы, но и вовсе предотвратить её возникновение.

Кроме того, начальное событие может быть инициировано не только, как в рассмотренной ситуации, экскаваторщиком, но и, например, разрывом снаряда, падением метеорита или воздействием на транк иных факторов, однако модель процесса, при этом, останется прежней.

Таким образом, данная модель позволяет формально представить рассмотренную информационную угрозу и применима к множеству других воздействий на транк вплоть до боевых действий или падения космических тел, если только они могут быть проявлены на территории размещения объекта.

Представляется вполне возможным, что при многократном построении диаграмм последовательностей для моделирования сценариев информационных угроз удастся выявить схожие последовательности событий или действий и, таким образом, выделить формальные типы угроз независимо от того, в каких сферах человеческой деятельности они проявляются. Далее, внутри каждого формального типа можно анализировать опыт из разных сфер деятельности, будь то логистика или банковская сфера, и с требуемым обобщением обмениваться этим опытом. Дальнейшие исследования в данном направлении позволят

подойти к формальной классификации информационных угроз и способов защиты от них.

Список литературы

1. SPBITRU. Разрыв магистральных линий - часть 4. Москва и Питер потеряли связь. [электронный ресурс]. – режим доступа: http://spbit.ru/news/n56359/, свободный [12.05.2015].

2. Wikipedia. Sequence diagram [электронный ресурс]. – режим доступа: https://en.wikipedia.org/wiki/Sequence_diagram, свободный [12.05.2015].

3. Джонсон Г., Грэхэм М. Высокоскоростная передача цифровых данных. – М.: Вильямс, 2005. – С. 136-139.

4. SPBITRU. Газификация на пути интернетизации [электронный ресурс]. – режим доступа: http://spbit.ru/news/n50981/, свободный [21.03.2015].

5. Нотация BPM. Элементы нотации BPM. [электронный ресурс]. – режим доступа: http://www.elma-bpm.ru/bpmn2/7_2.html#7_2, свободный [21.03.2015].

6. Pshenichny, C.A., and Mouromtsev, D.I., 2015. Grammar of Dynamic Knowledge for Collaborative Knowledge Engineering and Representation. In: Diviacco, P., Fox, P., Pshenichny, C., Leadbetter, A. (Eds): Collaborative Knowledge in Scientific Research Networks, IGI Global, pp 323-354.