РАЗРАБОТКА МАТЕМАТИЧЕСКОЙ МОДЕЛИ ДОВЕРИЯ

С. С. Яковлев, П. К. Шиверов

Самарский национальный исследовательский университет им. академ. С. П. Королева

Введение

Безопасность информационных систем тесно связана с понятием, которое мы называем доверие.

Зародилось это слово в древней Руси, как производное от слов «вера» и «вероятный». Слово «вера» означало «убежденность в чем-либо». Слово же «вероятный» было получено от древнерусского и старославянского сочетания «принять веру» и означало «позволяющий поверить или достойный доверия». Следовательно, сначала мы верим объекту: убеждаем себя в том, что он будет следовать правилам, которые мы предварительно обсудили, и только потом начинаем доверять.

Согласно словарю по социальной психологии под редакцией М. Ю. Кондратьева, доверие – это специфическое отношение субъекта к определенным объектам, связанным с ситуативной, актуальной значимостью и априорной надежностью (безопасностью) объекта для субъекта [1].

В наше время трудно представить функционирование любой компании, фирмы или системы без доверительных отношений. Если бы их не было, то заключение сделок стало бы огромным риском для обеих сторон, что в итоге привело бы к взаимному недоверию, несоблюдению правил соглашения и, следовательно, к расторжению договора.

В связи с этим разработка способа вычисления уровня доверия к объекту становится особо актуальной.

1. Информационная безопасность и доверие

Понятие доверия является одним из главных аспектов в информационной безопасности. При использовании цифровых подписей и в процедуре аутентификации необходимо быть уверенным в том, что подпись или какой-либо другой критерий, удостоверяющий личность, используется именно тем человеком, кому он принадлежит. С этой проблемой справляются Удостоверяющие Центры (УЦ), которые формируют цифровые сертификаты подчиненных центров сертификации и конечных пользователей. Инфраструктура открытых ключей(*PKI – Public Key Infrastructure*) – набор средств (технических, материальных, человеческих и т. д.), распределенных служб и компонентов, в совокупности используемых для поддержки криптографических задач на основе закрытого и открытого ключей [2].

Одним из важных компонентов инфраструктуры открытых ключей является использование криптографической системы с открытым ключом. В ее основе лежит несколько принципов:

1) удостоверяющий центр создает сертификат открытого ключа, тем самым, сертифицируя его;

2) пользователи не доверяют друг другу, но должны доверять удостоверяющему центру;

3) удостоверяющий центр может или подтвердить или опровергнуть принадлежность открытого ключа данному лицу, которое соответственно владеет закрытым ключом;

4) закрытый ключ должен быть известен только его владельцу[3].

Как видно, *PKI* является системой, где главенствующую роль занимает удостоверяющий центр и пользователи общаются друг с другом непосредственно через него. Так как *PKI* является стержневым понятием в современной криптографии, поэтому нельзя оставить без внимания и понятие доверия.

2. Доверие и принципы его построения

В системах, построенных на доверии, существует риск быть обманутым субъектом, с которым объект вступил в доверительные отношения. Следовательно, чем выше вероятность передачи данных третьим лицам, тем выше риск начала отношений с данным объектом – тем меньше к ним доверия.

Далее рассмотрим ситуацию, в которой вы разговариваете с объектом по сотовому телефону, у которого шанс перехвата информации, передающейся по данному каналу связи, высок. А теперь рассмотрим другую ситуацию, в которой вы обмениваетесь данными со своим собеседником через защищенный квантовый канал связи. Какому способу передачи вы бы доверились, если информация, которой необходимо обменяться, не должна попасть в руки третьих лиц? Определенно второму. Из этого следует, что чем выше безопасность использования какого-либо канала связи, тем выше к нему доверие, как к среде распространения информации.

Так как доверие основано на нашем прошлом опыте, на том, что данный объект не дискредитировал себя ранее, то это поддерживает в нас уверенность, что он будет соответствовать нашим ожиданиям в будущем. Вследствие того, что наша система представляет из себя комплексный объект, то необходимо учитывать ситуации, которые происходили с каждым отдельным элементом системы. В связи с этим введем статистику положительных результатов запуска каждого элемента системы и обозначим это понятием преддоверия или, по-другому, репутации элемента.

Из всего вышесказанного следует, что доверие можно считать совокупностью таких факторов, как риск, преддоверие и канал передачи информации. А теперь разберем более подробно каждую из этих переменных.

2.1. Оценки рисков и угроз в информационных системах

Риск – это сочетание потенциальной угрозы и потенциальной уязвимости.

Угроза – это совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности, конфиденциальности информации.

Уязвимость – это слабость в системе защиты, которая делает возможной реализацию угрозы.

Оценка рисков – это выявление угроз, определение вероятности реализации этих угроз и их возможных последствий.

Степень риска – это возможность наступления каких-либо последствий при реализации угрозы. Существует 3 степени риска:

1) допустимая – существует невысокая вероятность проявления угрозы. По возможности необходимо предпринять действия по устранению уязвимого места, но их стоимость не должна превышать размер прибыли от реализации проекта;

2) критическая – существует реальная возможность осуществления такого события, при котором ущерб может превысить размер прибыли;

3) катастрофическая – уязвимость представляет собой реальную угрозу для системы, при которой возможны потеря капитала и имущества руководителя предприятия.

Количественный анализ – численное определение величин отдельных рисков и угроз для проекта в целом.

Отметим, что стоит обратить внимание на описание методов количественного анализа информационного риска в связи с их многочисленностью.

В абсолютном выражении риск может определяться величиной возможных потерь в материально-вещественном (физическом) или стоимостном (денежном) выражении.

В относительном выражении риск определяется как размер возможных потерь, отнесенный к некоторой базе, в виде которой наиболее удобно принимать либо имущественное состояние предприятия, либо общие затраты ресурсов на данный вид предпринимательской деятельности, либо ожидаемый доход (прибыль). В таком случае потерями можно считать отклонение от ожидаемого результата в сторону снижения прибыли.

Предпринимательские потери – это случайное снижение предпринимательского дохода. Степень риска характеризуется размером таких потерь.

Таким образом, размер вероятных потерь можно разделить на 3 группы:

1) потери, размер которых не превышает или равен прибыли предприятия;

2) потери, размер которых превышает прибыль предприятия. В таком случае предпринимателю придется выплачивать оплачивать убытки из своих собственных средств;

3) потери, размер которых превышают капитал всего предприятия и имущества предпринимателя.

Если есть возможность оценить или проанализировать возможные потери от данного мероприятия, то это означает, что получена количественная оценка риска. Если разделить абсолютную величину возможных потерь на расчетный показатель затрат или прибыли, то получим количественную оценку риска в процентном соотношении.

Риск измеряется величиной вероятных потерь, следовательно необходимо учитывать случайный характер таких потерь. Можно определить вероятность наступления таких потерь объективным и субъективным методом. Объективным методом пользуются для определения вероятности наступления события на основе исчисления частоты, с которой происходит данное событие.

В свою очередь, субъективный метод основывается на использовании субъективных критериев, основанных на предположениях: оценка экспертов, мнение оценивающего либо его личный опыт в изучении данной проблемы.

Из этого следует, что оценка финансовых рисков предприятия зависит от вероятности возникновения угрозы и размеров потерь при ее реализации. Эта зависимость находит выражение в строящейся кривой вероятностей возникновения определенного уровня потерь.

Построение кривой требует от специалистов, занимающихся анализом информационных рисков большого багажа знаний, связанных с прогнозированием угроз. Существует множество способов создания данной кривой: статистический; анализ целесообразности затрат; метод экспертных оценок; аналитический способ; метод аналогий. Среди этих способов следует выделить два важных: метод экспертных оценок и аналитический способ.

Итогом работы метода экспертных оценок является результат анализа информации, поступающей от экспертов и специалистов, в процессе анализа собирается и анализируется вероятность возникновения различных уровней потерь. Оценки специалистов и экспертов базируются на учете всех возможных факторов финансового риска и статистических данных. Одним из нюансов использования данного метода является то, что в случае небольшого количества уровня оценок, усложняется процесс реализации способа.

Самым сложным способом построения кривой является аналитический метод, так как в процессе анализа используются элементы теории игр.

Для обеспечения защиты информации в определенных информационных системах (ИС) необходимо более конкретное рассмотрение составляющих ИС, расчеты и т. д.

С целью получения результата в виде формулы оценки риска, необходимо выполнить несколько шагов:

1) ввести определения и понятия для оценки рисков в ИС;

2) определить значимость угрозы информации, чтобы оценить их влияние на величину, которая определяет степень риска;

3) вывести конечную формулу, которая оценивает степень риска в системе.

Стоимость информации (*S*). Любая информация, которая представляет для компании какую-либо ценность, подразделяется на блоки, каждый из которых варьируется по степени значимости от 0 до 1. Но ни один блок не имеет значимость равную 1, максимальным является значение, стремящееся к 1.

Вероятность реализации атаки (*P*) является понятием, которое зависит от уровня безопасности системы защиты объекта и всех способов несанкционированного получения информации с данного элемента системы третьими лицами.

Чем выше ценность используемой информации на данном предприятии, тем выше вероятность атаки правонарушителей на данную систему. При получении таких данных злоумышленниками ставится под угрозу существование всей этой системы в целом. Следовательно, такая информация будет задавать цену всей системе, поэтому в формуле будем использовать $S_{\max}$, которое будет обозначать максимальную стоимость блока информации, используемого на предприятии. И чем выше стоимость информации, используемой на предприятии, тем выше вероятность атаки на элемент, содержащий такие данные.Поэтому будем использовать в формуле величину $P_{\max}$, которая будет обозначать максимальную вероятность атаки на конкретный элемент СЗИ(Система Защиты Информации), где значение этой вероятности будет также варьироваться от 0 до значения близкому к 1.

В экономике используется формула VaR (Value At Risk – стоимостная мера риска), которая выражается, как

$$R = L \cdot P, \qquad (1)$$

где R – это риск; L – это количество потерянных денег или жертв в результате одного нежелательного события; P – это вероятность одного нежелательного события.

Обозначим в нашей формуле за L такое потенциальное количество денежных средств, которые мы можем потерять в результате успешной атаки на нашу СЗИ ($S_{\max}$). Вместо P будем использовать максимальную вероятность атаки($P_{\max}$) на определенный элемент системы.

В результате данных рассуждений получаем формулу оценки рисков ИС в виде:

$$R = S_{\max} \cdot P_{\max} \qquad (2)$$

Из вышесказанного следует, что чем выше риск при использовании системы, тем выше вероятность доступа третьих лиц к хранящимся в этой системе данным, следовательно, тем меньше к ней доверия.

2.2. Оценка свойств канала связи

Следующей переменной является характеристика канала среды, в которой передается информация. У каждого канала передачи имеются свои минусы и плюсы, что сказывается на доверии к этому каналу передачи. К примеру, у сетей Ethernet существует высокий риск взлома канала, в отличие от оптоволоконных сетей передачи, в которых безопасность передачи информации выше, и, следовательно, уровень доверия к этой среде тоже.

На данный момент существует несколько типов каналов распространения информации:

1) беспроводные сети передачи данных: *Wi-Fi*, *WiMAX*, 3*G* и т. д. Слабозащищенные сети, высокая вероятность взлома, отследить перехват проблематично;

2) кабельные сети передачи данных (витая пара, коаксиальный кабель). Так же может быть совершен взлом канала передачи, но возможно зафиксировать перехват;

3) оптоволоконные сети передачи данных. Перехватить информацию тяжело, зафиксировать перехват возможно [5];

4) квантовые сети передачи данных. При попытке перехвата информации канал разрушается [6].

Из всего вышесказанного введем переменную (X_i), которая будет обозначать коэффициент безопасности передачи информации по каналам связи.

2.3. Понятие преддоверия в информационной системе

Предсказуемость информации – это способность исследуемого объекта при проведении исследований в конце каждого опыта выдавать позитивный результат. Технология работы *PKI* построена на предсказуемости, так как никто не знает: дойдет ли сообщение до нужного адресата, по этой причине все полагаются на удостоверяющий центр.

Неопределенность – отсутствие или недостаток информации для принятия какого-либо решения. Чем выше предсказуемость и ниже неопределенность, тем выше доверие к объекту СЗИ.

Расчет преддоверия к системе

Для примера представим способ, по которому высчитывается безотказность работы какой-либо системы. Берется статистика, в которой имеется количество успешных запусков системы (l), имеющих значение равное 1, и количество неудачных запусков (k), значение которых равно 0, и делится на общее количество запусков (m), таким образом, находится статистическая вероятность успешного запуска системы.

Используем такой же способ вычисления, что и для предыдущего примера, для нашей формулы. Рассмотрим такой способ передачи данных. A – это источник, B – это приемник и K_{AB} – это ключ. Исходя из предыдущих рассуждений, преддоверие системы будет высчитываться таким образом:

$$PD = \frac{\sum_{1}^{m} q_i}{m} \quad (3)$$

Далее необходимо посчитать преддоверие к каждому указанному ранее элементу, то есть к источнику (A), приемнику (B) и ключу (K_{AB}). Делается это по формуле указанной ранее. После этого мы суммируем значения преддоверия каждого элемента и делим на количество запусков (m), для нахождения преддоверие ко всей рассматриваемой системе. Таким образом, мы сможем высчитать коэффициент, обозначающий насколько хорошо элементы системы оправдывали наши ожидания в прошлом.

2.4. Математическая модель доверия

Из ранее сказанного следует то, что:

- во-первых, доверие (D_i) обратно пропорционально риску (R);
- во-вторых, доверие к элементу СЗИ, должно быть пропорционально преддоверию участника (PD), так как если элемент себя ни разу не скомпрометировал, то и доверие к нему будет высокое;
- в-третьих, доверие к участнику, который организовал обмен информации, через канал передачи данных (X_i), будет зависеть от коэффициента безопасности используемого канала связи, поэтому, чем выше коэффициент безопасности, тем выше доверие к среде передачи. Следовательно, доверие будет пропорционально данному коэффициенту.

В итоге математическая формула расчета доверия принимает такой вид:

$$D_i = \frac{PD \cdot X_i}{R} \quad (4)$$

Исходя из проведенной работы, можно сделать вывод, что в нынешних условиях каждый параметр формулы играет важную роль для построения математической модели доверия.

Литература

1. Социальная психология // Словарь под ред. М. Ю. Кондратьева [Электронный ресурс] – Режим доступа: http://www.insai.ru/slovar/2160/свободный – Яз., рус. – Загл с экрана.

2. Черемушкин А. В. Криптографические протоколы: основные свойства и уязвимости [Текст] / А. В. Черемушкин // Прикладная дискретная математика. – 2009. № 2. С. 14–25.

3. Инфраструктура открытых ключей [Электронный ресурс] – Режим доступа: https://infotecs.ru/solutions/pki/свободный – Яз., рус. – Загл с экрана.

4. Способы оценки степени риска [Электронный ресурс] – Режим доступа: http://www.askins.ru/index.php/methods/свободный – Яз., рус. – Загл с экрана.

5. Среда и методы передачи данных в вычислительных сетях – Режим доступа: http://www.lessons-tva.info/edu/telecom-loc/m1t2_2loc.html/свободный – Яз., рус. – Загл с экрана.

6. Квантовая криптография [Электронный ресурс] – Режим доступа: http://www.natural-sciences.ru/ru/article/view?id=30414/свободный – Яз., рус. – Загл с экрана.