МОДЕЛЬ ПРОГНОЗИРОВАНИЯ УГРОЗ ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ НА БАЗЕ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ

Израилов К.Е.

Введение.

Современный мир не может существовать без обмена информацией людей, находящихся на расстоянии друг от друга. Для обеспечения такой возможности предназначены телекоммуникационных систем (далее ТКС). Информация иметь определенную ценность, что приводит к необходимости выявления и устранения угроз, реализация которых может привезти к искажению, потере или компрометации передаваемых данных. Расчет вероятностных характеристик возникновения угроз позволяет с этой позиции оценить конкретную ТКС и принять соответствующие защитные меры. Оценку необходимо производить как на этапе проектирования и реализации ТКС, так и при ее эксплуатации. Это позволит уменьшить вероятность возникновения изначально и провести экстренные мероприятия по устранению угроз в случае их появления. Для такой оценки используются специальные модели угроз (далее Модели), учитывающие специфику конкретной ТКС, ее внешние и внутренние параметры. Классические Модели, имеющие широкое распространение, слишком упрощенно представляют современные ТКС. Их основной целью является расчет именно вероятностных характеристик угроз в конкретном состояния ТКС, не учитывая предпосылки к возникновению в будущем – то есть в них отсутствует элемент прогнозирования. Предлагается подход к прогнозированию угроз, использующий Модель, построенную на базе искусственной нейронной сети и несколько отличный от классического способа оценки возникновения угроз.

Классическая модель.

Классическая Модель построена в предположении что в любой ТКС существуют такие элементы безопасности, как: угроза ТКС (далее – Угроза), источник Угроз (далее – Источник), уязвимость ТКС (далее – Уязвимость) и защитные меры

(далее – Меры). Взаимосвязь между элементами с точки зрения механизма реализации Угроз показана на рис. 1.

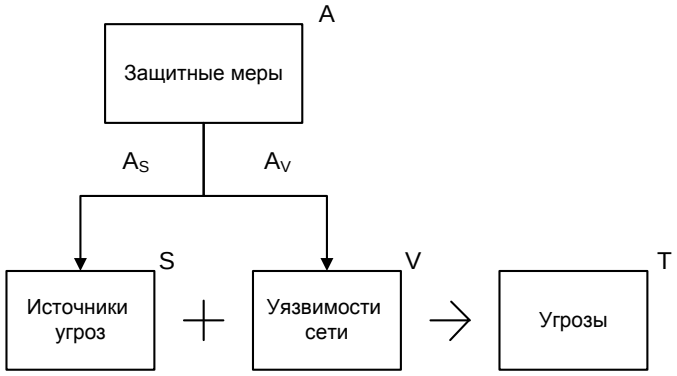

Рисунок 1 – Классическая модель реализации угроз

Источники, используя Уязвимости, приводят к реализации Угроз. Для устранения Угроз применяются Меры по минимизации Источников и Уязвимостей. При этом наличие Источников без используемых Уязвимостей, равно как и Уязвимостей без Источников однозначно приводит к отсутствию Угроз. Таким образом, как Источник, так и Уязвимость можно считать множеством предпосылок к возникновению Угроз, хотя их наличие по отдельности и не означает наличие последних. Переводя описание взаимодействий в математическую плоскость и сопоставляя каждому элементу соответствующее множество (буквенные обозначения множеств приведены на рис. 1), возникновение Угроз можно записать следующей логической формулой:

$$(S \ \& \ !A_S) \ \& \ (V \ \& \ !A_V) \rightarrow T, \qquad (1)$$

где символ '!' означает отрицание (то есть любое множество, не пересекающееся с данным), символ '&' – логическую операцию 'И' над множествами (то есть пересечение двух множеств), а '->' означает соответствие элементов множеств (то есть наличие элементов одного множества приводит к возникновению элементов другого).

Проблемы классической модели.

Хотя данная Модель и является часто используемой, она обладает рядом следующих недостатков. Модель использует грубые и не однотипные формы

Источников и Уязвимостей. Она не учитывает возможность возникновение новых внутренних Источников в результате реализации Угроз (например, угроза компрометации данных доступа в ТКС может привезти к новому Источнику – несанкционированному доступу персонала ТКС). Наличие Уязвимости при отсутствии данных об Источнике, который может ей воспользоваться, согласно Модели приведет к отсутствии Угрозы, хотя сам факт наличия критичной Уязвимости целесообразно учитывать в качестве предпосылки к Угрозе (ведь возможно, что хотя инцидентов, связанных с Источником и не было, тем не менее в реальности он гипотетически существует). Это позволит разработать и принять Меры еще до момента первой реализации Угрозы. Суть механизма оценки посредством классической Модели согласно формуле (1) заключается в нахождении пересечения множеств, что приводит к получению достаточно грубых и зачастую слишком очевидных результатов. При этом расчет исходных множеств Источников, Уязвимостей и Мер является трудоемкой и плохо формализуемой задачей.

Закон причинности.

Прежде чем перейти от классической Модели к новой, призванной избавиться от перечисленных недостатков, приведем один из наиболее надежных научных законов – «Закон причинности», говорящий о том, что любое явление имеет причину и является ее следствием. А первопричина в этой цепочке выходит за пределы рассматриваемого мира и имеет собственный смысл.

Применение закона причинности к классической модели.

Рассмотрим классическую Модель с позиции «Закона причинности». Как указывалось ранее, Источник является инициатором действий, ведущих к возникновению Угрозы. Следовательно, одной из причин Угрозы является Источник. Поскольку существование Угрозы без каких либо последствий лишено смысла, то сама реализация Угрозы является Источником дальнейших враждебных действия. Следовательно, причиной появления Источника является

реализация Угрозы. Таким образом, Источники (при наличии используемых им Уязвимостей) и Угрозы связанны между собой в бесконечную причинно-следственную цепочку. Полученные выводы отображены на рис. 2.

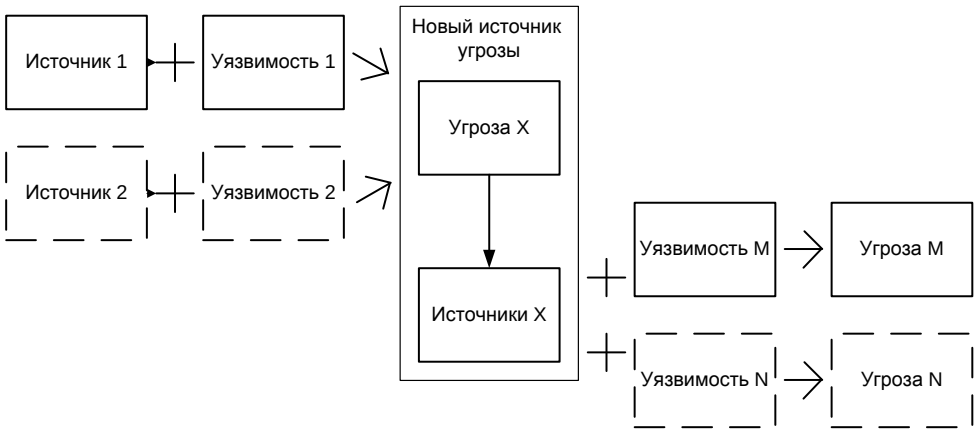

Рисунок 1 – Причинно-следственная связь источников и угроз

В общем случае, одна Угроза может иметь несколько Источников, использующих различные Уязвимости и имеющих разное влияние на ее реализацию. Аналогично, один Источник может приводить к различным Угрозам. Такие случаи показаны на рис. 2 пунктирной линией.

Уязвимости.

Уязвимость характеризует возможность, используя которую могут быть реализованы Угрозы. То есть, наличие Уязвимости само по себе является одной из причин возникновения Угроз. Следовательно, с точки зрения предпосылок к Угрозе, Источник и Уязвимость являются подобными – Угроза не может быть реализована как без Источника, так и без Уязвимости. Далее для упрощения будем считать Уязвимость тождественным Источнику условием реализации Угрозы и в контексте новой Модели называть термином – Предпосылка.

Новая модель.

Применение «Закон причинности» к классической Модели приводит к альтернативному подходу в рассмотрении процесса возникновения Угроз, что позволяет говорить и о новой Модели. Согласно этому подходу набор Предпосылок приводит к реализации Угроз, каждая из которых, в свою очередь,

означает возникновение новой Предпосылки. Будем считать Угрозу и порождаемую ею Предпосылку одним логическим элементом – новым источником предпосылок (НИП). Таким образом, логическая связь между Предпосылками и Угрозами описывается ориентированным графом, узлами которого являются НИП, а ребрами – следственные связи между Предпосылками и Угрозами соответствующих НИП. Такое представление используется в новой Модели.

Для отсечения бесконечных ветвей графа в сторону причин Предпосылок и следствий Угроз будем считать, что существуют начальные Предпосылки (не имеют первопричин и являются исходными данными Модели) и конечные Угрозы (не имеющие следствий и являющиеся результатом применения Модели). Отметим, что с этой позиции классическая Модель состоит только из начальных Источников и конечных Угроз, а связи между ними строятся лишь с помощью Уязвимостей.

Аналог с нейронной сетью. Нервная система с возбуждениями.

Предложенная Модель достаточно хорошо коррелирует с распространенной моделью искусственной нейронной сети (далее ИНС) с точки зрения предназначения, структуры, логики элементов и связей. ИНС является математической моделью, построенной по принципу организации и функционирования биологических нейронных сетей. Она состоит из соединенных и взаимодействующих простых процессоров – искусственных нейронов. Каждый нейрон способен получать сигналы от одних нейронов, обрабатывать их, возбуждаться и посылать новый сигнал другим. Начальные Предпосылки предлагаемой Модели с точки зрения ИНС являются входным возбуждением ИНС, а конечные Угрозы – ее выходной реакцией. НИП с точки зрения ИНС подобны нейронам, реагирующим на возбуждения (Предпосылки) и передаваемым возбуждения далее (создавая Угрозы). Для подтверждения этой аналогии на рис. 3 приведена модель нейрона ИНС.

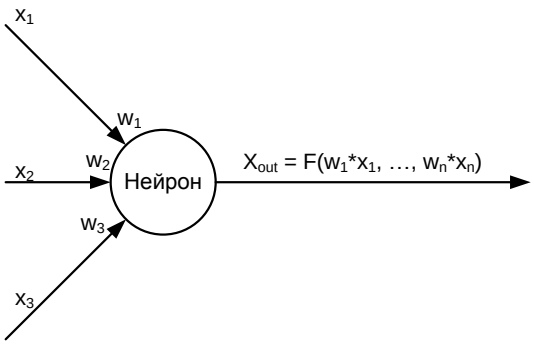

Рисунок 3 – Модель нейрона

Согласно рис. 4, нейрон представляет собой узел сети, имеющий множество входов со значениями $\{x_1, x_2, x_3\}$, множество внутренних весов $\{w_1, w_2, w_3\}$ и выход со значением X_{out}, вычисляемый с помощью функции F() по комбинации взвешенных значений x_n и w_n. Функция F() отражает чувствительность нейрона к возбуждению и в новой Модели описывает механизм возникновение НИП.

Будучи соединенные в сложную систему нейроны вместе способны выполнять задачи по распознаванием образов, что в контексте новой Модели соответствует выявление картины конечных Угроз по имеющимся начальным Предпосылкам.

Исходя из подобия приведенных моделей, целесообразно применять расчетные методы одной (ИНС) при использовании другой (новой Модели). Отметим важное отличие новой Модели от классической с точки зрения подхода к оценке Угроз. Согласно формуле (1), для ненулевой вероятности возникновения Угрозы обязательно наличие как Источников, так и Уязвимостей. То есть, какой бы «крупной» не была Уязвимость (множества V имеет большое количество элементов), в случае отсутствия Источника (множество S является пустым) считается, что Угроза не может быть реализована (множество T является пустым). В новой Модели Источники и Уязвимости тождественны и наличие хотя бы одного из них является Предпосылкой к Угрозе. То есть, классическая Модель предназначена для оценки вероятностных характеристик возникновения Угроз, а новая – для их прогнозирования.

Защитные меры в новой модели.

Введем понятие и учет Мер в новую Модель. Их назначением является минимизация Источников и Уязвимостей. Следовательно, наличие Мер в новой Модели тождественно отсутствию Предпосылок. Входные данные Модели характеризуют начальные Предпосылки, тогда учет Мер можно ввести путем задания их противоположных значений. Отметим, что для части начальных Предпосылок не существует Мер, и для конкретной ТКС они являются независимыми внешними факторами. Новая Модель с учетом введенных Мер имеет вид, представленный на рисунке 4.

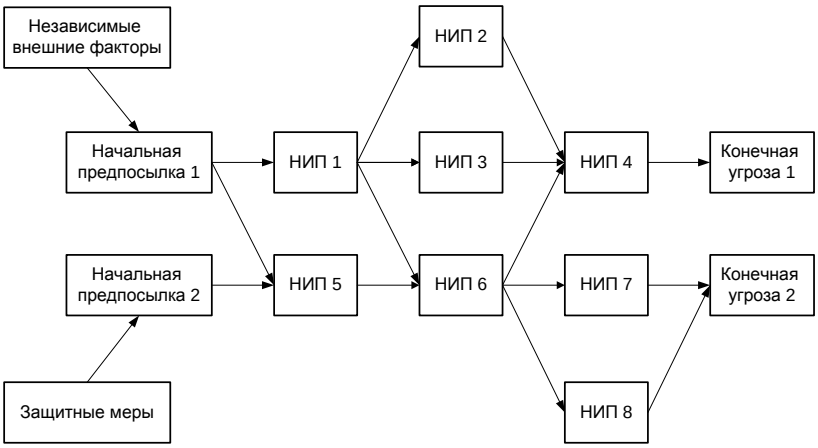

Рисунок 4 – Модель прогнозирования угроз

Расчет параметров Модели.

Расчет параметров новой Модели (весов и функций), как и способ построения ее графа, соответствует решению аналогичных задач для ИНС и выходит за рамки данной статьи. Отметим, что для расчета весов Модели применяется метод обучения ИНС, заключающийся в подстройке параметров по заданным входным и выходным данным. Это позволяет использовать для обучения, помимо теоретических основ безопасности ТКС, реально применяемый и формализованный успешный опыт борьбы с Угрозами («Лучшие практики»), использование которого с трудом поддерживается классическими Моделями.

Выводы.

Предложенная модель прогнозирования угроз ТКС по сравнению классическими имеет такие преимущества, как усовершенствованная причинно-следственная логика взаимодействия объектов безопасности, более точное представление современных ТКС, возможность учета «Лучших практик» борьбы с Угрозами, что позволяет говорить о целесообразности ее использования.