УДК 004.056 **Егоров Ф.И.**

ОЦЕНКА УЯЗВИМОСТИ ИНФОРМАЦИИ В СЕТЯХ СВЯЗИ

Введение

Одной из первоочередных задач, предшествующих оценке безопасности конфиденциальной связи, является задача оценки уязвимости информации. Для исследования и практического решения задач по защите информации необходимы показатели, которые характеризуют наиболее неблагоприятные ситуации с точки зрения уязвимости информации. Ими являются самый уязвимый структурный компонент сети связи (СС), самый опасный дестабилизирующий фактор, самый ненадежный элемент защиты, самый опасный потенциальный нарушитель, самая важная информация.

Большое значение для оценки защищенности и уязвимости имеет временной интервал, относительно которого оценивается защищенность. Несмотря на то, что время является категорией сугубо непрерывной, для рассматриваемых здесь целей его как параметр защищенности можно структурировать, выделив интервалы для анализа и оценки уровня защищенности или уязвимости информации.

Основная часть

Уязвимость информации есть событие, возникающее как результат такого стечения обстоятельств, когда в силу каких-то причин используемые в автоматизированных системах обработки данных средства защиты не в состоянии оказать достаточного противодействия проявлению дестабилизирующих факторам и нежелательного их воздействия на защищаемую информацию. Модель уязвимости информации в сетях связи в общем виде показана на рис.1.

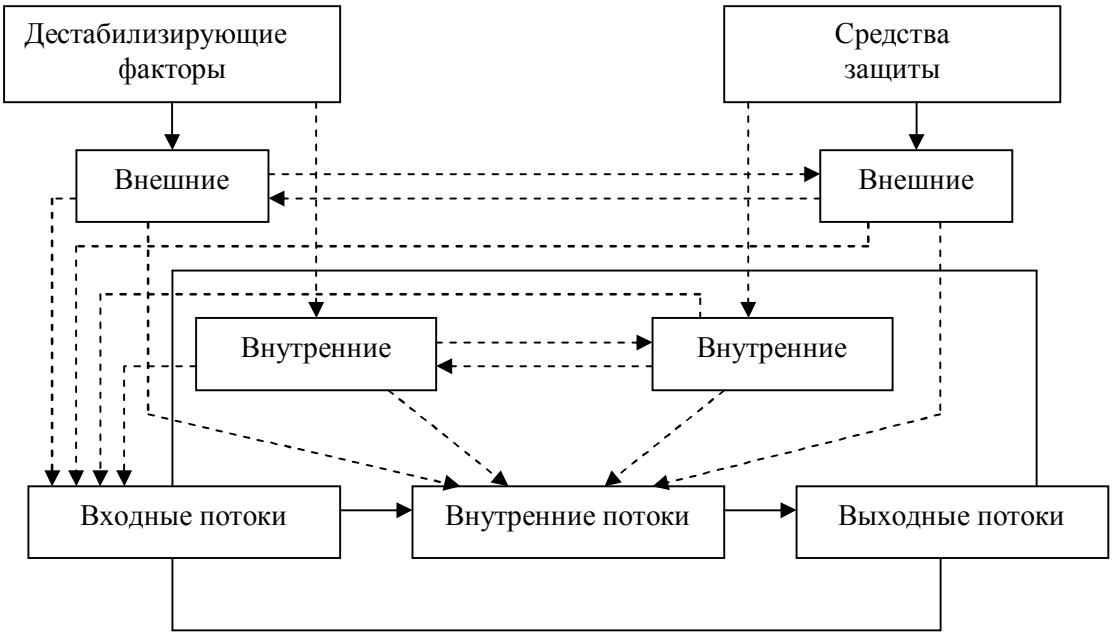

Рис.1. Общая модель воздействия на информацию

Данная модель детализируется при изучении конкретных видов уязвимости информации: нарушения физической или логической целостности, несанкционированной модификации, несанкционированного получения, несанкционированного размножения.

При детализации общей модели основное внимание акцентируется на том, что подавляющее большинство нарушении физической целостности информации имеет место в процессе её обработки на различных участках технологических маршрутов. При этом целостность информации зависит не только от процессов, происходящих на объекте, но и от целостности информации, поступающей на его вход. Основную опасность представляют случайные дестабилизирующие факторы (отказы, сбои и ошибки компонентов автоматизированных систем обработки данных), которые потенциально могут проявиться в любое время, и в этом отношении можно говорить о регулярном потоке этих факторов. Из стихийных бедствий наибольшую опасность представляют пожары, опасность которых в большей или меньшей степени также является постоянной. Опасность побочных явлений практически может быть сведена к нулю путем надлежащего выбора места для помещений автоматизированной системы обработки данных и их оборудования. Что касается злоумышленных действий, то они связаны главным образом с несанкционированным доступом к ресурсам автоматизированной системы обработки данных. При этом наибольшую опасность представляет занесение вирусов.

В соответствии с изложенным общая модель процесса нарушения физической целостности информации на объекте автоматизированной системы обработки данных представлена на рис. 2.

С точки зрения несанкционированного получения информации принципиально важным является то обстоятельство, что в современных автоматизированных системах обработки данных оно возможно не только путем непосредственного доступа к базам данных, но и многими путями, не требующими такого доступа. При этом основную опасность представляют злоумышленные действия людей. Воздействие случайных факторов непосредственно не ведет к несанкционированному получению информации, оно лишь способствует появлению каналов несанкционированного получения информации, которыми может воспользоваться злоумышленник.

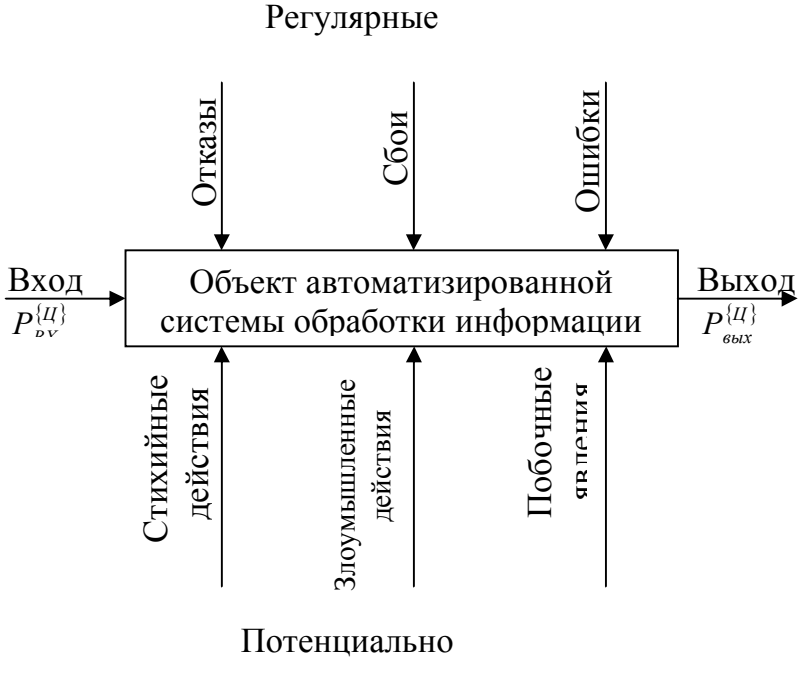

Рис. 2. Общая модель процесса нарушения физической целостности информации

Рассмотрим далее трансформацию общей модели уязвимости с точки зрения несанкционированного размножения информации. Принципиальными особенностями этого процесса являются:

• любое несанкционированное размножение есть злоумышленное действие;

• несанкционированное размножение может осуществляться в организациях-разработчиках компонентов автоматизированной системы обработки данных, непосредственно в автоматизированной системе обработки данных и сторонних организациях, причем последние могут получать носитель, с которого делается попытка снять копию как законным, так и незаконным путем.

Попытки несанкционированного размножения информации у разработчика и в автоматизированной системе обработки данных есть один из видов злоумышленных действий с целью несанкционированной) ее получения и поэтому имитируются приведенной моделью. Если же носитель с защищаемой информацией каким-либо путем (законным или незаконным) попал в стороннюю организацию, то для его несанкционированного копирования могут использоваться любые средства и методы, включая и такие, которые носят характер научных исследований и опытно-конструкторских разработок.

Как правило, модели позволяют определять текущие и прогнозировать будущие значения всех показателей уязвимости информации для любых компонентов автоматизированной системы обработки данных, любой их комбинации и для любых условий жизнедеятельности автоматизированной системы обработки данных. Некоторые замечания по использованию.

1. Практически все модели строятся в предположении независимости тех случайных событий, совокупности которых образуют сложные процессы защиты информации в современных автоматизированных системах обработки данных.

2. Для обеспечения работы моделей необходимы большие объемы таких исходных данных, подавляющее большинство которых в настоящее время отсутствует, а формирование сопряжено с большими трудностями.

Определим замечание первое - допущение независимости случайных событий, происходящих в системах защиты информации. Основными событиями, имитируемыми в моделях определения показателей уязвимости, являются: проявление дестабилизирующих факторов, воздействие проявившихся дестабилизирующих факторов на защищаемую информацию и воздействие используемых средств защиты на дестабилизирующие факторы. При этом обычно делаются следующие допущения.

1. Потенциальные возможности проявления каждого дестабилизирующего фактора не зависят от проявления других.

2. Каждый из злоумышленников действует независимо от других, т. е. не учитываются возможности формирования коалиции злоумышленников.

3. Негативное воздействие на информацию каждого из проявившихся дестабилизирующих факторов не зависит от такого же воздействия других проявившихся факторов.

4. Негативное воздействие дестабилизирующих факторов на информацию в одном каком-либо компоненте автоматизированной системы обработки данных может привести лишь к поступлению на входы связанных с ним компонентов информации с нарушенной защищенностью и не оказывает влияния на такое же воздействие на информацию в самих этих компонентах.

5. Каждое из используемых средств защиты оказывает нейтрализующее воздействие на дестабилизирующие факторы и восстанавливающее воздействие на информацию независимо от такого же воздействия других.

6. Благоприятное воздействие средств защиты в одном компоненте автоматизированной системы обработки данных лишь снижает вероятность поступления на

входы связанных с ним компонентов информации с нарушенной защищенностью и не влияет на уровень защищенности информация в самих этих компонентах.

В действительности же события, перечисленные выше являются зависимыми, хотя степень зависимости различна: от незначительной, которой вполне можно пренебречь, до существенной, которую следует учитывать. Однако для решения данной задачи в настоящее время нет необходимых предпосылок, поэтому остаются лишь методы экспертных оценок.

Второе замечание касается обеспечения моделей необходимыми исходными данными. Ранее уже неоднократно отмечалось, что для практическою использования моделей определения показателей уязвимости необходимы большие объемы разнообразных данных, причем подавляющее большинство из них в настоящее время отсутствует.

Сформулируем теперь рекомендации по использованию моделей, разработанных в рамках рассмотренных ранее допущений, имея в виду, что это использование, обеспечивая решение задач анализа, синтеза и управления в системах защиты информации, не должно приводить к существенным погрешностям.

Первая и основная рекомендация сводится к тому, что моделями должны пользоваться квалифицированные специалисты-профессионалы в области защиты информации, которые могли бы в каждой конкретной ситуации выбрать наиболее эффективную модель и критически оценить степень адекватности получаемых решении.

Вторая рекомендация заключается в том, что модели надо использовать не просто для получения конкретных значений показателей уязвимости, а для оценки поведения этих значений при варьировании существенно значимыми исходными данными в возможных диапазонах их изменений. В этом плане модели определения значений показателей уязвимости могут служить весьма ценным инструментом при проведении деловых игр по защите информации.

Третья рекомендация сводится к тому, что для оценки адекватности моделей, исходных данных и получаемых решений надо возможно шире привлекать квалифицированных и опытных экспертов.

Четвертая рекомендация заключается в том, что для эффективною использования моделей надо непрерывно проявлять заботу об исходных данных, необходимых для обеспечения моделей при решении задач защиты. Существенно важным при этом является то обстоятельство, что подавляющее количество исходных данных обладает высокой степенью неопределенности. Поэтому надо не просто формировать необходимые данные, а перманентно их оценивать и уточнять.

Выводы

Разработана модель уязвимости информации в сетях связи в общем виде. Она детализируется при изучении конкретных видов уязвимости информации, которые основываются на базе сформулированных замечаний по их использованию. Причем они сформулированы с учетом допущений, которые позволяют решение задач анализа, синтеза и управления в системах защиты сетей связи, но не должны приводить к существенным погрешностям.

Поступила 27.01.2010