Узбекское агентство связи и информатизации
Ташкентский университет информационных технологий

На правах рукописи

Шомаксудов Бобир Юлдашевич

Исследование методов оценки рисков информационной безопасности в волоконно-оптических сетях телекоммуникации

Специальность: 5А522203 –“Оптические системы связи и обработки информации”

Диссертация

На соискание академической степени магистра

Работа рассмотрена
и допушена к защите
Зав. кафедрой
«ТСП», к.т.н, доцент Исаев. Р. И

«____»_____2010 г

Научный руководитель
к.т.н, доц. Исаев Р. И.
_____

Ташкент – 2010

СОДЕРЖАНИЯ

ВВЕДЕНИЕ

Президент Республики Узбекистан И.Каримов неоднократно подчеркивал необходимость последовательного развития сферы информационно-коммуникационных технологий и внедрения их во все сферы жизни. В результате постоянного внимания Правительства Республики Узбекистан за последние четыре года отмечается динамичное развитие услуг этой отрасли. В соответствии с предотвращением негативного влияния глобального экономического кризиса по инициативе главы государства в 2008 году была принята Антикризисная программа на 2009-2012 годы, в которой определены соответствующие меры, а также приоритетные направления социально-экономического развития страны.

В Республике Узбекистан уделяется особое внимание задачам и проблемам обеспечения информационной безопасности на государственном уровне. Об этом свидетельствуют законы Республики Узбекистан, указы и постановления Президента Республики Узбекистан, постановления Правительства, руководящие документы Узбекского агентства связи и информатизации, министерств и ведомств, связанные с регулированием различных аспектов в области информационных технологий. Одной из основных целей информационной безопасности является оценки риска информационной безопасности, целостности информации в процессе ее передачи, хранения и обработки.

Международная практика развитых стран показывает, что стратегической задачей в сфере связи и информатизации является кардинальная перестройка национальных информационных инфраструктур (НИИ) на пути к глобальному информационному обществу (ГИО) в соответствии с основополагающими принципами его создания. В этой связи в развитых странах в последнее десятилетие серьёзно проработаны основополагающие принципы создания и интеграции НИИ в глобальную информационную инфраструктуру

(ГИИ), поэтому успешная интеграция в мировое информационное пространство невозможна без развитой НИИ и её технологической основы – высокоскоростных оптических сетей телекоммуникаций (ОСТ), способных обеспечить доступ к современным инфокоммуникационным услугам. Такой доступ может быть обеспечен только на базе современных ОСТ, отвечающих мировым тенденциям развития. Однако интенсивное развитие НИИ обуславливает появление ряда проблем, в том числе проблем, касающихся их информационной безопасности.

В последние годы в Узбекистане в сфере телекоммуникации и информатизации осуществляется большая работа по модернизации существующих и построению современных ОСТ. Многообразие ОСТ ставит ряд проблем, среди которых одной из важнейших является проблема координации создания и развития защищенных ОСТ, поэтому построение современных ОСТ необходимо осуществлять с учетом требований безопасности их функционирования, что требует соответствующей разработки необходимых требований к информационной безопасности ОСТ.

Современные технологии и оборудование телекоммуникаций, используемые в ОСТ, являясь одними из самых сложных и наукоёмких продуктов, традиционно относятся к группе критических технологий. Учитывая постоянное усложнение оптических технологий телекоммуникаций и процессов функционирования ОСТ необходимо своевременно изучать новые технологии как объекты информационной безопасности, выявлять в них уязвимые места и разрабатывать механизмы и методы обеспечения их информационной безопасности.

Актуальность темы: Интенсивное внедрение технологий и оборудования оптических сетей телекоммуникаций в различные сферы деятельности общества приводит к необходимости пересмотра их роли и значения в связи с возрастанием зависимости общества от безопасного функционирования составляющих инфраструктуры телекоммуникаций, так

как наличие скрытых уязвимостей усиливает опасность несанкционированного вмешательства в их функционирование.

Поэтому одним из ключевых аспектов решения проблемы создания защищённых оптических сетей телекоммуникаций является исследование и разработка показателей и критериев оценки уровня их информационной безопасности. В этой связи существует острая необходимость исследование риско-ориентированных методов оценки информационной безопасности оптических сетей телекоммуникации.

Цель работы: Основной целью данной магистерской диссертации является определение методов оценки рисков информационной безопасности оптических сетей телекоммуникации и разработка методики использования методов нечетких множеств для оценки рисков информационной безопасности оптической сети телекоммуникации.

Задача работы. Основными задачами данной магистерской диссертации являются:

- анализ оптической сети телекоммуникации как объекта оценки рисков информационной безопасности;
- изучение современных подходов к оценке рисков информационной безопасности;
- анализ методов оценки рисков информационной безопасности оптических сетей телекоммуникации;
- составление общего положения алгоритма оценки рисков информационной безопасности на основе теории нечетких множеств;
- моделирование параметрических алгоритмов оценки рисков информационной безопасности оптических сетей телекоммуникации на основе теории нечетких множеств с использованием MATLAB.

Объект и предмет исследования: Объектом исследования данной работы является система информационной безопасности в оптических сетях телекоммуникаций.

Предмет исследования составляют методы и алгоритмы оценки рисков информационной безопасности в оптических сетях телекоммуникаций.

Методы исследования: Методами исследования выбраны: анализ и проработка литературы по данной магистерской диссертации, изучение современные подходы к оценке рисков информационной безопасности оптических сетей телекоммуникации, обзор стандартов в области оценки информационной безопасности, методы оценки рисков информационной безопасности оптических сетей телекоммуникации, моделирование параметрические алгоритмы оценки рисков информационной безопасности на основе теории нечетких множеств с использованием MATLAB.

Научная новизна: диссертационной работы заключается в следующем:

1. На основе анализа эффективности методов оценки рисков информационной безопасности оптических сетей телекоммуникации предложен алгоритм на основе методов теории нечетких множеств.

2. Разработана методика использования методов теории нечетких множеств для оценки рисков информационной безопасности оптических сетей телекоммуникаций.

Практическая ценность полученных результатов: в основу работы положены результаты полученные при исследование методов оценки рисков информационной безопасности на основе метода нечеткой логики. Разработанные алгоритмы и методики использования методов нечеткой логики для оценки рисков информационной безопасности оптической сети телекоммуникации позволить качественный и количественный оценки рисков информационной безопасности непосредственно на практике даже когда не достаточно статистических данных о исследуемых объектах.

Апробация результатов работы: результаты научных разработок и исследований, выполненных по теме диссертации, обсуждались на международной, республиканской научно-технической конференции для студентов, аспирантов и молодых специалистов.

Структура диссертации. Диссертация состоит из введения, трех глав с выводами, заключения, списка используемых источников. Работа изложена на 130 страницах машинописного текста, содержит 29 рисунков и 15 таблицы, список литературы состоит из 34 наименования, в приложении приведена слайды презентации.

1 ПРОБЛЕМЫ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 Анализ оптической сети телекоммуникаций как объектов оценки рисков информационной безопасности

Оптическая сеть телекоммуникаций – совокупность оптических средств телекоммуникаций, обеспечивающих один или несколько видов передач: телефонную, телеграфную, факсимильную, передачу данных и других видов документальных сообщений, трансляцию телевизионных и радиовещательных программ.

Основными компонентами используемых в оптических сетях телекоммуникаций (ОСТ) являются: волоконно-оптические кабели, разветвители, ответвители, мультиплексоры, демультиплексоры, оптические усилители, оптические передатчики (или лазеры) и оптические приемники, оптические кросс коммутатори и др [1].

Рассмотрим уязвимости отдельных компонентов ОСТ более подробно.

1.1.1 Уязвимости волоконно-оптических кабелей связи

Волоконно-оптические линии связи состоять из строительных длин волоконно-оптических кабелей соединенных с помощью оптических муфт и при необходимости, включенные через разветвитель, ответвитель, оптический усилитель и др. [2]. Основным уязвимым элементом волоконно-оптических кабелей является оптическое волокно (ОВ).

ОВ обладает затуханием, вызванным целым рядом причин: френелевское отражение, собственное поглощение, поглощение на ионах ОН-, излучение на микро- и макро изгибах и др. (рис.1.1).

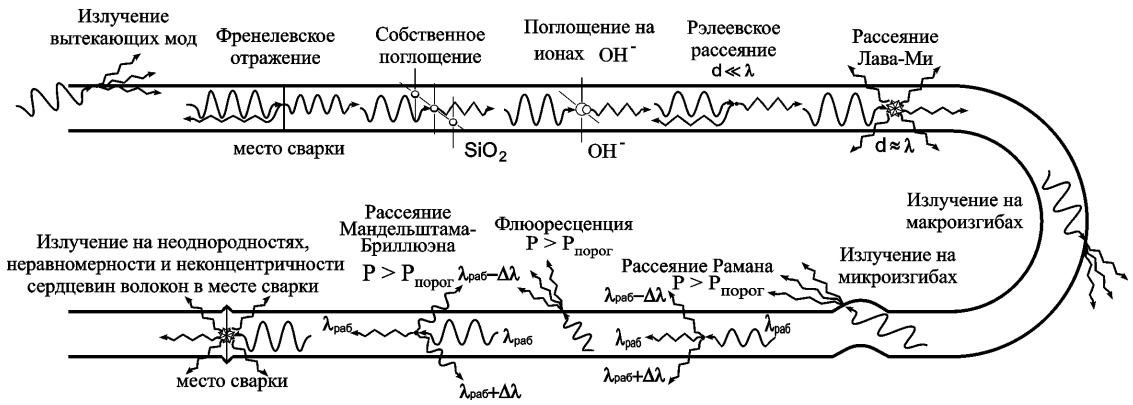

Рис.1.1 - Причины излучения и рассеивания в оптическом волокне

Используя эти явления в своих целях, злоумышленник может осуществлять различные виды несанкционированных воздействий на передаваемую информацию.

За счет макроизгиба можно добиться преобразования направляемых мод в вытекающие, что приведет к выводу части мощности оптического волокна за пределы оболочки. Тем самым злоумышленник получит несанкционированный доступ к сигналу. Кроме того, есть опасность использования вытекающих мод в местах стыковки ОВ между собой или с оптическим разветвителем. Это обусловлено тем, что для волоконно-оптических линий связи (ВОЛС) такой отбор мощности является незаметным из-за «естественной» утечки мод [3].

Внедрение фотодетектирующих элементов в оболочку ОВ или использование механических и термических способов воздействия на ОВ для создания микроизгиба, который и приведет к ответвлению части мощности из ОВ.

ВОЛС, в силу особенностей распространения электромагнитной энергии в оптическом волокне, обладают повышенной скрытностью. Это объясняется тем, что оптическое излучение, являющееся носителем информации, распространяется в ОВ согласно закону полного внутреннего отражения [2], а за ОВ электромагнитное излучение экспоненциально спадает. Участки, где возможна утечка электромагнитного излучения и

несанкционированный съем информации (НСИ), относительно малочисленны, «классические» радиотехнические методы (приемо-передающая аппаратура, регенерационные пункты) изучены и локализованы.

По этой причине эти участки сравнительно легко могут быть поставлены под контроль.

Известны следующие нарушения полного внутреннего отражения:

1. Изменение угла падения. Использование внешнего воздействия для уменьшения угла падения до значения, меньшего значения предельного угла падения, при котором начинает наблюдаться полное внутреннее отражение.

2. Изменение отношения показателя преломления оболочки к показателю преломления сердцевины оптического волокна. Использование внешнего воздействия для увеличения угла полного внутреннего отражения до значений, больших характерных углов падения в оптическом волокне.

3. Оптическое туннелирование. Оптическое туннелирование состоит в прохождении излучения через оболочку оптического волокна с показателем преломления меньшим, чем у сердцевины, при углах падения больше угла полного внутреннего отражения.

Рассмотрим формирование каналов утечки сигнала из ОВ [11].

а) Формирование каналов утечки при изменениях формы оптического волокна.

Изменение угла падения может достигаться путем механического воздействия на ОВ, например, его изгибом. При изгибе оптического волокна происходит изменение угла падения электромагнитной волны на границе сердцевина-оболочка. Угол падения становится меньше предельного угла, что означает выход части электромагнитного излучения из оптического волокна (рис.1.2). Изгиб оптического волокна приводит к сильному побочному излучению в месте изгиба, что создает возможность несанкционированного съема информации в локализованной области.

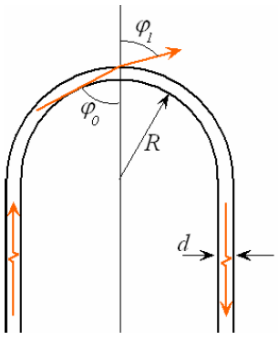

Рис.1.2 - Формирование канала утечки при изгибе радиусом R оптического волокна с диаметром сердцевины *d*, φ_0 - угол падения, φ_1 - угол преломления

Оценим максимальный радиус изгиба *R*, при котором наблюдается побочное излучение в точке изгиба световода с диаметром сердцевины *d*, связанное с нарушением полного внутреннего отражения. Максимальный радиус определяется выражением [13]

$$R \le d \frac{n_2}{n_1 - n_2}, \tag{1.1}$$

где n_1, n_2 – показатели преломления сердцевины и оболочки оптического волокна соответственно.

Интенсивность электромагнитной волны, выходящей из ОВ в точке изгиба, определяется по формулам Френеля для *p*- и *s*- поляризаций, соответственно

$$I_p = I_0 \frac{\sin 2\varphi_0 \sin 2\varphi_1}{\sin^2(\varphi_0 + \varphi_1)\cos^2(\varphi_0 - \varphi_1)}, \tag{1.2}$$

$$I_S = I_0 \frac{\sin 2\varphi_0 \sin 2\varphi_1}{\sin^2(\varphi_0 + \varphi_1)}, \tag{1.3}$$

где I_0 – интенсивность падающего излучения и I_p, I_s – интенсивности прошедшего излучения для *p*- и *s* – поляризаций [15].

Оценка радиуса изгиба для многомодового волокна с диаметром сердцевины d=50 мкм и оптической оболочки – D=125 мкм (n_1=1,481, n_2=1,476) показывает, что при $R \leq 3{,}5$ см начинает наблюдаться сильное прохождение излучения в точке изгиба (до 80% значения интенсивности основного светового потока в ОВ). Надо отметить, что при оценке изгиба не учитывались форма светового потока, цилиндрическая форма преломляющей поверхности и другие эффекты, изменяющие показатель преломления оптического волокна, например, фотоупругий эффект. Их вклад значительно меньше.

Нарушение полного внутреннего отражения при механическом воздействии возможно не только при изгибе ОВ, но и при локальном давлении на оптическое волокно, то вызывает неконтролируемое рассеяние (в отличие от изгиба) в точке деформации.

б) Формирование каналов утечки внешним воздействием, вызывающим изменением отношения показателей преломления. Изменения угла падения можно добиться не только изменением формы оптического волокна при механическом воздействии, но и акустическим воздействием на оптическое волокно. В сердцевине ОВ создается дифракционная решетка периодического изменения показателя преломления, которая вызвана воздействием звуковой волны. Электромагнитная волна отклоняется от своего первоначального направления, и часть её выходит за пределы канала распространения. Физическое явление, с помощью которого возможно решить поставленную задачу, является дифракция Брэгга на высокочастотном звуке (f>10МГц), длина волны Λ которого удовлетворяет условию:

$$(\lambda L / \Lambda^2) > 1, \qquad (1.4)$$

где λ – длина волны электромагнитного излучения, L – ширина области распространения звуковой волны.

Деформации, создаваемые упругой волной, формируют периодическое изменение показателя преломления внутри ОВ для света являющейся дифракционной решеткой (рис.1.3).

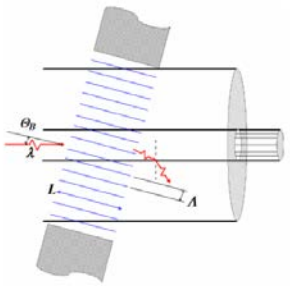

Рис.1.3 - Формирование дифракционной решетки в сердцевине оптического волокна звуковой волной

Максимальный угол отклонения единственного наблюдаемого дифракционного максимума равен двум углам Брэгга ($2\Theta B$) . Частота отклоненной электромагнитной волны приблизительно равна частоте основного информационного потока. Интенсивность дифракционного максимума может быть определена по формуле

$$I = I_0 \sin^2\left(\frac{\pi}{2}\sqrt{J_0 M_2}\,\frac{L}{\lambda}\right), \qquad (1.5)$$

где J_0 – интенсивность звуковой волны;

M_2=1.51*10^{-15} сек^3/кг- акустооптическое качество кварца.

Вычисления показывают, что для многомодового ОВ с параметрами (d/D)=(50/125) при акустическом воздействии с длиной волны звука Λ=10 мкм и длине взаимодействия L=10^{-3}м, максимальный угол отклонения от первоначального направления распространения составляет 5 градусов. График зависимости интенсивности первого дифракционного максимума от интенсивности звуковой волны представлен на рис.1.4. Из графика видно,

что даже при невысоких интенсивностях звуковой волны выводимое электромагнитное излучение достаточно велико для регистрации его современными фотоприемниками. При фиксированной интенсивности звука, путем изменения области озвучивания L можно добиться максимального значения интенсивности в дифракционном максимуме, тем самым увеличить интенсивность света, отводимого в канал утечки [5].

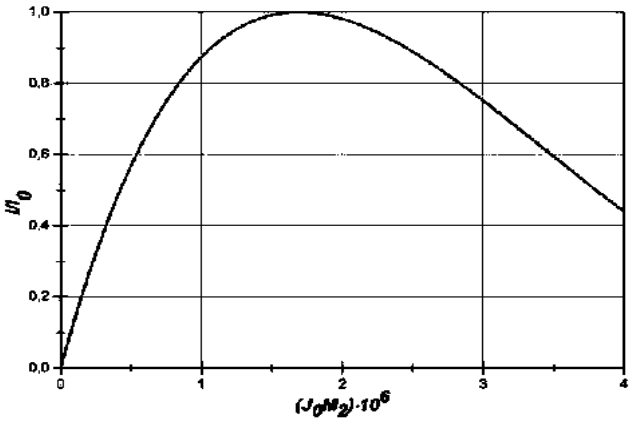

Рис.1.4 - Зависимость интенсивности дифракционного максимума от интенсивности звуковой волны

Другим внешним воздействием, изменяющим отношение показателя преломления оболочки к показателю преломления сердцевины ОВ (n_1/n_2), является механическое воздействие без изменения формы ОВ, например, растяжение.

При растяжении оптического волокна происходит изменение показателей преломления сердцевины и оболочки оптического волокна на Δn_1 и Δn_2. При этом увеличивается значение угла полного внутреннего отражения от φ_r до $\varphi_r^{'}$.

Значения углов связаны выражением

$$\sin\varphi_r^{'} \approx \left(1-\frac{\Delta n_1}{n_1}+\frac{\Delta n_2}{n_2}\right)\sin\varphi_r . \qquad (1.6)$$

Выражение для отношения ($\Delta n/n$) определяется фотоупругим эффектом так, что

$$\frac{\Delta n}{n} = -\frac{1}{2} n^2 p\varepsilon, \qquad (1.7)$$

где p, ε – эффективные составляющие тензоров фотоупругости и деформации, это связано с анизотропией оптического волокна возникающей при растяжении.

С учетом того, что плавленный кварц выдерживает большие напряжения (до 10^6 Па в идеальном состоянии), то, прикладывая большие механические напряжения к ОВ, возможно добиться изменения предельного угла на величину $\varphi_r^{'} - \varphi_r \approx 2 \cdot 10^{-6} \sin \varphi_r$, которое может оказаться достаточным для вывода части интенсивности основного информационного потока за пределы оптического волокна (рис.1.5).

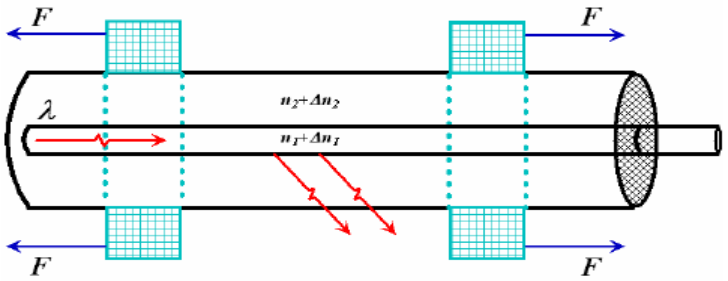

Рис.1.5 - Формирование канала утечки информации растяжением оптического волокна при воздействии внешнего усилия F

К способам вызывающим изменение отношения показателя преломления оболочки к показателю преломления сердцевины ОВ путем механического напряжения так же относится и скручивание оптического волокна.

К бесконтактным способам изменения отношения (n_2/n_1) можно отнести воздействие стационарных электрических полей, которые изменяют показатель преломления сердцевины и оболочки на Δn_1 и Δn_2. Выражение для отношения ($\Delta n/n$) определяется из уравнения для обратного пьезоэлектрического эффекта и явления фотоупругости

$$\frac{\Delta n}{n} = -\frac{1}{2} n^2 pbE\,, \qquad (1.8)$$

где b – модуль пьезоэлектрического эффекта;

E – напряженность электрического поля.

Новый угол полного внутреннего отражения (при $\Delta n_1>0$ и $\Delta n_2>0$), если для оценки принять значение напряженности электрического поля для пробоя идеального плавленого кварца (10^8В/м), то воздействием стационарного электрического поля, можно добиться изменения предельного угла на величину $\varphi_r^{'} - \varphi_r \approx 2\cdot 10^{-8} \sin\varphi_r$.

Несмотря на то, что изменения значения предельного угла, вызываемое как механическими напряжениями, так и электрическим полем малы, но комплексное воздействие с другими способами может привести к эффективному способу формирования канала утечки. Рассмотренные выше методы обладают одним недостатком, который позволяет легко фиксировать каналы утечки, созданные на их основе. Это определяется значительным обратным рассеянием света в местах каналов утечки. С помощью рефлектометрии обратно рассеянного света такие подключения легко обнаруживаются высоким пространственным и временным разрешением [15].

в) Формирование канала утечки методом оптического туннелирования.

Способ, который позволяет захватывать часть электромагнитного излучения, выходящего за пределы сердцевины информационного оптического волокна дополнительным ОВ, не внося дополнительных потерь и обратного рассеяния, является оптическое туннелирование. Явление оптического туннелирования состоит в прохождении оптического излучения из среды показателем преломления n_1 через слой с показателем преломления n_2 меньшим n_1 в среду с показателем преломления n_3 при углах падения больших угла полного внутреннего отражения. На принципах оптического туннелирования в интегральной и волоконной оптике создаются такие

устройства как оптический ответвитель, оптофоны, волоконно-оптические датчики физических величин.

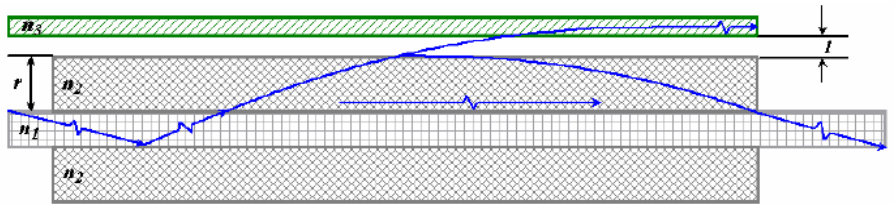

Рис.1.6 - Формирование канала утечки оптическим туннелированием. n_1, n_2 – показатели преломления сердцевины и оболочки оптического волокна, n_3 – показатель преломления дополнительного оптоволокна

При распространении света в оптическом волокне часть светового потока выходит за пределы сердцевины ОВ [16]. Интенсивность излучения вышедшего из сердцевины в оболочку ОВ на расстояние $r = (D-d)/2$ в зависимости от угла падения на границе сердцевина-оболочка φ определяется выражением

$$I = I_0 \cdot \exp(-4\pi n_1 (r/\lambda)\sqrt{\sin^2\varphi - \sin^2\varphi_r}). \qquad (1.9)$$

Это приводит к тому, что при изготовлении оптического волокна оболочка занимает значительную часть. Причем у одномодового волокна оболочка занимает гораздо больший объем, чем у многомодового. Это следует из приведенной формулы проникновения света из сердцевины в оболочку. При приближении угла падения φ к углу полного отражения φ_r показатель степени экспоненты стремится к нулевому значению, свет распространяется по всей структуре волокна – сердцевине и оболочке. Это приводит к тому, что часть интенсивности из основного ОВ может перейти в дополнительное ОВ. Интенсивность излучения переходящего в дополнительный волновод определяется выражением

$$I = I_0 \cdot \sin^2(k \cdot S), \quad (1.10)$$

где k – коэффициент связи оптических волокон;

S – длина оптического контакта двух волокон.

Максимум значения коэффициента связи достигается при нулевом расстоянии между оболочкой и дополнительным ОВ (l=0) и показателе преломления дополнительного волокна $n_3=n_1$. Как видно из выражения, излучение из основного оптического волокна переходит в дополнительное ОВ полностью при некотором значении длины оптического контакта $S=\pi/2k$. При дальнейшем увеличении длины оптического контакта происходит обратный процесс. Таким образом, излучение периодически переходит из одного ОВ в другой, если не учитывать потери на поглощение, рассеяние.

1.1.2 Типы и методы атаки в оптических сетях телекоммуникации

Атаку на ОСТ в целом можно разделить на семь областей, основанных на цели злоумышленника: анализ трафика, подслушивание, задержка данных, отказ в обслуживание, ухудшение QoS, спуфинг, человек - посредник.

Каждый компонент, уязвимый в ОСТ в той или иной форме может привести к отказу в обслуживании или прослушиванию. Методы атак, которые, наиболее относительны помехой - подавляющие законных сетевых сигналов с сигналами атаки, которые могут быть использованы для ухудшение или отказу в обслуживании, а также эксплуатации устройств с перекрестными помехами. Устройство перекрестных помех существует в большинстве современных оптических устройствах, а также такое явление, где сигналы от одной части оптических устройств утекают в другие части устройств. Перекрестные помехи могут быть использованы для отказа в обслуживании или прослушивания. Отметим, что перехват сигнала не отделён от анализа трафика. Необходимо понимать, что обнаружение атаки в ОСТ немного отличается от обнаружения атаки в электрооптических или электронных сетей [1].

Основным преимуществом безопасности ОСТ над электрооптических или электронных сетей телекоммуникаций является его устойчивость к атакам вида перехват телефонных сообщений. Основные законы физики излагают, что вокруг электрических токов создаются электромагнитные поля и излучения. В электрооптических и электронных сетях есть возможность злоумышленнику слушать или нарушить трафик внутри транспортных средств (проволока) без физического прикасания. Атака может происходить как изнутри так и снаружи. Такой тип перехвата телефонных сообщений, особенно изнутри, практически невозможно обнаружить. Поскольку целая инфраструктура ОСТ не включает никакого электрического потока, не генерируется электромагнитное излучение и, следовательно, нет никакой внешней утечки информации за пределами транспортного средства (волокно). Это огромное преимущество, и возможно самое важное преимущество безопасности ОСТ над электрооптическими или электронными сетями.

Как упоминалось раньше, атаку в ОСТ в целом можно разделить на семь областей: анализ трафика, подслушивание, задержка данных, отказ в обслуживании, ухудшение QoS, человек-посредник и спуфинг. Такое разделение очень удобно для группирования, чтобы уменьшить методы атаки изучаемую следующим образом: (1) анализ трафика и подслушивание, они имеют сходные характеристики, и они могут быть рассмотрены вместе; оптические сети отчасти устойчивые к задержке атаки, в связи отсутствием оптической памяти и задержка атаки игнорируются. (2) спуфинг это атака, которая может быть устранена использованием криптографических методов защиты и поэтому здесь не рассматривается. (3) отказ в обслуживании и ухудшение QoS могут считаться в виде «нарушение обслуживания».

В результате типы атак уменьшены к двум: подслушиванию и анализу трафика и нарушению обслуживания. Более полный список типов атаки мог включать в себя такие области, как возможность отказа, но такие атаки обычно направлены на сетевые протоколы, систем управления, а не в сетевые

инфраструктуры - инфраструктура является основной проблемой в этой работе. Хотя подслушивание и анализ трафика, обычно имеют существенно различны эффекты в нормальном использовании сети, этот анализ не требует разграничения. При более высоких уровнях сетевых протоколов, различия становятся более важными, но на физическом уровне, любая возможная утечка сигналов очень важна для целей данного анализа [2].

Для реализации одного из двух типов атак, злоумышленнику необходимы методы атаки. Рассмотрим следующие три конкретные атаки. Они выбраны поскольку они очень легко, реализуемы, особенно эффективно против сетевых услуг, или иметь по существу, разный эффект, чем аналогичная атака против традиционных сетей. Методы приведены в табл. 1.1.

Таблица 1.1

Методы атак на ОСТ

Методы атаки	**Реализация**	**Способ**
Внутриполостная помеха	нарушение обслуживания	Нарушитель вводит спланированный сигнал, ослабляя способность получателя для правильной интерпретации передачи данных
Внеполосная помеха	нарушение обслуживания	Нарушитель уменьшает компонент сигнала связи, используя имеющие компоненты или эффекты кросс- коммутации
Несанкционированное наблюдение	подслушивание	Нарушитель прослушивает перекрестные каналы, вытекающие из соседнего сигнала через общие ресурсы в целях получения информации от соседних сигналов

Эти методы не являются единственными методами пригодными для злоумышленника, чтобы реализовать один из двух типов атаки. Однако эти методы достаточно легко реализовать с использованием коммерчески доступных технологий, и может вызвать серьезные проблемы незащищённый ОСТ [11].

Есть много других возможных признаков классификации атак. Например, каждую атаку можно классифицировать по её ресурсам (пассивные, активные); средства атаки (передача/прием, протокол, управляющая система); цель (конкретные пользователи или сети/подсети); намеренный эффект (анализ трафика, подслушивание или нарушение обслуживания); нахождение (позиция) атаки (терминал, узел, линия, многочисленные позиции), и готовность атакующего для обнаружения (скрытые, тонкие, открытые)[5].

1.1.2.1 Методы атаки в оптических сетях телекоммуникации

Каждый компонент ОСТ является уязвимым к атаке. Три примера суммируют все возможности. Рассмотрим сначала внутриполосные помехи с помощью единственного мощного передатчика, который вводится в лини.

Атака может уничтожить сигнал на этой линии, не выделяя его от традиционной сети. Но в ОСТ атака может ухудшить сигналы на этой линии и на других сетевых линиях, связанных с этим узлом. Это является следствием прозрачности, которая позволяет сигналам, проходящим через узлы без их регенерации рис.1.7 показывает единственную атаку точки на центре линии (2;5), которая влияет не только на узел, которого сигнал атаки первым достигает (узел #2), но и связывает два других узла с первым атакованном узле (узел #1, и узел #3). Компоненты ОСТ, в качестве которых могут быть использованы сумматоры, мультиплексоры, или оптические усилители. Текущие методы обнаружения не предлагают правильное местоположение точки атаки. Например, мощность обнаружения на узле #1, возможно ошибочно приписывают проблеме атаки расположена на линии (1;2). Эта атака может быть сделана дешевой, тонкой, и может быть конкретно ориентирована на индивидуальных пользователей.

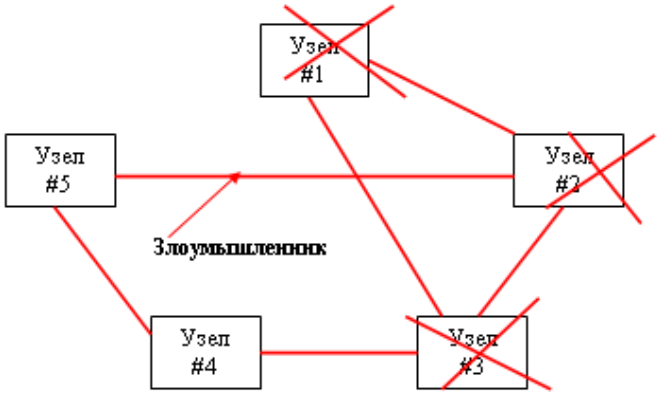

Рис.1.7 - Внутриполосная помеха

Второй атакой применяется внеполосная помеха, чтобы использовать перекрестные помехи в оптических компонентах. В частности, из-за эффектов перекрестного усиления сигнала, в пределах оптического усилителя, преднамеренные помехи используются внеполосном высокой мощности сигнала. Этот эффект сильно отличается от эффекта сжатия усиления обнаружения в электронном усилителе. Нарушитель может вводить сигнал на различные длины волны вне полосы частот сигнала связи, но в пределах полосы пропускания усилителя, как показано на рис.1.8. Атака может работать поскольку усилитель не может отличить атакующие сигналы и полезные сигналы сети связи, и обеспечить усиление для каждого сигнала без разбора из возникновения. Усилитель позволяет возможность в сигнале атаки обнаружить в нормальный сигнала связи и увеличивает мощность сигнала атаки в потоке данных к абоненту, что позволяет ему распространяться через прозрачные узлы. В нынешнее время принимаются средства обнаружения атаки, не обязательным является обнаружение помех, поскольку среднее значение полученной внутриполосной мощности могут быть использованы для уменьшения, или остаётся неизменными во время атаки. Этот тип атаки может быть установлен в оптическом усилителе в пределах узла или в рамка участка усиления волоконно-оптической линии связи [11].

Усилитель EDFA имеет разные временные характеристики, чем обычные электронные усилители. Оптические усиления происходят из-за возбуждения ионов эрбия путем поглощения стационарной оптической накачки. Динамика результирующего возбуждения может сильно усилена особенно когда они становятся достаточно интенсивными, чтобы насытить прирост извлечения энергии из возбуждения эрбия.

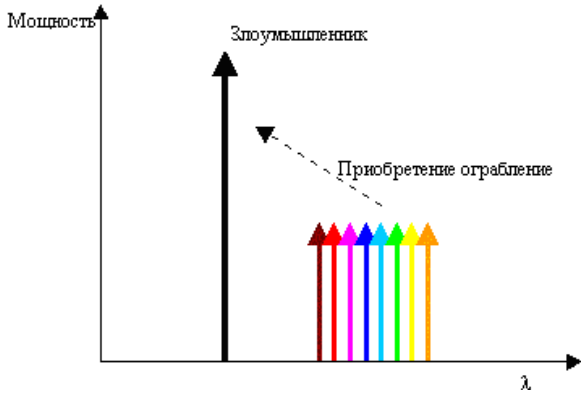

Рис.1.8 - Внеполосная помеха по причине усиления конкуренции

Третья атака является реализацией несанкционированного наблюдения (подслушивание), сбор сигналов злоумышленником которые ему не были предназначены. Прослушивание возможно в нескольких точках в пределах сети. Рассматриваются два примера. Первый пример использует компонент перекрестные помехи - современные демультиплексоры в пределах сетевых узлов и показывают уровень переходной помехи в пределах от 0,03% до 1,0%. Демультиплексор предназначен разделения каждую отдельную длину волны полученную от одного волокна на отдельном физическом пути, но перекрестные помехи допускают небольшую утечку каждой длины волны которая просачивается в неправильном пути. Этот сигнал может иметь достаточную точность, чтобы разрешать злоумышленнику обнаружить свое присутствие, и, возможно, восстановить часть данных из потока. В пределах электронных или электрооптических регенерационные сетей, уровень перекрестных помех, как правило, значительно ниже чем 0,03% и составляет меньшую угрозу подслушивания через перекрестные помехи. Во втором примере используется оптический усилитель. Усиления предоставляемые от

EDFA к отдельному каналу зависит от суммы всех уровней сигналов, проходящих через усилитель. Это означает, что возникновение сигналов небольшой амплитудной модуляции основан на наличии или отсутствии сигнала на соседних каналах. Злоумышленник может использовать эту небольшую модуляцию для восстановления части предполагаемого сигнала в соседнем канале. Атака в оптические усилители может быть эффективным в электро-оптических, или полностью оптических сетях. Потенциальные атаки являются более сложными и многочисленными.

Используемые в настоящее время на практике подходы к обеспечению информационной безопасности ОСТ должны определяться следующими этапами [12]:

a) требованиями к информационной безопасности, реализуемыми системами обеспечения информационной безопасности и регламентирующими (заданными) соответствующими нормативными документами в области информационной безопасности;

b) реальными услугами и механизмами защиты, реализуемыми в системах обеспечения информационной безопасности;

c) существующей статистикой угроз безопасности для конкретной ОСТ, потенциально возможных угроз и нарушителей, а также причинами уязвимостей.

Таким образом, основной целью обеспечения информационной безопасности ОСТ является поддержка и сохранение в условиях информационных воздействий на их информационную сферу основных характеристик информационной безопасности сетей. Поэтому общие требования к информационной безопасности ОСТ должны формироваться и устанавливаться на основе анализа серьезности последствий нарушений каждой из составляющих информационной безопасности: конфиденциальность, целостность и доступность.

В основе формирования требований, определяющих необходимый уровень информационной безопасности, лежит анализ ОСТ как объектов оценки рисков информационной безопасности. Оценка рисков информационной безопасности ОСТ должна производиться с целью проверки соответствия достигнутого уровня информационной безопасности заданному уровню при проектировании ОСТ. Оценка риска информационной безопасности ОСТ является также важным средством обеспечения гарантии реализации выбранных механизмов, методов и средств информационной безопасности. Однако в настоящее время не существует общей методологии, методов и конкретных методик оценки рисков информационной безопасности, поэтому сравнение различных сетей безопасности чрезвычайно затруднительно.

Анализ показывает, что разработка методики оценки информационной безопасности предполагает наличие или разработку [3-5]:

a) модели объекта оценки риска;
b) модели системы защиты;
c) модели потенциального нарушителя.

Наличие модели объекта оценки риска необходимо для определения существующих в нем связей и процессов, выявления конкретных элементов, требующих защиты, характерных уязвимостей и угроз, а также выработки показателей (критериев) информационной безопасности.

В условиях динамичного развития ОСТ и возникновения новых угроз информационной безопасности важным становится анализ и управление рисками информационной безопасности. В этой связи построение систем обеспечения информационной безопасности современных ОСТ должно начинаться с анализа рисков информационной безопасности [3,9-11].

Анализ рисков состоит в том, чтобы выявить существующие риски информационной безопасности и оценить их величину (дать им качественную или количественную оценку). В результате выявляются угрозы

информационной безопасности с большой вероятностью реализации, приводящие к существенным размерам ущерба. Управление рисками информационной безопасности связано с принятием мер обеспечения информационной безопасности, направленных на снижение частоты реализации угроз и размера ущерба в случае их реализации.

В основу разработки методики положена оценка риска, который требует построения полной модели ОСТ, включающей:

a) описание сетевых ресурсов;

b) описание и оценку существующих в них уязвимостей;

c) анализ и оценку возможных угроз;

d) описание возможных дестабилизирующих воздействий, способных осуществить реализацию угроз;

e) оценку противодействия угрозам, принятым на ОСТ мерами обеспечения безопасности и реализованными механизмами безопасности.

Таким образом при анализе рисков осуществляется:

a) классификация информационных ресурсов;

b) составление модели потенциального злоумышленника;

c) анализ уязвимостей;

d) идентификация и оценка угроз нарушений информационной безопасности;

e) оценка рисков нарушения информационной безопасности.

Международная практика развитых зарубежных стран показывает, что вопросам анализа и оценки риска информационной безопасности уделяется самое серьезное внимание.

Основными этапами оценки риска являются [9-11]:

a) анализ характеристик ОСТ на предмет наличия уязвимостей и возможности их использования угрозами информационной безопасности;

b) определение уязвимостей в рассматриваемых компонентах и ресурсах ОСТ;

c) определение перечня угроз с ранжированием их по вероятности;

d) анализ критерий безопасности и вычисление их вероятностных характеристик.

Рассмотрим этапы оценки и управления информационными рисками:

a) сначала необходимо определить все ценные информационные ресурсы, а также объекты их хранения и обработки;

b) далее определяется стоимость информационных ресурсов (или ущерб, который нанесен от нарушения конфиденциальности, целостности или доступности ресурсов);

c) кроме того, оценивается вероятность возникновения нарушений информационной безопасности. В рамках оценки данной вероятности определяются уязвимости, существующие в информационных системах, и вероятности их реализации;

d) на основании полученных данных рассчитывается риск для каждого информационного ресурса, который равен произведению вероятности возникновения нарушений и ущерба, который понесет в случае нарушения информационной безопасности владелец информационного ресурса.

1.2 Проблемы анализа рисков информационной безопасности оптических сетей телекоммуникации

Проблема обеспечения информационной безопасности в ОСТ является на сегодня одной из самых острых не только у нас в стране, но и в развитых странах мира. Опыт эксплуатации ОСТ и ресурсов в различных сферах жизнедеятельности показывает, что существуют различные и весьма реальные угрозы потери информации, приводящие к материальным и иным ущербам.

Интерес к проблемам информационной безопасности определяется все возрастающей ролью информации в различных сферах жизни общества (например, экономической, политической сферах).

Проблема обеспечения информационной безопасности является одной из актуальных проблем, которая стоит перед мировым сообществом.

Оптические телекоммуникационные технологии значительно расширили возможности бизнеса. Но новые возможности всегда сопряжены с новыми рисками. Чем сильнее основная деятельность компании зависит от телекоммуникационных технологий, тем выше риск осуществления по отношению к ней различных угроз: например, финансового мошенничества или хищения конфиденциальной информации.

Известно, что риск — это вероятность реализации угрозы информационной безопасности. В классическом представлении оценка рисков включает в себя оценку угроз, уязвимостей и ущерба, наносимого при их реализации. Анализ риска заключается в моделировании картины наступления этих самых неблагоприятных условий посредством учета всех возможных факторов, определяющих риск как таковой. С математической точки зрения при анализе рисков такие факторы можно считать входными параметрами.

Перечислим эти параметры [10]:

1) активы — ключевые компоненты инфраструктуры системы, вовлеченные в бизнес-процесс и имеющие определенную ценность;

2) угрозы, реализация которых возможна посредством эксплуатации уязвимости;

3) уязвимости — слабость в средствах защиты, вызванная ошибками или несовершенством в процедурах, проекте, реализации, которая может быть использована для проникновения в систему;

4) ущерб, который оценивается с учетом затрат на восстановление системы в исходное состояние после возможного инцидента ИБ.

Когда возможный ущерб от потенциальных угроз достаточно велик, необходимо внедрять адекватные и экономически оправданные меры защиты. Но здесь возникает целый ряд вопросов. Как оценить степень риска или

размер возможного ущерба? Как определить, что именно угрожает основной деятельности в силу использования оптических телекоммуникационных технологий и систем, насколько они уязвимы?

Анализ рисков информационной безопасности дает оператору ОСТ возможность определить наиболее проблемных областей в части обеспечения информационной безопасности, а также определения приоритетов в реализации защитных мер ОСТ.

В результате анализа рисков информационной безопасности оператор телекоммуникаций получит следующие основные выгоды:

a) определение наиболее проблемных областей в обеспечении информационной безопасности;

b) возможность аргументированного выбора мер по обеспечению информационной безопасности и планирования порядка их применения;

c) получение качественных или количественных характеристик значимости угроз и уязвимостей информационной безопасности, ранжирование активов и угроз по значимости;

d) получение начальной методологической базы, необходимой для реализации процесса управления рисками.

ОСТ зарождаются как перспективная технология для очень высоких скоростей передачи данных, гибкость коммутации и поддержки широкополосных приложений. В частности, они обеспечивают прозрачность и возможности новых особенностей, позволяющих маршрутизации и коммутации трафика без регресса или изменении сигналов в сети. Хотя ОСТ предлагают множество преимуществ для высокой скоростью передачи данных, они обладают уникальными особенностями и требованиями в области безопасности и управления, которые отличают их от традиционных сетей телекоммуникаций. В частности, уникальные характеристики компонентов ОСТ и сетевых архитектур принесла множество новых проблем для обеспечения безопасности сети. По своей природе, компоненты ОСТ

являются особенно уязвимыми для различных формы атак отказа обслуживании, ухудшение QoS, и подслушивание. Поскольку даже короткие (по срокам) разломы и атаки могут вызвать большое количество данных, которые будут утрачены, необходимость для обеспечения и защиты оптических сетей становится более значимой.

В контексте этого, атака определяется как преднамеренные действия против надлежащего и безопасного функционирования сети, а ошибки определяются как непреднамеренные действия против идеальное и надежное функционирование сети. Сбой называют ошибки и атаки, которые могут прерывать идеального функционирования сети.

Безопасность от атак на ОСТ может варьироваться от простого физического доступа к более сложным:

a) своеобразное свойства оптические волокно;

b) уникальные характеристика компонентов ОСТ;

c) имеющие недостатки надзорные методы и методы контроля.

Атаки могут быть классифицированы как прослушивание или отказ в обслуживание. В этом случае, они различают по своей природе от злоумышленника (например, пользователь вставляет сигнал высокое мощности) усиления для перехвата. Таким образом, атаки отличают от обычных ошибок и поэтому действуют по-разному.

Это потому, что они появляются и исчезают, и время от времени может быть запущены в другом месте сети. В частности, злоумышленник может сорвать простые методы обнаружения, которые в целом не достаточно чувствительным, чтобы обнаружить малые и случайный ухудшению производительности. Кроме того, разрушительное атаки, которые ошибочно определили как неисправность, может быстро распространиться по сети вызывая дополнительные ошибки и вызвать множество ошибочных сигналов. Безопасность атаки, следовательно, должны быть обнаружены и определены на любой узел в сети, где они могут иметь место. Кроме того, скорость

обнаружения атак и локализация должна быть соизмерима со скоростью передачи данных. Кроме того, прозрачность в ОСТ может внести значительно разные нарушения передачи таких как оптические перекрестные помехи, усиливаются шумы спонтанной эмиссии и расхождения мощности. В ОСТ, эти дефекты накапливаются и полученный коэффициент интенсивности ошибочных битов на узле назначения может стать неприемлемо высокой [3].

Один из основным проблемы анализа рисков информационной безопасности ОСТ является разветвленность и отсутствие статистической информации о угрозах, уязвимостях и атаках.

Анализ рисков информационной безопасности - процесс получения информации, содержащей определение и анализ потенциальных угроз информационной безопасности ОСТ, необходимый для принятия решений, связанных с оптимизацией капиталовложений для обеспечения информационной безопасности ОСТ.

При проведении анализа рисков необходимо определить:

a) уязвимые места в ОСТ;

b) существующие угрозы и их уровень;

c) допустимый уровень угроз;

d) комплекс мер, позволяющий снизить риски до допустимого уровня.

По каждому из этих пунктов требуется проведение специальных исследований.

Оценка рисков включает в себя мероприятия по определению того, какие ресурсы и от каких угроз надо защищать, а также в какой степени те или иные ресурсы нуждаются в защите. Риск определяется вероятностью причинения ущерба и величиной ущерба, наносимого организации в случае осуществления угрозы безопасности. Оценка рисков состоит в том, чтобы выявить существующие риски и оценить их величину. Процедура оценки рисков включает в себя ряд последовательных этапов:

a) настройка методологии оценки под конкретную организацию;

b) выбор шкалы оценки рисков;

c) оценка стоимости ресурсов, вероятности угроз и величины уязвимостей;

d) определение допустимого уровня остаточных рисков;

e) оценивание рисков;

f) подготовка отчета по результатам оценки рисков;

g) разработка реестра информационных рисков;

h) принятие решений по обработке рисков;

i) разработка Плана обработки рисков;

j) разработка Декларации о применимости;

k) согласование и презентация отчетных документов.

Построение эффективной системы управления рисками безопасности ОСТ — это не разовый проект, а комплексный процесс, направленный на минимизацию внешних и внутренних угроз при учете ограничений на ресурсы и время. Для построения эффективной системы безопасности ОСТ необходимо первоначально обобщенно описать процессы деятельности и выделить риски. Затем следует определить порог риска. Превышение подобного порога означает, что данным риском необходимо управлять. Требуется построить такую систему безопасности ОСТ, которая обеспечит минимизацию рисков с высоким уровнем опасности. Причем риски, имеющие уровень ниже критического, можно вообще исключить из анализа.

С точки зрения процессного подхода, систему управления рисками можно представить как процесс управления рисками (рис.1.9). На данной рисунке прямоугольниками показаны процессы, а стрелками - их взаимосвязи.

Режим информационной безопасности в ОСТ обеспечивается:

a) на *процедурном уровне* - путем разработки и выполнения разделов инструкций для персонала в области информационной безопасности, а также мерами физической защиты;

b) на *программно-техническом уровне* - применением апробированных и сертифицированных решений, стандартного набора контрмер: резервное копирование, антивирусная защита, парольная защита, межсетевые экраны, шифрование данных и т.д.

Анализ рисков в области информационной безопасности может быть качественным и количественным. Количественный анализ, точнее, так как он позволяет получить конкретные значения рисков, но он отнимает заметно больше времени, что не всегда оправдано. Чаще всего бывает достаточно быстрый качественный анализ, задача которого - распределение факторов риска по группам. Шкала качественного анализа может различаться в разных методах оценки, но всё сводится к тому, чтобы выявить самые серьезные угрозы [7].

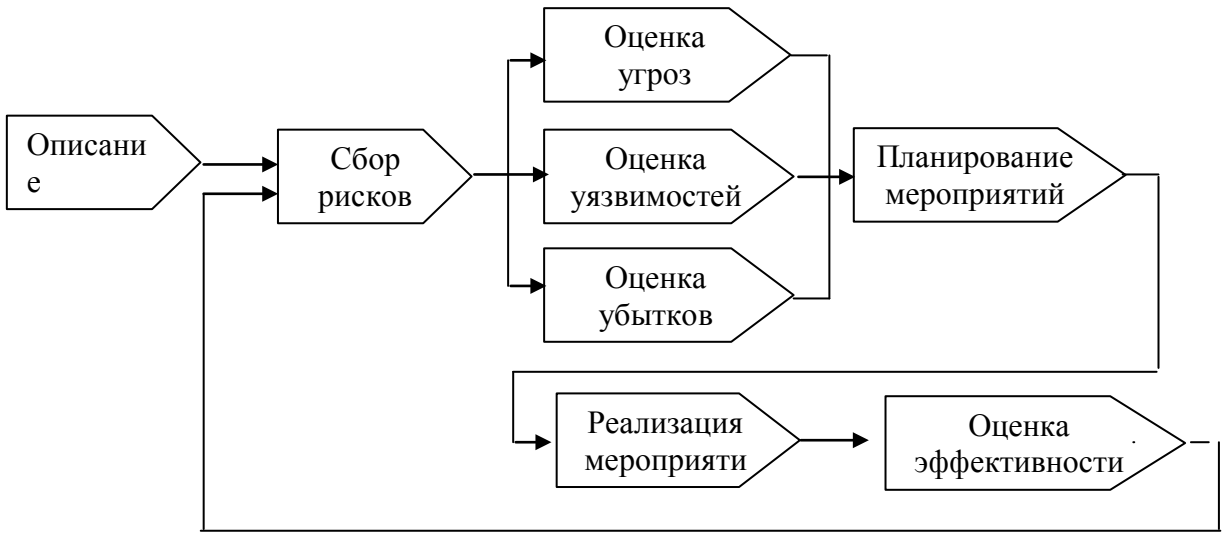

Рис.1.9 – Процесс управления рисками

Важно различать понятия единичного и приведенного убытков. Единичный убыток — это расходы на один инцидент. Приведенный убыток учитывает количество конкретных инцидентов безопасности за некоторый

промежуток времени, обычно за год. Если единичные и приведенные убытки запутаны, то полученные результаты будут иметь мало общего с действительностью.

Для полного анализа рисков необходимо:

a) определить ценность ресурсов;

b) добавить к стандартному набору список угроз, актуальных для исследуемой информационной системы;

c) оценить вероятность угроз;

d) определить уязвимость ресурсов;

e) предложить решение, обеспечивающее необходимый уровень информационной безопасности.

Существующих или планируемых к внедрению средств обеспечения информационной безопасности, которые уменьшают число уязвимостей, вероятность возникновения угроз и возможность негативных воздействий.

При выполнении полного анализа рисков приходится решать ряд сложных проблем: Как определить ценность ресурсов? Как составить полный список угроз информационной безопасности и оценить их параметры? Как правильно выбрать эффективные контрмеры?

Процесс анализа рисков делится на несколько этапов:

a) идентификация информационных ресурсов;

b) выбор критериев оценки и определение потенциального негативного воздействия на ресурсы и приложения;

c) оценка угроз;

d) оценка уязвимостей;

e) оценка рисков;

f) оценка эффективности существующих и предполагаемых средств обеспечения информационной безопасности.

Информационная сфера ОСТ состоит из:

a) информационных ресурсов ОСТ (хранимой, обрабатываемой и передаваемой информации);

b) информационной инфраструктуры (программного обеспечения, протоколов, интерфейсов, процедур, обеспечивающих процессы функционирования ОСТ и т.п.);

Проблема обеспечения информационной безопасности ОСТ включает в себя уже традиционную проблему защиты информации, но значительно шире нее как по функциям защиты, так и по принципам и подходам к защите ОСТ от несанкционированных и непреднамеренных воздействий нарушителя (рис. 1.10) [7 - 10].

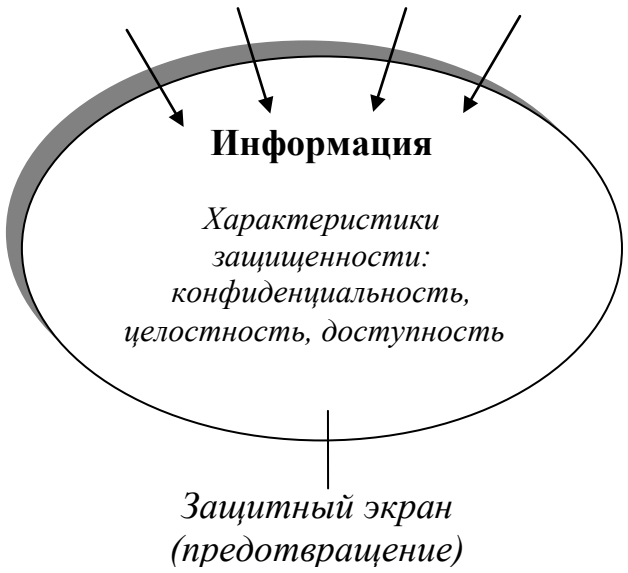

Рис.1.10 - Воздействия нарушителя на информацию

Международный опыт развитых стран показывает, что важнейшим и непременным условием повышения эффективности многих сфер деятельности общества становится совершенствование телекоммуникационного комплекса, так как именно благодаря телекоммуникациям все в большей степени обеспечивается эффективное функционирование систем

государственного управления, банковских и финансовых структур, оборонных и специальных структур, транспорта, систем электроснабжения и др.

Однако истинное развитие ОСТ, сопровождающееся появлением потенциальных уязвимостей оптических телекоммуникационных технологий, порождает достаточно серьезные проблемы информационной безопасности. Нарушение функционирования ОСТ может являться следствием дестабилизирующих воздействий, которые могут осуществляться как с использованием штатных возможностей самих систем, так и с использованием специальных средств программно-технического воздействия. Обеспечение информационной безопасности необходимо рассматривать как совокупность организационно-технических мер для предотвращения угроз при создании ОСТ - противодействие угрозам технологической безопасности, и в процессе эксплуатации оптический сетей – противодействие угрозам эксплуатационной безопасности.

Анализ международной практики показывает, что одной из важных проблем анализа рисков информационной безопасности ОСТ является исследование оценки риска их информационной безопасности. Однако оценка риска информационной безопасности ОСТ представляет собой трудно формализуемую и более того, практически трудно выполнимую из-за своей многоаспектности задачу. В настоящее время существует ряд методологических подходов к оценке рисков информационной безопасности отдельных оптических телекоммуникационных технологий. Что же касается решения задач комплексной оценки риска безопасности ОСТ в целом, то в настоящее время не существует сложившейся методологии оценки риска безопасности.

Между тем, проблема оценки риска информационной безопасности ОСТ становится ключевым фактором, влияющим на безопасность всей телекоммуникационной инфраструктуры.

Проблема оценки риска информационной безопасности ОСТ обусловлена ниже перечисленными факторами [12]:

a) недостаточной проработанностью международных стандартов и рекомендаций ISO, ITU-T, ETSI и др. с точки зрения показателей и методов оценки информационной безопасности ОСТ;

b) отсутствием конкретных методик количественной оценки информационной безопасности ОСТ.

На основании вышеизложенного ключевыми аспектами решения проблемы создания и развития безопасных ОСТ:

a) разработка требований, показателей и критериев для оценки уровня безопасности;

b) исследование методов качественной и количественной оценок рисков информационной безопасности;

c) анализ инструментальных средств оценки рисков информационной безопасности;

d) разработка методов и механизмов оценки рисков информационной безопасности.

В новых международных стандартах и рекомендациях ISO, ITU-T, ETSI и др. информационная безопасность рассматривается как один из показателей качества обслуживания ОСТ. Как известно, комплексную характеристику степени удовлетворения пользователя предоставляемыми услугами определяют параметры качества обслуживания.

Параметры качества обслуживания ОСТ рассмотрим на примере службы передачи данных, принимая во внимание при этом, служба передачи данных является одним важных элементом ОСТ.

Для определения качества обслуживания в службах передачи данных необходимо использовать совокупность общих показателей, расположенных в так называемой «матрице 3x3» (таблица 1.2). К такой матрице добавляются показатели надежности службы. Эти показатели не зависят от

типа службы, метода коммутации, протокола установления соединения и протокола передачи сообщений пользователя. Эти показатели ориентированы на пользователей различных служб передачи данных [6].

Таблица 1.2

Совокупность общих показателей качества обслуживания, ориентированных на пользователей служб передачи данных

Функция службы телекоммуникаций	Показатели для критериев оценки качества обслуживания		
	Скорость	Достоверность	Надежность
Доступ	Время доступа	Вероятность неправильного доступа	Вероятность отказа в доступе
Передача сообщений пользователя	Время передачи сообщений пользователя Скорость передачи сообщений пользователя	Вероятность ошибки в сообщениях пользователя Вероятность доставки лишних сообщений пользователя Вероятность ошибочной доставки сообщений пользователя	Вероятность потери сообщений пользователя
Освобождение	Время освобождения	Вероятность преждевременного освобождения	Вероятность отказав освобождении
Критерий отказа Коэффициент готовности службы Среднее время между отказами (или среднее время восстановления)			

Нормы на показатели качества обслуживания рекомендуется разделять на две группы [17]:

a) нормы для показателей, которые могут меняться в процессе эксплуатации и поэтому должны контролироваться;

b) нормы для показателей, которые не меняются в процессе эксплуатации и поэтому могут не контролироваться.

В состав контролируемых показателей обязательно должны входить:

a) вероятность отказа в доступе;

b) время передачи сообщений пользователя;

c) вероятность ошибки в сообщениях пользователя.

Однако в настоящее время информационная безопасность не имеет количественной оценки, хотя большая часть других показателей качества обслуживания, как уже говорилось выше, имеют количественные оценки.

Современные операторы телекоммуникаций являются коммерческими компаниями, а их основным товаром являются услуги, поэтому основной бизнес-задачей операторов телекоммуникаций является повышение прибыльности своего бизнеса за счёт увеличения доходной части и снижения расходной части.

Международная практика показывает, что увеличить доходную часть операторов телекоммуникаций можно, предложив новые услуги, в том числе по обеспечению информационной безопасности. Проблема информационной безопасности – это, в первую очередь, проблема бизнеса оператора телекоммуникаций, а не технологий.

В настоящее время приоритетным направлением международных организаций ISO, ITU, ETSI и др. является разработка стандартов и рекомендаций, связанных с уменьшением рисков информационной безопасности, которые сопутствуют внедрению и эксплуатации ОСТ, поэтому важной задачей является исследование процессов стандартизации в области

информационной безопасности, включая анализ эволюции стандартов с точки зрения их бизнес-приложений.

Построив бизнес-модель функционирования ОСТ, включающую также процесс управления информационной безопасностью, необходимо определить список международных стандартов, поддерживающих эту модель, и разработать спецификацию технических средств для неё. В связи с этим для обеспечения информационной безопасности необходимо чёткое понимание бизнес-целей и особенностей бизнес-процессов операторов телекоммуникаций, а также эффективности от выделяемых на обеспечение информационной безопасности ресурсов. Однако из-за отсутствия критериев, показателей оценки информационной безопасности и, соответственно, методов её количественной оценки в настоящее время неизвестен ответ на вопрос «Сколько будет стоить обеспечение информационной безопасности в конкретных ОСТ и во что может обойтись игнорирование его?». Как правило, операторы телекоммуникаций, не зная какой будут иметь в конечном итоге выигрыш от повышения уровня безопасности ОСТ, не могут предъявлять научно-обоснованные требования к системе обеспечения информационной безопасности в составе требований к ОСТ.

Таким образом, существующая неопределенность в проблеме анализа риска информационной безопасности ОСТ во многом связана с тем, что:

a) до конца прошлого века ОСТ, реализованные на базе аппаратных средств, подвергались только угрозам несанкционированного доступа к содержанию информации, то есть нарушению конфиденциальности информации;

b) отсутствовали преднамеренные угрозы безопасности, связанные с несанкционированным доступом к ОСТ, и, соответственно, с нарушением целостности и доступности;

c) не предъявлялись требования к защите ОСТ от несанкционированного доступа к ним и передаваемой по ним информации;

d) при отсутствии вышеуказанных угроз не было необходимости исследовать вопросы, связанные с оценкой информационной безопасности ОСТ;

e) отсутствовали критерии, количественные показатели (характеристики) степени информационной безопасности.

Стратегическим направлением работ в области обеспечения информационной безопасности становится использование системного подхода к самой проблеме информационной безопасности и ее оценке в частности. Понятие системного подхода интерпретируется как создание соответствующих мер и механизмов обеспечения информационной безопасности, а также регулярность процесса, осуществляемого на всех стадиях жизненного цикла ОСТ при комплексном подходе к использованию всех мер, мероприятий, методов и средств обеспечения информационной безопасности.

Системный подход предполагает, что информационная безопасность от возможных угроз нарушителя должна планироваться для элементов ОСТ на всех этапах:

a) *на этапе проектирования*:

- определение перечня и стоимости информационных ресурсов, подлежащих защите;

- анализ технологий, используемых на ОСТ, как объекта защиты и определение в ней в соответствии с заданной моделью (поведения) потенциального нарушителя максимально возможного количества каналов несанкционированного доступа к информации и возможных воздействий случайного характера;

- разработка средств защиты, перекрывающих выявленные каналы несанкционированного доступа и обеспечивающих заданный уровень безопасности информации;

- разработка средств функционального контроля системы, повышения достоверности и резервирования информации;

- создание и/или поиск и внедрение готовых средств контроля и управления безопасностью информации в данной системе;

- оценка уровня ожидаемой эффективности (прочности) защиты на предмет соответствия заданным требованиям;

b) *на этапе внедрения*:

- настройка параметров и характеристик системы;

- выбор режимов функционирования системы;

- определение реальных характеристик системы;

c) *на этапе эксплуатации и сопровождения*:

- контроль и поддержка функционирования системы безопасности информации в данной ОСТ;

- своевременное предупреждение, обнаружение и блокировка несанкционированного доступа;

- регистрация и учет всех обращений к защищаемой информации, документирование, ведение статистики и прогнозирование несанкционированного доступа;

- поиск и внедрение новых, более совершенных средств, существенно повышающих защищенность системы и/или удобство эксплуатации системы безопасности.

Таким образом, требуемый уровень информационной безопасности ОСТ может быть достигнут только на основе системного подхода на всех этапах разработки и создания ОСТ и в процессе ее функционирования. Кроме того, при решении задач обеспечения информационной безопасности ОСТ обязательным является комплексный подход. Его идея заключается в рациональном сочетании различных организационных и программно-технических мер и средств с учетом требований действующих нормативно-правовых и нормативно-технических документов. Однако на практике эту «комплексность» обеспечить совсем не просто. При создании комплексной системы необходимо защищать информацию во всех фазах ее существования.

В комплексной системе защищать информацию необходимо не только от несанкционированного доступа к ней, но и от несанкционированного вмешательства в процесс ее обработки, хранения и передачи, попыток нарушения работоспособности программно-технических средств и т.п.

1.3 Обзор стандартов в области оценки информационной безопасности

1.3.1 O'zDSt ISO/IEC 15408:2005 «Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий»

На основе международного стандарта ISO/IEC 15408 был разработан государственный стандарт Узбекистана O'zDSt ISO/IEC 15408:2005 "Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий", часто в литературе называемый "Общие критерии".Этот стандарт состоит из трех частей:

a) O'zDSt ISO/IEC 15408-1:2005 "Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий". Введение и общая модель [20];

b) O'zDSt ISO/IEC 15408-2:2005 "Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий". Функциональные требования безопасности [21];

c) O′zDSt ISO/IEC 15408-3:2005 "Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий". Требования доверия к безопасности [22].

На рис.1.11 представлена определяемая стандартом взаимосвязь высокоуровневых понятий в области информационной безопасности. Безопасность связана с защитой активов информационных систем от угроз. За сохранность рассматриваемых активов отвечают их владельцы, для которых эти активы имеют ценность. Существующие или предполагаемые

нарушители также могут придавать значение этим активам и стремиться использовать их вопреки интересам их владельца. Владельцы будут воспринимать подобные угрозы как потенциал воздействия на активы, приводящего к понижению их ценности для владельца.

Стандарт разработан таким образом, чтобы удовлетворить потребности трех групп специалистов: разработчиков, экспертов по сертификации и пользователей объекта оценки. Под объектом оценки понимаются "подлежащие оценке продукт информационных технологий или система с руководствами администратора и пользователя". К таким объектам относятся, например,

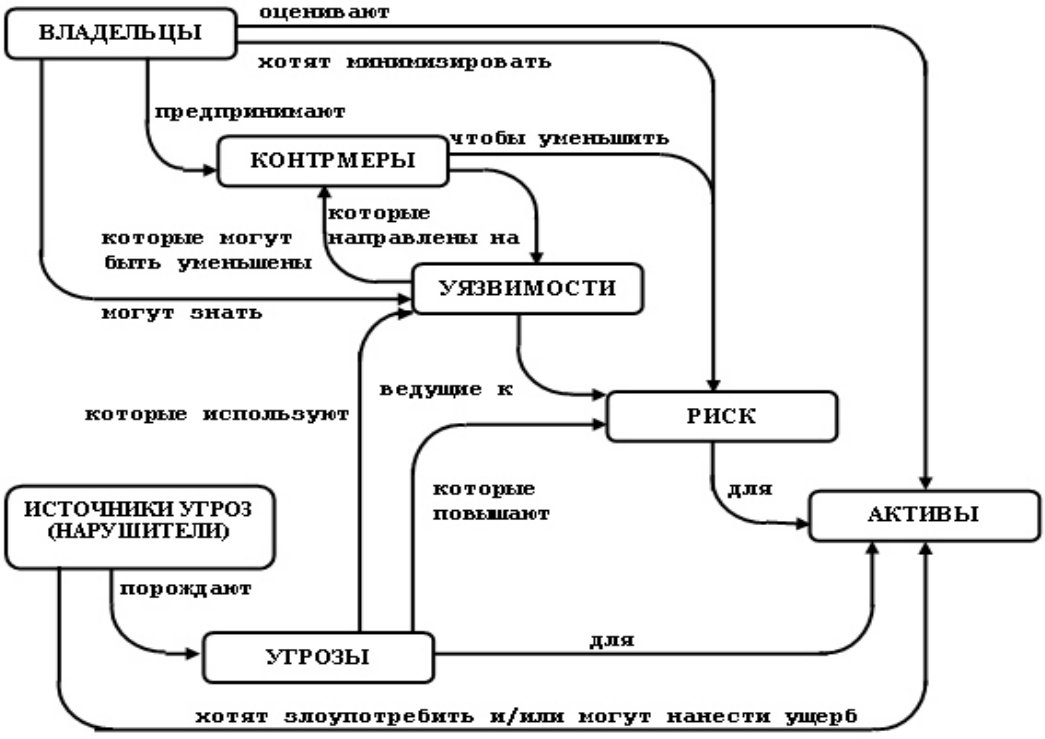

Рис.1.11 - Понятия безопасности и их взаимосвязь в соответствии с O'z DSt ISO/IEC 15408

операционные системы, прикладные программы, информационные системы и т.д.

В поддержку стандарта ISO/IEC 15408 под эгидой ISO разработан целый ряд нормативно-методических документов. Среди них:

a) руководство по разработке профилей защиты и заданий по безопасности;

b) процедуры регистрации профилей защиты;

c) общая методология оценки безопасности информационных технологий [21].

"Общие критерии" предусматривают наличие двух типов требований безопасности - функциональных и доверия. Функциональные требования относятся к сервисам безопасности, таким как идентификация, аутентификация, управление доступом, аудит и т.д. Требования доверия к безопасности относятся к технологии разработки, тестированию, анализу уязвимостей, поставке, сопровождению, эксплуатационной документации и т.д.

Описание обоих типов требований выполнено в едином стиле: они организованы в иерархию "класс - семейство - компонент - элемент". Термин "класс" используется для наиболее общей группировки требований безопасности, а элемент - самый нижний, неделимый уровень требований безопасности.

В стандарте выделены 1.11 классов функциональных требований:

a) аудит безопасности;
b) связь (передача данных);
c) криптографическая поддержка (криптографическая защита);
d) защита данных пользователя;
e) идентификация и аутентификация;
f) управление безопасностью;
g) приватность (конфиденциальность);
h) защита функций безопасности объекта;
i) использование ресурсов;
j) доступ к объекту оценки;
k) доверенный маршрут/канал.

При описании стандарта также необходимо отметить используемое в нем понятие «Стойкость функции безопасности» (СФБ), которое определяется как «характеристика функции безопасности объекта оценки, выражающая минимальные усилия, предположительно необходимые для нарушения ее ожидаемого безопасного поведения при прямой атаке на лежащие в ее основе механизмы безопасности». Процедуры анализа стойкости функции безопасности объекта оценки и анализа уязвимостей используют понятие «потенциал нападения». Потенциал нападения - прогнозируемый потенциал для успешного (в случае реализации) нападения, выраженный в показателях компетентности, ресурсов и мотивации.

СФБ может быть базовой, средней и высокой.

Базовая стойкость означает, что функция обеспечивает адекватную защиту от случайного нарушения безопасности объекта оценки нарушителем с низким потенциалом нападения.

Средняя стойкость - функция обеспечивает защиту от целенаправленного нарушения безопасности объекта оценки нарушителем с умеренным потенциалом нападения.

Высокая стойкость - уровень стойкости функции безопасности объекта оценки, на котором она обеспечивает защиту от тщательно спланированного и организованного нарушения безопасности объекта оценки нарушителем с высоким потенциалом нападения.

«Общие критерии» применительно к оценке безопасности изделий информационных технологий являются, по сути, метасредствами, задающими систему понятий, в терминах которых должна производиться оценка, но не предоставляющих конкретных наборов требований и критериев, подлежащих обязательной проверке. Эти требования и критерии фигурируют в профилях защиты и заданиях по безопасности.

Как показывают оценки специалистов в области информационной безопасности, «Общие критерии» представляют собой по уровню

систематизации, полноте и возможностям детализации требований, универсальности и гибкости в применении наиболее совершенный из существующих в настоящее время стандартов в области ИТ. Причем, что очень важно, в силу особенностей построения он имеет практически неограниченные возможности для развития и представляет собой базовый стандарт, содержащий методологию задания требований и оценки безопасности, но опять же только для ИТ. В области телекоммуникаций «Общие критерии» не позволяют провести оценку влияния механизмов защиты на общий уровень информационной безопасности ОСТ, оценить уровень информационной безопасности ОСТ с учетом возможного наличия уязвимостей. Ни один из критериев не содержит количественных оценок, не приведено никаких примеров использования всех критериев, а также отсутствует обоснование и подтверждение необходимости и достаточности данной системы критериев [21].

1.3.2 ISO/IEC 27001:2005 «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования» и ISO/IEC 27002:2005 «Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью»

В 1995 году Британским институтом стандартов (BSI) была опубликована первая часть стандарта BS 7799 "Code of Practice for Information Security Management" (название обычно переводится как "Практические правила управления информационной безопасностью"). На его основе в 2000 году был принят международный стандарт ISO/IEC 17799:2000 "Information technology. Code of practice for information security management". Следующая дополненная версия была принята в 2005 году и обозначается ISO/IEC 17799:2005. А в 2007 году данный стандарт был

переиздан под номером ISO/IEC 27002. Как следует из названия, он описывает рекомендуемые меры в области управления информационной безопасностью и, в целом, не предназначался для проведения сертификации систем на его соответствие [23].

В 1999 году была опубликована вторая часть стандарта BS 7799 "Information Security Management Systems - Specification with guidance for use" (Системы управления информационной безопасностью - спецификации с руководством по использованию). На его базе был разработан стандарт ISO/IEC 27001:2005 "Information Technology. Security techniques. Information security management systems. Requirements", на соответствие которому может проводиться сертификация.

В Республике Узбекистан на данный момент действуют стандарты O'zDSt ISO/IEC 27002:2008 «Информационная технология. Практические правила управления информационной безопасностью» (аутентичный перевод ISO/IEC 27002:2007)[21] и O'zDSt ISO/IEC 27001:2009 «Информационная технология. Методы и средства обеспечения безопасности. Системы управления информационной безопасностью. Требования» (перевод ISO/IEC 27001:2005)[23]. Несмотря на некоторые внутренние расхождения, связанные с разными версиями и особенностями перевода, наличие этих стандартов позволяет привести систему управления информационной безопасностью в соответствие их требованиям и, при необходимости, сертифицировать.

Согласно данным стандартам, цель информационной безопасности - обеспечить бесперебойную работу организации, по возможности предотвратить и/или минимизировать ущерб от нарушений безопасности.

Управление информационной безопасностью позволяет коллективно использовать данные, одновременно обеспечивая их защиту и защиту вычислительных ресурсов.

Подчеркивается, что защитные меры оказываются значительно более дешевыми и эффективными, если они заложены в информационные системы и сервисы на стадиях задания требований и проектирования.

Предлагаемые в стандарте ISO/IEC 27002 регуляторы безопасности разбиты на десять групп:

a) политика безопасности;

b) общеорганизационные аспекты защиты;

c) классификация активов и управление ими;

d) безопасность персонала;

e) физической безопасности и безопасность окружающей среды;

f) администрирование систем и сетей;

g) управление доступом к системам и сетям;

h) разработка и сопровождение информационных систем;

i) управление бесперебойной работой организации;

j) контроль соответствия требованиям.

В стандарте выделяется десять ключевых регуляторов, которые либо являются обязательными в соответствии с действующим законодательством, либо считаются основными структурными элементами информационной безопасности. К ним относятся:

a) документ о политике информационной безопасности;

b) распределение обязанностей по обеспечению информационной безопасности;

c) обучение и подготовка персонала к поддержанию режима информационной безопасности;

d) уведомление о случаях нарушения защиты;

e) антивирусные средства;

f) процесс планирования бесперебойной работы организации;

g) контроль за копированием программного обеспечения, защищенного законом об авторском праве;

h) защита документации;

i) защита данных;

j) контроль соответствия политике безопасности.

Для обеспечения повышенного уровня защиты особо ценных ресурсов или оказания противодействия злоумышленнику с исключительно высоким потенциалом нападения могут потребоваться другие (более сильные) средства, которые в стандарте не рассматриваются.

Следующие факторы выделены в качестве определяющих для успешной реализации системы информационной безопасности в организации:

a) цели безопасности и ее обеспечение должны основываться на производственных задачах и требованиях. Функции управления безопасностью должно взять на себя руководство организации;

b) необходима явная поддержка и приверженность к соблюдению режима безопасности со стороны высшего руководства;

c) требуется хорошее понимание рисков (как угроз, так и уязвимостей), которым подвергаются активы организации, и адекватное представление о ценности этих активов;

d) необходимо ознакомление с системой безопасности всех руководителей и рядовых сотрудников организации.

Во второй части стандарта ISO/IEC 27001 "Системы управления информационной безопасностью - спецификация с руководством по использованию" предметом рассмотрения, как следует из названия, является система управления информационной безопасностью.

Под системой управления информационной безопасностью (СУИБ) (Information Security Management System, ISMS) понимается часть общей системы управления, базирующаяся на анализе рисков и предназначенная для проектирования, реализации, контроля, сопровождения и совершенствования мер в области информационной безопасности. Эту систему составляют

организационные структуры, политика, действия по планированию, обязанности, процедуры, процессы и ресурсы.

В основу процесса управления положена четырехфазная модель, включающая:

a) планирование;

b) реализацию;

c) оценку;

d) корректировку.

Процесс управления имеет циклический характер; на фазе первоначального планирования осуществляется вход в цикл. В качестве первого шага должна быть определена и документирована политика безопасности организации. Затем определяется область действия системы управления информационной безопасностью (СУИБ). Она может охватывать всю организацию или ее части. Следует специфицировать зависимости, интерфейсы и предположения, связанные с границей между СУИБ и ее окружением; это особенно важно, если в область действия попадает лишь часть организации. Большую область целесообразно поделить на подобласти управления.

Ключевым элементом фазы планирования является анализ рисков. Результат анализа рисков - выбор регуляторов безопасности. Фаза планирования должна включать график и приоритеты, детальный рабочий план и распределение обязанностей по реализации этих регуляторов.

На второй фазе - фазе реализации - руководством организации выделяются необходимые ресурсы (финансовые, материальные, людские, временные), выполняются реализация и внедрение выбранных регуляторов, сотрудникам объясняют важность проблемы информационной безопасности, проводятся курсы обучения и повышения квалификации. Основная цель этой фазы - ввести риски в рамки, определенные планом.

Назначение фазы оценки - анализ эффективности работы регуляторов и СУИБ в целом. Кроме того, следует принять во внимание изменения, произошедшие в организации и ее окружении, способные повлиять на результаты анализа рисков. При необходимости намечаются корректирующие действия, предпринимаемые в четвертой фазе. Коррекция должна производиться, только если выполнено по крайней мере одно из двух условий:

a) выявлены внутренние противоречия в документации СУИБ;

b) риски вышли за допустимые границы.

Оценка может выполняться в нескольких формах:

a) регулярные (рутинные) проверки;

b) проверки, вызванные появлением проблем;

c) изучение опыта (положительного и отрицательного) других организаций;

d) внутренний аудит СУИБ;

e) инспекции, проводимые по инициативе руководства;

f) анализ тенденций.

Аудит должен выполняться регулярно, не реже одного раза в год. В процессе аудита следует убедиться в следующем:

a) политика безопасности соответствует производственным требованиям;

b) результаты анализа рисков остаются в силе;

c) документированные процедуры выполняются и достигают поставленных целей;

d) технические регуляторы безопасности (например, межсетевые экраны или средства ограничения физического доступа) расположены должным образом, правильно сконфигурированы и работают в штатном режиме;

e) действия, намеченные по результатам предыдущих проверок, выполнены.

Даже если не выявлено недопустимых отклонений и уровень безопасности признан удовлетворительным, целесообразно зафиксировать изменения в технологии и производственных требованиях, появление новых угроз и уязвимостей, чтобы предвидеть будущие изменения в СУИБ.

СУИБ надо постоянно совершенствовать, чтобы она оставалась эффективной. Эту цель преследует четвертая фаза рассматриваемого в стандарте цикла - корректировка. Она может потребовать как относительно незначительных действий, так и возврата к фазам планирования (например, если появились новые угрозы) или реализации (если следует осуществить намеченное ранее).

При корректировке прежде всего следует устранить несоответствия следующих видов:

a) отсутствие или невозможность реализации некоторых требований СУИБ;

b) неспособность СУИБ обеспечить проведение в жизнь политики безопасности или обслуживать производственные цели организации.

Задача фазы оценки - выявить проблемы. На фазе корректировки необходимо докопаться до их корней и устранить первопричины несоответствий, чтобы избежать повторного появления. С этой целью могут предприниматься как реактивные, так и превентивные действия, рассчитанные на среднесрочную или долгосрочную перспективу.

Важно, что данный стандарт не концентрируется исключительно на конфиденциальности, он обеспечивает также и целостность и доступность. Однако, как и в случае с ISO/IEC 15408 стандарт не позволяют провести оценку влияния механизмов защиты на общий уровень информационной безопасности сетей телекоммуникаций, полностью обойдены вопросы о методиках вычисления уровня риска и ценности ресурсов с учетом того, что

в каждом конкретном случае потери различны. Отсутствие меры степени безопасности не позволяет задать требуемый уровень информационной безопасности [22].

1.3.3 ISO/IEC 31010:2009, «Управление рисками - методы оценки рисков»

ISO/IEC 31010:2009 был разработан ИСО совместно с ее партнером МЭК (IEC, International Electrotechnical Commission / Международная Электротехническая комиссия) [29].

ISO/IEC 31010:2009 будет оказывать помощь организациям в осуществлении управления рисками, принципы и руководящие указания в недавно опубликованном ISO 31000:2009, дополняются Руководством ИСО 73:2009 лексикой по управлению рисками.

В новом стандарте приведены:

a) концепция оценки рисков;

b) процесс оценки рисков;

c) выбор методов оценки рисков.

Стандарт отражает текущую практику и дает ответы на следующие вопросы:

a) что может произойти и почему?

b) каковы последствия?

c) какова вероятность их появления в будущем?

d) существуют ли какие-либо факторы, смягчающие последствия риска или снижению появления риска?

Вводится применение целого ряда методов, с конкретными ссылками на другие международные стандарты, где концепция и применение методов описаны более подробно. Оценка рисков не является автономной деятельности и должны быть полностью интегрирована в другие компоненты процесса управления рисками.

ISO/IEC 31010 разработан для применения как новичкам в управлении рисками, так и для опытных профессионалов. Он является составной частью интегрированной структуры стандартов по управлению рисками, разработанный с целью предоставления "лучшего практического" подхода.

1.4 Современные подходы к оценке рисков информационной безопасности оптических сетей телекоммуникации

1.4.1 Основные подходы к оценке рисков информационной безопасности оптических сетей телекоммуникаций

В настоящее время, наряду с традиционными угрозами несанкционированного доступа к содержанию передаваемых сообщений, появились новые угрозы, связанные с нарушением безопасного функционирования и целостности ОСТ, поэтому проблема оценки рисков информационной безопасности ОСТ является крайне важной и актуальной.

Анализ ОСТ как объектов информационной безопасности, моделей их функционирования, источников угроз безопасности и уязвимостей, а также различных методов и средств информационной безопасности показывает, что одной из важнейших проблем информационной безопасности ОСТ является отсутствие объективний методов количественной оценки рисков состояния их безопасности. Поэтому для решения проблем, связанных с количественной оценкой рисков информационной безопасности необходимо глубоко разобраться сущностью проблемы и сформулировать цели, задачи и пути их решения с учетом особенностей ОСТ.

Ключевым аспектом решения проблемы создания и развития защищенных ОСТ является разработка требований, показателей и критериев оценки уровня их безопасности. Здесь необходимо отметить, что оценка рисков информационной безопасности ОСТ должна проводиться в три этапа:

a) оценка оптических телекоммуникационных технологии, внедряемых на ОСТ, с точки зрения информационной безопасности;

b) сертификация аппартно-программного комплекса, внедряемого на ОСТ по требованиям безопасности информации;

c) аудит информационной безопасности ОСТ с целью проверки соответствия достигнутого уровня их информационной безопасности, заданному в техническом задании на их разработку.

В этой связи существует острая необходимость выработки общей технической политики и создания нормативной базы, методологического и инструментального обеспечения в области оценки рисков информационной безопасности. Также особого внимания заслуживает то, что в последнее время по мере расширения масштабов и сфер применения программных средств в оптических системах и сетях телекоммуникаций появилось много новых угроз безопасности, аналогичных тем, которые возникают в информационно-вычислительных системах. Вследствие этого, во многих случаях использование методик, разработанных для сферы информационных технологий, допустимо и в области телекоммуникаций.

На практике наибольшее распространение получили два основных подхода к оценке риска информационной безопасности ОСТ.

Первый из них основан на проверке соответствия уровня защищенности ОСТ строго определенным требованиям одного из стандартов или руководящих документов в области информационной безопасности, так называемые качественные методы оценки рисков информационной безопасности.

Второй подход к оценке рисков информационной безопасности ОСТ основывается на определении числовых характеристик информационной безопасности – это так называемые количественные методы оценки рисков информационной безопасности. Поскольку само понятие «информационная безопасность» как одно из свойств ОСТ не имеет количественных

показателей, для ее оценки в основном используются либо статистические показатели, заимствованные из предметных областей надежности технических и программных систем, либо оценка рисков информационной безопасности.

Основной задачей оценки рисков информационной безопасности ОСТ является разработка методологии задания угроз ИБ для этих сетей и определение потерь (ущерба) пользователей и операторов этих сетей вследствие реализации той или иной угрозы ИБ.

Теоретические и практические методы реализации потенциальных возможностей защиты процесса передачи информации от его блокирования в решающей степени определяются показателями эффективности использования различных средств защиты информации, общая методология получения (определения) которых практически отсутствует. В настоящее время не существует общепринятых методов оценки рисков ИБ ОСТ, поэтому сравнение защищенности различных ОСТ чрезвычайно затруднено. Такое положение определяется, с одной стороны, спецификой ОСТ как объекта оценки, а с другой стороны спецификой предметной области обеспечения ИБ оптических технологий телекоммуникаций.

Специфика ОСТ, как объекта оценки, определяется присутствием в них в качестве определяющего - компонента программного обеспечения, реализующего протоколы функционирования сетей. Ввиду большой функциональной, структурной и логической сложности программного обеспечения на практике невозможно в полном объеме оценить его поведение во всем возможном диапазоне применения. Значительно сложнее также, в отличие от объектов, имеющих физическую природу, использовать результаты оценок, полученных в одних условиях, для прогноза поведения технологий телекоммуникаций в других условиях.

Предметная область ИБ технологий телекоммуникаций обладает той особенностью, что при ее оценке приходится применять как объективные,

так и субъективные критерии. Оцениваемые характеристики ИБ технологий телекоммуникаций могут иметь как детерминированную, так и случайную природу. В силу указанных обстоятельств получение точных и универсальных оценок показателей ИБ технологий телекоммуникаций является практическим невозможным. В то же время получение объективной оценки рисков уровня ИБ технологий телекоммуникаций является насущной необходимостью в целях принятия обоснованных решений о возможности использования тех или иных средств защиты информации в составе систем обеспечения информационной безопасности (СОИБ) ОСТ. Причем эти оценки должны обладать свойствами сравнимости и повторяемости, чтобы быть доказательными при анализе альтернативных вариантов СОИБ ОСТ и оценке уровней ИБ на различных этапах их жизненного цикла.

При оценке ИБ ОСТ вводится понятие риска R, под которым понимается вероятный ущерб, зависящий от защищенности сети.

Оценка рисков ИБ ОСТ выполняется либо количественно (риск измеряется в денежных единицах), либо - качественно (по уровням риска: высокий, средний, низкий).

Для создания оптимальных по критерию эффективность/стоимость СОИБ ОСТ от различных угроз необходимо знать, где и в какой степени уязвимы эти сети. Двумя ключевыми элементами при оценке риска является определение последствий угроз, то есть оценка стоимости ущерба и вероятности его нанесения. Используя эти два параметра можно определить риск в терминах затрат в единицу времени. Предложенная методика оценки риска заключается в:

a) составлении списка возможных угроз;

b) определении оценки ущерба в денежных единицах (по порядку величины) при реализации каждой угрозы;

c) оценке частоты реализации каждой угрозы.

1.4.2 Качественный подход к оценке рисков информационной безопасности оптических сетей телекоммуникации

Качественные методологии, используемые для оценки ИБ ОСТ, исходят из того, что зачастую потенциальные потери неосязаемы, поэтому опасность или риск ИБ ОСТ в результате реализации той или иной угрозы ИБ нельзя представить в денежном выражении. При качественном подходе результаты риска скорее выражаются словесно, чем численно: от «нет опасности» до «очень большая опасность».

В настоящее время известно множество методов качественной оценки рисков, большинство из которых построено на использовании таблиц. Такие методы сравнительно просты в использовании и достаточно эффективны. Однако не стоит говорить о «лучшем» методе, так как для различных случаев они будут разными. Важно из имеющегося многообразия методов выбрать именно тот, который обеспечивал бы воспроизводимые результаты для данной ОСТ.

Некоторые качественные подходы оценивают результаты анализа риска ИБ ОСТ эффективнее всего, выражая его математически в виде скалярной величины с описанием условий для каждой точки. Другие подходы предлагают графическое изображение дерева решения, которое показывает распределение вероятностей самых общих случаев.

Ни одно из указанных направлений не способно в отдельности обеспечить получение объективной, представительной и конструктивной оценки ИБ ОСТ. Задача выбора эффективной критериальной основы оценки ИБ технологий телекоммуникаций заключается в определении рационального сочетания этих направлений и в правильном выборе частных показателей ИБ технологий телекоммуникаций. В наиболее полном и законченном виде качественные критерии оценки безопасности информационных технологий представлены в международном стандарте

«Общие критерии оценки безопасности информационных технологий», явившегося прообразом стандарта O'z DSt ISO/IEC 15408:2008.

Существует несколько моделей качественной оценки. Все они достаточно просты. Варианты различаются лишь количеством градаций риска. Одна из самых распространенных моделей - трехступенчатая. Каждый фактор оценивается по шкале «низкий - средний – высокий».

Некоторые эксперты в области ИБ считают, что трех ступеней для точного разделения рисков недостаточно и предлагают пятиуровневую модель. Однако это не принципиально, ведь в целом любая модель анализа сводится к простейшему разделению угроз на критические и второстепенные. Трех, пятиуровневые и прочие модели используются для наглядности. При работе с моделями с большим числом градаций, например с пятью, у аналитиков могут возникнуть затруднения - отнести риск к пятой или к четвертой группе. Качественная оценка допускает подобные «ошибки», поскольку является саморегулирующейся. Не критично, если первоначально риск необоснованно отнесли к четвертой категории вместо пятой. Качественный подход позволяет проводить анализ за считанные минуты. Предполагается, что такая оценка рисков будет осуществляться регулярно. И уже на следующем шаге категории будут переназначены, фактор перейдет в пятую группу, поэтому качественная оценка также называется итерационным методом.

При использовании качественных шкал числовые значения заменяются на эквивалентные им понятийные уровни. Каждому понятийному уровню в этом случае будет соответствовать определённый интервал количественной шкалы оценки. Количество уровней может варьироваться в зависимости от применяемых методик оценки рисков. В таблицах 1.3 и 1.4 приведены примеры качественных шкал оценки рисков информационной безопасности, в которых для оценки уровней ущерба и вероятность реализации угрозы используется пять понятийных уровней.

При использовании качественных шкал для вычисления уровня риска применяются специальные таблицы, в которых в первом столбце задаются понятийные уровни ущерба, а в первой строке – уровни вероятности реализации угрозы. Ячейки же таблицы, расположенные на пересечении первой строки и столбца, содержат уровень риска безопасности. Размерность таблицы зависит от количества концептуальных уровней вероятности реализации угрозы и ущерба.

Таблица 1.3

Качественная шкала оценки уровня ущерба

Уровень ущерба	Описание
1 Малый ущерб	Приводит к незначительным потерям материальных активов, которые быстро восстанавливаются, или к незначительному влиянию на репутацию компании
2 Умеренный ущерб	Вызывает заметные потери материальных активов или к умеренному влиянию на репутацию компании
3 Ущерб средней тяжести	Приводит к существенным потерям материальных активов или значительному урону репутации компании
4 Большой ущерб	Вызывает большие потери материальных активов и наносит большой урон репутации компании
5 Критический ущерб	Приводит к критическим потерям материальных активов или к полной потере репутации компании на рынке, что делает невозможным дальнейшую деятельность организации

В методиках качественной оценки рисков, как правило, используются субъективные критерии, измеряемые в качественных шкалах, поскольку:

a) оценка должна отражать субъективную точку зрения владельца информационных ресурсов;

b) должны быть учтены различные аспекты, не только технические, но и организационные, психологические, и т.д.;

c) для получения субъективной оценки при оценке риска выхода из строя сети телекоммуникаций можно использовать либо прямую экспертную оценку, либо определить функцию, отображающую объективные данные (вероятность) в субъективную шкалу рисков;

Таблица 1.4

Качественная шкала оценки вероятности реализации угрозы

Уровень вероятности реализации угрозы	Описание
1 Очень низкая	Угроза практически никогда не будет реализована. Уровень соответствует числовому интервалу вероятности (0; 0,25)
2 Низкая	Вероятность реализации угрозы достаточно низкая. Уровень соответствует числовому интервалу вероятности (0,25; 0.5)
3 Средняя	Вероятность реализации угрозы приблизительно равна 0,5
4 Высокая	Угроза скорее всего будет реализована. Уровень соответствует числовому интервалу вероятности (0,5; 0.75)
5 Очень высокая	Угроза почти наверняка будет реализована. Уровень соответствует числовому интервалу вероятности (0,75; 1)

d) субъективные шкалы могут быть количественными и качественными, но на практике, как правило, используются качественные шкалы от трех до семи градаций. С одной стороны, это просто и удобно, с другой – требует грамотного подхода к обработке данных.

Пример таблицы, на основе которой можно определить уровень риска, приведён ниже (табл.1.5) .

Таблица 1.5

Пример таблицы определения уровня риска информационной безопасности

Вероятность реализации угрозы / Ущерб	Очень низкая	Низкая	Средняя	Высокая	Очень высокая
Малый ущерб	Низкий Риск	Низкий риск	Низкий риск	Средний риск	Средний риск
Умеренный ущерб	Низкий Риск	Низкий риск	Средний риск	Средний риск	Высокий риск
Ущерб средней тяжести	Низкий Риск	Средний риск	Средний риск	Средний риск	Высокий риск
Большой ущерб	Средний риск	Средний риск	Средний риск	Средний риск	Высокий риск
Критический ущерб	Средний риск	Высокий риск	Высокий риск	Высокий риск	Высокий риск

1.4.3 Количественный подход к оценке рисков информационной безопасности оптических сетей телекоммуникации

Рациональное применение разнообразных средств защиты информации в ОСТ с учетом критерия экономической эффективности – это сложная научно-техническая задача. Умножая величину ущерба на число вероятных реализаций угрозы получают грубую уровень риска от данной угрозы. По этим данным можно определить целесообразность применения системы защиты с точки зрения критерия эффективность/стоимость. Если затраты на

систему защиты меньше ущерба от угрозы, то применять эту систему защиты целесообразно [6].

Критическим шагом при принятии решения о применении защиты информации является определение ценности информации. Для оценки рисков ИБ требуются не только распределение информации по категориям в соответствии с ее ценностью, но и учет того, что одна и та же информация для разных групп потребителей может иметь различную ценность. Так же как ценность информации может быть различной для разных групп, так и последствия, связанные с совершением некоторых операций над информацией, могут быть различными в зависимости от вида операций. При оценке угроз специалист хочет знать, каковы будут экономические последствия (обычно они выражаются как потери или утраты), если над определенной информацией будут произведены некоторые операции. В процессе определения ценности информации необходимо учитывать свойства самой информации, возможные угрозы и заинтересованную сторону. Оценка угроз проводится для того, чтобы определить затраты по выполнению определенных действий с информацией.

Количественный подход требует значительно больше времени, так как каждому фактору риска присваивается конкретное значение. Результаты количественного анализа могут быть более полезны для бизнес-планирования.

Для количественной оценки рисков необходимо оценивать частотность потерь и стоимость потерь (распределение величины потерь), зависящую от стоимости информационных ресурсов. При оценке величины риска необходимо иметь в виду не только непосредственные расходы на замену оборудования или восстановление информации, но и величину ущерба, нанесенного процессам ОСТ, посредством которых они выполняют свои функции. Еще имеются более отдаленные от факторов риска по причинно-следственной цепочке, но и более сильные по воздействию последствия -

потеря репутации операторов телекоммуникаций, ослабление надежности ОСТ.

Для определения стоимости информационных ресурсов (активов) может быть использована, например, шкала типа:

a) *низкая стоимость* - от ресурса не зависят критически важные процессы, он может быть восстановлен с небольшими затратами денежных средств и времени;

b) *средняя стоимость* - от ресурса зависит ряд важных функций процессов, ресурс может быть восстановлен за допустимое время, стоимость восстановления средняя;

c) *высокая стоимость* - от ресурса зависят критически важные процессы, время восстановления превышает критически допустимое и (или) стоимость восстановления очень высока.

Оценив возможную частотность потерь и уязвимости, можно принять решение относительно выбора средств защиты информации. Достоинство методологии в том, что она позволяет довольно быстро и с точностью, зависящей от квалификации экспертов, расположить риски по приоритетам (отранжировать) и выявить уязвимости.

Классический количественный алгоритм для оценки риска информационных потерь был разработан Национальным институтом стандартов и технологий (США) еще в 1974 г., опубликован в «Guidelines for Automated Data Processing Physical Security and Risk Management, NIST FIPSPUB-65, 1974» (Руководящие принципы управления рисками и физической безопасностью при автоматизированной обработке данных) и используется по сей день.

Согласно этому алгоритму:

Информационный актив $\times$ *Фактор подверженности воздействию* $\times$ *Ежегодная частота проявления = Ожидаемые ежегодные потери*

Информационный актив (Asset Value, AV) - сущность, составленная из аппаратного и программного обеспечения, накопленных и обрабатываемых данных. Измерять информационные активы можно, оценивая стоимость их разработки, лицензирования, поддержки и замены.

Фактор подверженности воздействию (Exposure Factor, EF) - процент потери, который могла бы принести реализованная угроза на определенном активе (когда определенная угроза совпадает с определенной уязвимостью).

Ожидаемые единоразовые потери (Single Loss Expectancy, SLE). Риск рассчитывается в денежных единицах. Для любой определенной угрозы, мы берем ценность подверженного ей актива и умножаем ее на фактор подверженности. В промежуточном итоге получается ожидаемая при исполнении угрозы потеря, которая и называется ожиданием единичной потери:

$$SLE = EF \times AV . \qquad (1.11)$$

Ежегодная частота проявления (Annual Rate of Occurrence, ARO) - ожидаемое количество проявлений угрозы по отношению к определенному активу: чем больше риск относящийся к угрозе, тем выше ее значение.

Ожидаемые ежегодные потери (Annual Loss Expectancy, ALE).

В итоге можно посчитать ожидаемые за год финансовые потери актива от одной определенной угрозы:

$$ALE = SLE \times ARO . \qquad (1.12)$$

Таким образом получают несложные для использования метрики и формулы для количественной оценки рисков, которые могут быть успешно использованы специалистами, на которых возложено управление рисками.

Основной трудностью практической реализации оценки риска при обеспечении ИБ становится получение исходных данных, необходимых для количественной оценки рисков, поэтому возникает задача создания

определенной системы сбора и обработки информации о проявлении угроз и уровень их последствий, а также задача разработки организационно-методических документов для обработки и объединения этой информации. Необходимые данные можно получить из различных источников – результатов испытаний и подтверждения соответствия, баз данных, мнений специалистов, экспертов и др.

Анализ рассмотренных методик показывает, что для выбора технических средств обеспечения информационной безопасности с учетом экономической эффективности необходимо располагать достаточно представительными данными по угрозам и их последствиям. Только собственники информации (объектов) могут определить необходимые объемы информации (объектов), требующие защиты, и соответствующие затраты, которые для этого необходимы.

В связи с этим актуальной задачей в сфере ОСТ является организация непрерывного и регулярного сбора, обработки и анализа (аудита) информации о воздействиях угроз и их последствиях, охватывающего большое число объектов различных ОСТ.

1.5 Выводы и постановка задачи

На основании проведенного анализа оптических сетей телекоммуникации как объекта оценки рисков информационной безопасности и анализ рисков информационной безопасности оптических сетей телекоммуникации можно сделать следующие выводы:

1. Анализ показывает, что разработка методики оценки информационной безопасности предполагает наличие или разработку:

a) модели объекта оценки;

b) модели системы защиты;

c) модели потенциального нарушителя.

2. В результате анализа рисков информационной безопасности оператор телекоммуникаций получит следующие основные выгоды:

a) определение наиболее проблемных областей в обеспечении информационной безопасности;

b) возможность аргументированного выбора мер по обеспечению информационной безопасности и планирования порядка их применения;

c) получение качественных или количественных характеристик значимости угроз и уязвимостей информационной безопасности, ранжирование активов и угроз по значимости;

d) получение начальной методологической базы, необходимой для реализации процесса управления рисками.

3. При рассмотрение вопроса о защите информации в ОСТ необходимо выделить главным образом несколько аспектов: защита информации от расшифровки; защита оптического сигнала от физического перехвата. В первом случае используются, как правило, разнообразные криптографические методы, а также защита оптического сигнала от дешифровки на физическом уровне, с использованием поляризационных или спектральных методов.

4 Возможно также использование квантовой криптографии, в основе которой лежит понятие фотонов и законов квантовой физики. Применение такого способа защиты возможно в силу того, что оптические волокно ВОЛС позволяет обеспечить передачу фотонов на большие расстояния с минимальными искажением.

5 В целях обеспечения информационной безопасности оптических сетей телекоммуникаций необходимо определить общие требования по безопасности с учетом международных стандартов и рекомендаций, а также методологические основы обеспечения их безопасности.

6 При разработке общих требований по безопасности оптических сетей телекоммуникаций необходимо исходить из перечня наиболее опасных угроз

безопасности, уязвимостей используемых технологий и возможных воздействий нарушителей.

7 Требования по безопасности информации и услуги безопасности взаимосвязаны. Основой для проведения анализа рисков информационной безопасности являются перечни угроз и уязвимостей, оценки вероятностей их появления, а также модель нарушителя.

8 Анализ современных подходов к оценке информационной безопасности показал, что в настоящее время развиваются два основных методических направления: качественные критерии и количественные критерии.

Качественная оценка рисков включает ряд последовательных этапов:

a) выявление факторов, увеличивающих и уменьшающих конкретный вид риска;

b) определение системы оценочных показателей риска, которая должна отвечать требованиям адекватности, комплексности, динамичности, объективности, а также допускать пополнение и развитие;

c) установление потенциальных областей риска, т.е. выявление мероприятий, операций, работ, при выполнении которых может возникнуть неопределенность в получении положительного результата;

d) идентификация всех возможных рисков, т.е. определение возможных рисков в результате данного действия либо бездействия.

Как указывалось ранее, второе направление оценки информационной безопасности сетей телекоммуникаций основывается на определении числовых характеристик информационной безопасности технологий телекоммуникаций (количественные критерии). Методика количественной оценки рисков дает точные цифры возможных потерь при возникновении инцидента информационной безопасности.

Количественный методы требует значительно больше времени, так как каждому фактору риска присваивается конкретное значение; это даёт полную информацию о проведенном анализе ресурсов и объектов.

Постановка задачи диссертации

На основании проведенного анализа информационной безопасности оптических сетей телекоммуникаций, а также практической потребностью защиты передачи информации, целью настоящей диссертации является проведение детальных исследований методов оценки рисков информационной безопасности оптических сетей телекоммуникаций на основе нечетких множеств, анализа методов качественного и количественного оценка рисков информационной безопасности.

Также в диссертационной работе будут рассмотрены следующие задачи:

a) анализ методов оценки рисков информационной безопасности;

b) анализ методов качественных оценки рисков информационной безопасности;

c) анализ методов количественных оценки рисков информационной безопасности;

d) методика использования параметрических алгоритмов для оценки рисков безопасности на основе нечетких множеств;

e) модель и алгоритм оценки рисков информационной безопасности;

f) моделирование оценки рисков информационной безопасности на основе аппарата нечетких множеств;

g) сравнительный анализ методов оценки рисков информационной безопасности оптических сетей телекоммуникации на базе программных продуктов;

h) оценка рисков информационной безопасности на основе теории нечетких множеств с использованием программного продукта MATLAB.

2 МЕТОДЫ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОПТИЧЕСКИХ СЕТЕЙ ТЕЛЕКОММУНИКАЦИИ

2.1 Обзор методов оценки рисков информационной безопасности

Оценка риска во многом субъективна и зависит от умения оператора оценивать ситуацию и принимать решения. И тем не менее в мировой практике существует несколько методов оценки риска. Для верного установления зон и источников риска используют методы качественных и количественных оценок рисков.

Таким образом, весь процесс управления рисками можно отобразить следующим образом (рис.2.1):

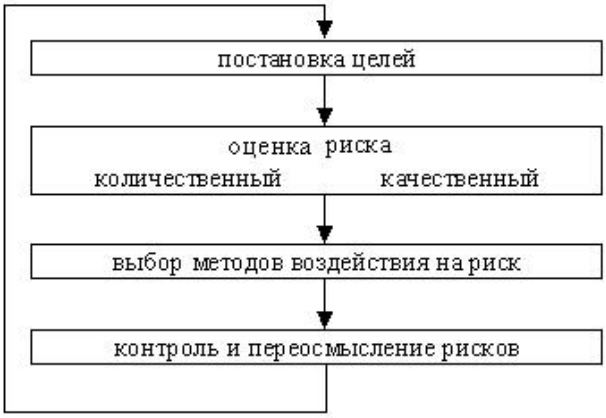

Рис.2.1 - Процесс исследования риска

На каждом из этапов используются свои методы исследования рисков, каждый из них по отдельности дает результаты, являющиеся исходными данным и для последующих этапов, что требует объединения этих этапов в систему. Это позволит максимально эффективно добиваться целей, поставленных перед организацией, поскольку информация, получаемая на каждом из этапов, позволяет корректировать не только методы воздействия на риск, но и переосмысливать цели, ставящиеся перед организацией.

К методам качественных оценок относятся следующие методы

При качественной оценке риска используемые методы можно разделить на четыре группы:

1. Методы, базирующиеся на анализе имеющейся информации:

- рассмотрение и анализ первичных документов финансовой и управленческой;

- анализ данных периодических (годовых, квартальных) отчетов организаций.

2. Методы сбора новой информации:

- стандартизированный опросный лист;

- персональные инспекционные посещения производственных подразделений организации;

- консультации со специалистами, как работающими в самой организации, так и внешними.

3. Методы моделирования деятельности организации:

- составление и анализ диаграммы организационной структуры организации;

- анализ карты потоков, отражающей технологические потоки производственных процессов.

4. Эвристические методы качественного анализа.

К методам количественной оценки относятся следующие методы [11]

На основе количественного анализа и оценки рисков, можно составить следующую классификацию методов:

1. Аналитические методы:

- анализ чувствительности;

- анализ сценариев.

2. Вероятностно-теоретические методы:

- статистические методы;

- имитационное моделирование (метод симуляций Монте-Карло, метод исторических симуляций);

- методы построения деревьев (деревья событий, деревья отказов, события-последствия);

- логико-вероятностные методы.

3. Эвристические методы количественного анализа.

4. Нетрадиционные методы:

- системы искусственного интеллекта (нейронные сети);

- моделирование на основе аппарата нечеткой логики (fuzzy logic).

Ещё на оценке рисков традиционно используются математические методы поддержки принятия решений: табличный метод, метод анализа иерархий, метод экспертных оценок. Рассмотрим вкратце эти методы и определим их основные недостатки.

Табличный метод – метод, опирающийся на таблицу, которая является схемой связей между угрозами, уязвимостями и ресурсами. Количественные и качественные показатели оцениваются при помощи балльных шкал.

Качественные оценки используются в случаях, когда количественные оценки по ряду причин затруднены [10].

Относящиеся к каждому типу негативных воздействий уровни рисков, соответствующих показателям ценности ресурсов, а также показателям угроз и уязвимостей, оцениваются при помощи таблицы. Количественный показатель риска определяется в фиксированной шкале. Для каждого ресурса рассматриваются относящиеся к нему уязвимые места и соответствующие им угрозы. Каждая строка в таблице определяется показателем ресурса, а каждый столбец – степенью опасности угрозы и уязвимости.

Как правило, значения риска находятся в определённой линейной зависимости от показателей ценности ресурса, угроз и уязвимостей. Шкалы качественных показателей при этом легко конвертируются в шкалы с численными значениями.

Описанный метод позволяет провести классификацию рассматриваемых рисков. Кроме того, метод даёт возможность наглядно

отразить в таблице связь между угрозами, негативными воздействиями и возможностями реализации. Для этого необходимо умножить показатель негативного воздействия каждой угрозы на реальность её реализации. Оба эти показателя предварительно оцениваются по фиксированной шкале. По итогам вычисления проводится ранжирование угроз.

Метод анализа иерархий – метод, применение которого сводит исследование практически любых сложных систем к последовательности попарных сравнений компонент данных систем [13]. Иерархия в данном случае — система наслаиваемых уровней, каждый из которых состоит из многих элементов, или факторов. Иначе говоря, иерархия — структура, копирующая естественный ход человеческого мышления, при котором разум объединяет множество элементов, отражающих сложную ситуацию, в группы в соответствии с распределением некоторых свойств между элементами.

Центральным вопросом на языке иерархии является следующий: насколько сильно влияют отдельные факторы самого низкого уровня иерархии на вершину – общую цель? Неравномерность влияния по всем факторам приводит к необходимости определения интенсивности влияния, или приоритетов факторов.

Модель должна включать в себя и позволять измерять все важные количественные и качественные факторы. Однако метод работает лишь в том случае, когда практически все эти факторы измерены объективно и в полном объёме, значения показателей непротиворечивы, результаты задач принятия решений однозначны и соответствуют мнению эксперта. Иначе можно ожидать появления систематических и случайных ошибок в оценках [13].

Метод экспертных оценок – метод, в центре которого лежит декомпозиция сложной трудно формализуемой задачи на последовательность более простых подзадач, соответствующих определённому числу элементарных экспертиз. Оценка параметров входит в число наиболее

распространённых элементарных экспертиз. Как правило, под оценкой нечисловой информации понимается приписывание нечисловым характеристикам количественных или качественных значений по выбранной шкале измерений.

В общем случае оценка заключается в назначении вероятностей совершения событий, реализации угрозы, дат событий или весов. Определение весовых коэффициентов рисков используется для их упорядочения и определения первоочередных действий по защите. Затем для определения степени безопасности системы на основании уже определённых параметров используется линейный метод взвешивания и подсчёта [30].

У описанных методов есть ряд недостатков, в целом, не являющихся критическими. Их устранение могло бы повысить эффективность оценивания. Перечислим недостатки подробнее.

Во-первых, методы, особенно метод анализа иерархий, требуют предоставления исчерпывающей исходной информации об объекте оценки. Однако для этого необходимо проанализировать большое количество разнородных параметров состояния. Исчерпывающее количественное описание состояния исследуемой системы в этом случае получить невозможно, поскольку за время, необходимое для его получения, обстановка внутри и вне системы может значительно измениться. Кроме того, даже в случае получения такого описания оно будет представлять собой огромный объём информации, требующий для своей обработки большого количества времени и вычислительных ресурсов.

Далее, оценки даются относительно дискретной шкалы и являются, как правило, численными. Это утверждение в какой-то степени относится и к качественным оценкам. Такая схема представления данных не учитывает особенностей представления сложных знаний в человеческом мозге. В результате математическая модель объекта оценки, служащая основой для принятия решений, обедняется, упрощается и, возможно, даже искажается.

Например, объект оценки может обладать частью характерных признаков определённой категории, а другой частью в то же время не обладать. Иными словами, принадлежность объекта к определённому классу может быть размыта. Соответственно, в таком случае принципиально меняется логика взаимосвязи входных и выходных данных.

Оценка всегда зависит от субъективных суждений эксперта, его знаний и опыта. В целом, влияние субъективности при обработке субъективных данных неизбежно и даже полезно. Однако возможны случаи отрицательного влияния субъективности, и в таких случаях должны быть надёжные механизмы для коррекции субъективности.

Наконец, для проведения аудита при помощи указанных методов и реализующих их средств эксперт должен обладать достаточно большим опытом аудита и навыками работы с системой. Средства, реализующие описанные методы, являются средствами поддержки принятия решений. К самостоятельным действиям, направленным на накопление собственного опыта, коррекцию субъективности при оценивании и поиск оптимального решения поставленной задачи они не способны.

Таким образом, для повышения качества оценки рисков необходимо исследовать и реализовать, во-первых, механизмы представления нечётких и неполных данных (нечёткие механизмы), во-вторых, механизмы устранения субъективности нечётких и неполных данных и поиска оптимального решения задачи (эволюционные механизмы). Для указанных целей в настоящее время исследуются вопросы применения нечетких механизмов несколькими исследователями независимо друг от друга.

Нечеткая логика не требует моделирования точных и однозначных формулировок закономерностей, она предполагает совершенно иной уровень мышления, благодаря которому творческий процесс моделирования происходит на наивысшем уровне абстракции, при котором постулируется лишь минимальный набор закономерностей.

2.2 Особенности и методика оценки рисков безопасности оптических сетей телекоммуникации на основе нечеткой логики

2.2.1 Основные понятия нечёткой логики

Основным этапом анализа рисков является оценка рисков. Известны различные методики оценки рисков безопасности, их можно классифицировать по типу используемой в них процедуры принятия решения на:

a) одноэтапные, в которых оценка риска выполняется с помощью одноразовой решающей процедуры;

b) многоэтапные, с предварительным оцениванием ключевых параметров.

Одноэтапные методики, как правило, используются на начальной стадии развития информационной инфраструктуры, когда ключевые факторы, определяющие информационную безопасность, еще не выявлены.

Многоэтапные методики, с предварительным оцениванием ключевых параметров, являются более конструктивными [25].

Однако используемый механизм оценки риска в этих методиках представлен в виде таблицы, отражающей зависимость риска от двух, либо трёх входных переменных. При этом значение каждой переменной, включая риск, оценивается по трёхуровневой, либо пятиуровневой шкале. Такой «жёсткий» механизм получения оценок риска существенно ограничивает возможности подобных методик в целом. Механизм же получения оценок рисков безопасности ОСТ на основе нечёткой логики позволяет заменить приближённые табличные методы грубой оценки рисков современным математическим методом. При использовании нечёткой логики для оценки рисков необходимо рассмотреть основные понятия и определения.

Нечетким множеством (fuzzy set) *A* на универсальном множестве *U* называется совокупность пар *(Ma(u), u)*, где *Ma(u)* - степень принадлежности элемента $u \in U$ к нечеткому множеству *A*. Степень принадлежности - это число из диапазона [0, 1]. Чем выше степень принадлежности, тем в большей мере элемент универсального множества соответствует свойствам нечеткого множества.

Функцией принадлежности (membership function) называется функция, которая позволяет вычислить степень принадлежности произвольного элемента универсального множества к нечеткому множеству.

Если универсальное множество состоит из конечного количества элементов $U = \{u_1, u_2, ..., u_k\}$, тогда нечеткое множество *A* записывается в виде:

$$A = \sum Ma/Ui \ . \qquad (2.1)$$

В случае непрерывного множества *U* используют такое обозначение $A = Ma(u)/u$.

Лингвистической переменной (linguistic variable) называется переменная, значениями которой могут быть слова или словосочетания некоторого естественного или искусственного языка.

Лингвистическая переменная задается пятеркой <*x, T, U, G, M*>, где *x* - имя переменной; *T* - терм-множество, каждый элемент которого (терм) представляется как нечеткое множество на универсальном множестве *U*; *G* - синтаксические правила, часто в виде грамматики, порождающие названия термов; *M* - семантические правила, задающие функции принадлежности нечетких термов, порожденных синтаксическими правилами *G*.

Терм-множеством (term set) называется множество всех возможных значений лингвистической переменной.

Термом (term) называется любой элемент терм-множества. В теории нечетких множеств терм формализуется нечетким множеством с помощью

функции принадлежности. Дефазификацией (defuzzification) называется процедура преобразования нечеткого множества в четкое число.

В теории нечетких множеств процедура дефазификации аналогична нахождению характеристик положения (математического ожидания, моды, медианы) случайных величин в теории вероятности. Простейшим способом выполнения процедуры дефаззификации является выбор четкого числа, соответствующего максимуму функции принадлежности.

Дефазификация нечеткого множества $\tilde{A} = \int_{[\underline{u},\bar{u}]} \mu_A(u)/u$ по методу центра тяжести осуществляется по формуле:

$$a = \frac{\int_{\underline{u}}^{\bar{u}} u \cdot \mu_A(u)\, du}{\int_{\underline{u}}^{\bar{u}} \mu_A(u)\, du} \quad . \tag{2.2}$$

Дефазификация нечеткого множества $\tilde{A} = \int_{[\underline{u},\bar{u}]} \mu_A(u)/u$ по методу медианы состоит в нахождении такого числа a, что

$$\int_{\underline{u}}^{a} \mu_A(u)\ du = \int_{a}^{\bar{u}} \mu_A(u)\, du \ . \tag{2.3}$$

Дефазификация нечеткого множества $\tilde{A} = \int_{[\underline{u},\bar{u}]} \mu_A(u)/u$ по методу центра максимумов осуществляется по формуле:

$$a = \frac{\int_{G} u\, du}{\int_{G} du} \ , \tag{2.4}$$

где: G - множество всех элементов из интервала $[\underline{u}, \bar{u}]$, имеющих максимальную степень принадлежности нечеткому множеству $\tilde{A}$.

Нечеткой базой знаний (fuzzy knowledge base) о влиянии факторов $X = \{x_1, x_2, \ldots, x_n\}$ на значение параметра y называется совокупность логических высказываний типа:

$$\text{ЕСЛИ}\left(x_1 = a_1^{j1}\right)\text{И}\left(x_2 = a_2^{j1}\right)\text{И...И}\left(x_n = a_n^{j1}\right)$$
$$\text{ИЛИ}\ \left(x_1 = a_1^{j2}\right)\text{И}\left(x_2 = a_2^{j2}\right)\text{И...И}\left(x_n = a_n^{j2}\right),$$
$$\dots$$
$$\text{ИЛИ}\ \left(x_1 = a_1^{jk_j}\right)\text{И}\left(x_2 = a_2^{jk_j}\right)\text{И...И}\left(x_n = a_n^{jk_j}\right),$$
$$\text{ТО } y=d_j, \text{ для всех } j=\overline{1,m},$$

где: a_i^{jp} - нечеткий терм, которым оценивается переменная x_i в строчке с номером jp ($p=\overline{1,k_j}$);

k_j - количество строчек-конъюнкций, в которых выход y оценивается нечетким термом d_j, $j=\overline{1,m}$;

m - количество термов, используемых для лингвистической оценки выходного параметра y.

С помощью операций $\cup$ (ИЛИ) и $\cap$ (И) нечеткую базу знаний перепишем в более компактный вид:

$$\bigcup_{p=1}^{k_j}\left[\bigcap_{i=1}^{n}\left(x_i = a_i^{jp}\right)\right] \to y = d_j, \quad j=\overline{1,m}\ . \tag{2.5}$$

Нечетким логическим выводом (fuzzy logic inference) называется аппроксимация зависимости $y=f(x_1,x_2,..,x_n)$ с помощью нечеткой базы знаний и операций над нечеткими множествами.

Высотой нечеткого множества $\tilde{A}$ называется верхняя граница его функции принадлежности [25]:

$$hgt\,(\tilde{A}) = \sup_{u\in U}\mu_A(U)\ . \tag{2.6}$$

Нечеткое множество $\tilde{A}$ называется нормальным, если его высота равна единице. Нечеткие множества не являющиеся нормальными называются субнормальными. Нормализация - преобразование субнормального нечеткого множества $\tilde{A}$ в нормальное $\tilde{A}$ определяется по формуле:

$$\tilde{A} = norm\left(\tilde{A}'\right) \Leftrightarrow \mu_A(u) = \frac{\mu_{A'}(u)}{hgt\,(\tilde{A}')},\ \forall u \in U\ . \tag{2.7}$$

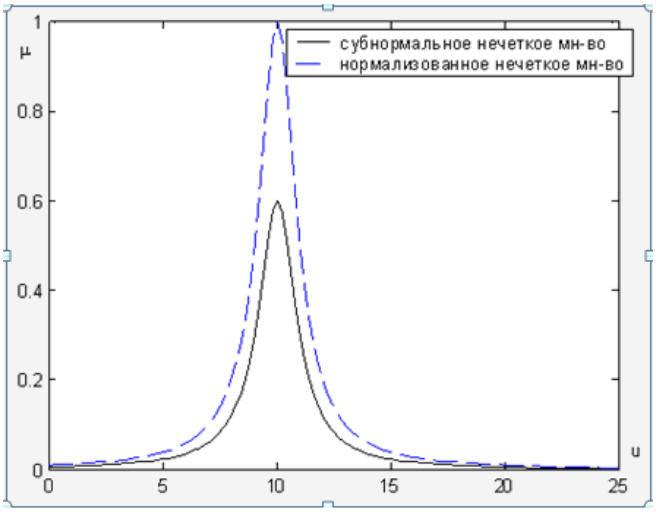

Рис.2.2 - Нормализация нечеткого множества

Носителем нечеткого множества $\tilde{A}$ называется четкое подмножество универсального множества U, элементы которого имеют ненулевые степени принадлежности:

$$\sup p(\tilde{A}) = \{u : \mu_A(u) > 0\} , \qquad (2.8)$$

α-сечением (или множеством α-уровня) нечеткого множества $\tilde{A}$ называется четкое подмножество универсального множества U, элементы которого имеют степени принадлежности большие или равные α:

$$A_\alpha = \{u : \mu_A(u) \geq \alpha\}, \quad \alpha \in [0,1] . \qquad (2.9)$$

Значение α называют α-уровнем (рис.2.3). Носитель (ядро) можно рассматривать как сечение нечеткого множества на нулевом (единичном) α-уровне, рис.2.3.

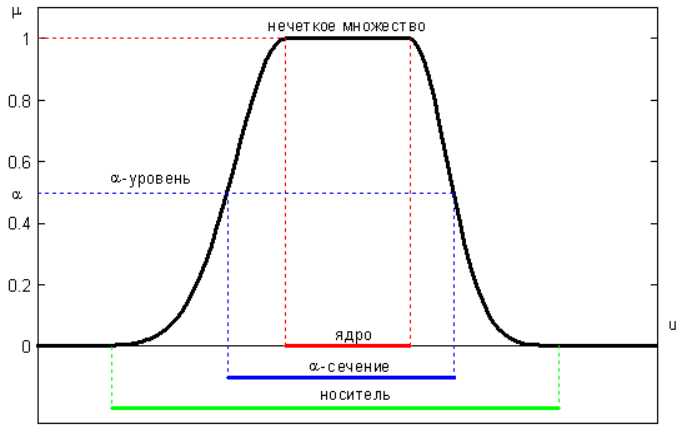

Рис. 2.3 - Ядро, носитель и α-сечение нечеткого множества

Дополнением нечеткого множества $\tilde{A}$ заданного на U называется нечеткое множество $\tilde{A}$ с функцией принадлежности $\mu_{\bar{A}}(u) = 1 - \mu_A(u)$ для всех $u \in U$, рис.2.4.

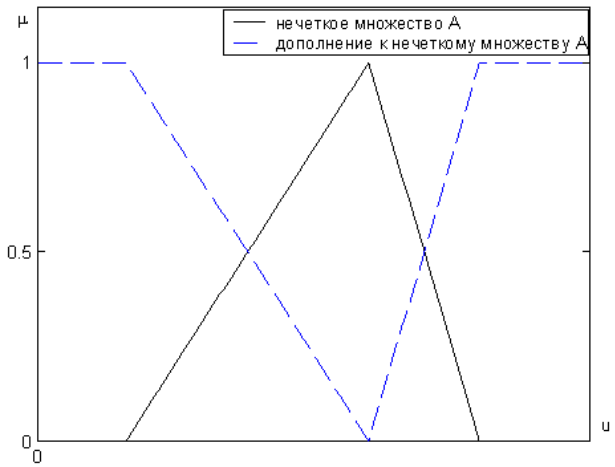

Рис.2.4 - Дополнение нечеткого множества

Пересечением нечетких множеств $\tilde{A}$ и $\tilde{B}$ заданных на U называется нечеткое множество $\tilde{C} = \tilde{A} \cap \tilde{B}$ с функцией принадлежности $\mu_C(u) = \min(\mu_A(u), \mu_B(u))$ для всех $u \in U$. Операция нахождения минимума также обозначается знаком $\cap$, т.е. $\mu_C(u) = \mu_A(u) \cap \mu_B(u)$ (рис.2.5).

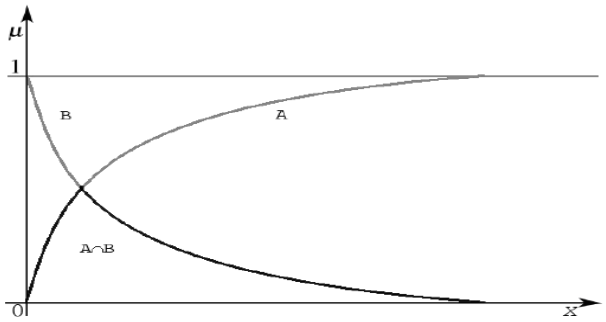

Рис.2.5 - Операция нахождения минимума

Объединением нечетких множеств $\tilde{A}$ и $\tilde{B}$ заданных на U называется нечеткое множество $D = \tilde{A} \cup \tilde{B}$ с функцией принадлежности $\mu_D(u) = \max(\mu_A(u), \mu_B(u))$ для всех $u \in U$. Операция нахождения максимума также обозначается знаком $\cup$, т.е. $\mu_D(u) = \mu_A(u) \cup \mu_B(u)$ (рис.2.6).

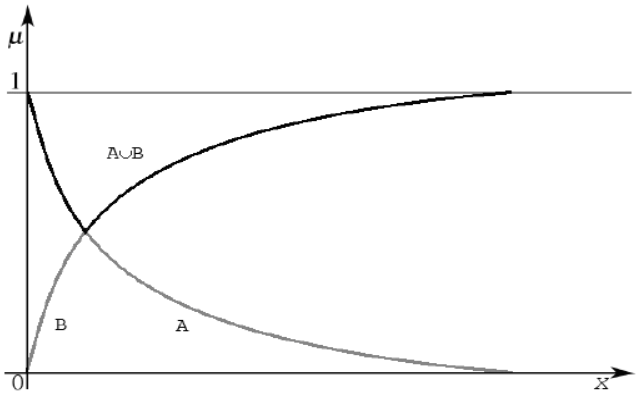

Рис.2.6 - Операция нахождения максимума

2.2.2 Механизм нечеткого логического вывода

В основе методики оценки рисков безопасности ОСТ лежит механизм нечёткого логического вывода [25].

Нечётким логическим выводом называется получение заключения в виде нечёткого множества, соответствующего текущим значениям входов, с использованием нечёткой базы знаний и нечётких операций.

В качестве базового нечёткого логического вывода можно использовать вывод Мамдани.

Нечеткий логический вывод по алгоритму Мамдани выполняется по нечеткой базе знаний(2.10):

$$\bigcup_{p=1}^{k_j}\left(\bigcap_{i=1}^{n} x_i = a_{i,jp}\ c\ весом\ w_{jp}\right) \to y = d_j, \quad j = \overline{1,m}\ , \tag{2.10}$$

в которой значения входных и выходной переменной заданы нечеткими множествами. Введем следующие обозначения:

$\mu_{jp}(X_i)$ - функция принадлежности входа X_i нечеткому терму $a_{i,jp}$, т.е.

$$a_{i,jp} = \int_{\underline{x_i}}^{\overline{x_i}} \mu_{jp}(x_i)/x_i,\ x_i \in \left\lfloor \underline{x_i}, \overline{x_i} \right\rfloor. \tag{2.11}$$

$\mu d_j(y)$ - функция принадлежности выхода y нечеткому терму d_j, т.е.

$$d_j = \int_{\underline{y}}^{\overline{y}} \mu d_j(y)/y,\ y \in \left\lfloor \underline{y}, \overline{y} \right\rfloor. \tag{2.12}$$

Степени принадлежности входного вектора $x^* = (x_1^*, x_2^*, ...x_n^*)$ нечетким термам d_j из базы знаний рассчитывается по формуле (2.13):

$$\mu_{dj}(X^*) = \underset{p=1,k_j}{\vee} w_{jp} . \underset{i=1,n}{\wedge}\left[\mu_{jp}\left(X_i^*\right)\right], j = \overline{1,m}\quad , \tag{2.13}$$

где $\vee(\wedge)$ - операция из множества реализаций логической операций «ИЛИ(И)».

Наиболее часто используются следующие реализации: для операции «ИЛИ» - нахождение максимума и для операции «И» - нахождение минимума.

В результате получаем такое нечеткое множество $\overline{Y}$, соответствующее входному вектору X`:

$$\overline{Y} = \frac{\mu d_1(X^*)}{d_1} + \frac{\mu d_2(X^*)}{d_2} + ... + \frac{\mu d_m(X^*)}{d_m}. \tag{2.14}$$

Для перехода от нечеткого множества, заданного на универсальном множестве нечетких термов $\{d_1, d_2, ..., d_m\}$ нечеткому множеству на интервале $\left\lfloor \underline{y}, \overline{y} \right\rfloor$ необходимо: 1) «срезать» функции принадлежности $\mu d_j(y)$

на уровне $\mu d_j(X^*)$; 2) объединить (агрегировать) полученные нечеткие множества.

Математически это записывается следующим образом:

$$\overline{Y} = \underset{j=1,m}{agg}\left(\int_{\underline{Y}}^{\overline{Y}} \min\left(\mu d_j\left(X*\right), \mu d_j\left(Y\right)\right)/Y \right), \qquad (2.15)$$

где $\underset{j=1,m}{agg}$ – агрегирование нечетких множеств, которое наиболее часто реализуется операцией нахождения максимума.

Четкое значение выхода y , соответствующее входному вектору X` определяется в результате деффаззификации нечеткого множества $\overline{Y}$. Наиболее часто применяется дефаззификация по методу центра тяжести:

Четкое значение выхода y, соответствующее входному вектору

$$Y = \frac{\int_{\underline{Y}}^{\overline{Y}} \cdot \mu_{\overline{Y}}(Y)\, dY}{\int_{\underline{Y}}^{\overline{Y}} \cdot \mu_{\overline{Y}}(Y)\, dY}. \qquad (2.16)$$

где $\int_{\underline{Y}}^{\overline{Y}}$ – символ интеграла.

2.2.3 Общие положения алгоритма оценки рисков безопасности методами нечеткой логики и теории нечетких множеств

Общие положения алгоритма оценки рисков:

1) определяются наборы лингвистических термов, характеризующих значения входных параметров (уровень угрозы УУ1, уровень уязвимости УУ2, уровень ущерба УУ3) и выходного параметра (уровень риска УР);

2) задается набор входных параметров YY1i (i = 1…M), определяющих уровни угроз. Входные параметры имеют количественные значения [0…1] или качественные значения, выраженные в термах лингвистических переменных;

3) задается набор входных параметров YY2i (i = 1…N), определяющих уровни уязвимостей. Входные параметры имеют качественные значения, выраженные в термах лингвистических переменных;

4) задается набор входных параметров YY3i (i = 1…K), определяющих уровни ущерба. Входные параметры имеют количественные значения [0…1] или качественные значения, выраженные в термах лингвистических переменных;

5) находится выходной параметр УР, определяющий уровень риска;

6) формируется набор продукционных правил вида «ЕСЛИ, …, ТО», отражающих взаимосвязи входных параметров с выходным;

7) производится фазификация входных параметров – нахождение значений функций принадлежности, соответствующих полученным значениям оценок входных переменных;

8) производится агрегирование – определение степени истинности условий по каждому из продукционных правил;

9) производится аккумулирование заключений – нахождение функции принадлежности выходного параметра с учетом агрегирования;

10) производится дефазификация выходного параметра.

Таким образом, представленный подход к оценке рисков информационной безопасности позволяет:

− производить оценку уровня риска;

− производить оценку уровня риска как в общем, так и по различным критериям (например, риск потери репутации, финансовый риск, риск на соответствие различным нормам и т.д.).

2.2.4 Параметрические алгоритмы оценки риска безопасности

Построение параметрических алгоритмов может быть основано на нескольких параметрах, которые оцениваются по *n*–уровневым шкалам.

Далее рассмотрим двухпараметрический алгоритм оценки риска с трехуровневыми шкалами входных параметров [6].

Механизм получения оценок риска на основе нечеткой логики с предварительным оцениванием двух входных параметров: оценки вероятности некоторого инцидента и ущерба от этого инцидента, предполагает, что:

a) для входных величин и риска заданы трехуровневые шкалы, на которых определены нечеткие термы, соответствующие «большому», «среднему» и «низкому» значениям переменных;

b) логика связи входных величин и риска соответствует «табличному» механизму оценки риска, представленному в рекомендациях NIST 800-30 (таблица 2.1);

c) значимость всех логических правил вывода одинакова (все весовые коэффициенты продукционных правил равны единице);

d) тем или иным способом получены оценки входных переменных.

Таблица 2.1.

Оценка риска по трехуровневым шкалам

Вероятность	Ущерб		
	«Большой»	«Средний»	«Низкий»
«Большая»	Б	С	Н
«Средняя»	С	С	Н
«Низкая»	Н	Н	Н

Продукционные правила, соответствующие табл.2.1., можно представить следующим образом:

a) ЕСЛИ Вероятность «Большая» И Ущерб «Большой», ТО Риск = «Большой» (Б);

b) ЕСЛИ Вероятность «Большая» И Ущерб «Средний», ТО Риск = «Средний» (С);

c) ЕСЛИ Вероятность «Большая» И Ущерб «Низкий», ТО Риск = «Низкий» (H);

d) ЕСЛИ Вероятность «Средняя» И Ущерб «Большой», ТО Риск = «Средний» (C);

e) ЕСЛИ Вероятность «Средняя» И Ущерб «Средний», ТО Риск = «Средний» (C);

f) ЕСЛИ Вероятность «Средняя» И Ущерб «Низкий», ТО Риск = «Низкий» (H);

g) ЕСЛИ Вероятность «Низкая» И Ущерб «Большой», ТО Риск = «Низкий» (H);

h) ЕСЛИ Вероятность «Низкая» И Ущерб «Средний», ТО Риск = «Низкий» (H);

i) ЕСЛИ Вероятность «Низкая» И Ущерб «Низкий», ТО Риск = «Низкий» (H).

А теперь рассмотрим двухпараметрический алгоритм с пятиуровневыми шкалами. Предположим, что алгоритм остается двухпараметрическим, но для измерения входных параметров используются пятиуровневые шкалы. Шкала вероятности содержит следующие уровни:

a) A – событие практически никогда не происходит;

b) B – событие случается редко;

c) C – вероятность события за рассматриваемый промежуток времени приблизительно равна 0,5 (событие вполне возможное при соответствующем стечении обстоятельств);

d) D – скорее всего событие произойдет (при организации атаки);

e) E – событие, вероятнее всего, произойдет (при организации атаки).

Шкала ущерба содержит также пять уровней:

a) N (Negligible) – ущерб, которым можно пренебречь;

b) Mi (Minor) – незначительный ущерб, последствия которого легко устранить;

c) Mo (Moderate) – умеренный ущерб;

d) S (Serious) – серьезный ущерб, ликвидация которого возможна, но связана со значительными затратами;

e) C (Critical) – критический ущерб, который ставит под сомнение возможность устранения его последствий.

Шкала для оценки риска может быть задана в виде последовательности чисел от 0 до 8, включительно. Зависимость риска от вероятности ущерба приведена в табл.2.2.

Таблица 2.2

Шкала оценки риска по пятиуровневым шкалам

Вероятность	Ущерб				
	N	Mi	Mo	S	C
A	0	1	2	3	4
B	1	2	3	4	5
C	2	3	4	5	6
D	3	4	5	6	7
E	4	5	6	7	8

Рассмотрим трехпараметрический алгоритм оценки риска. С помощью продукционных правил нечеткой логики необходимо воспроизвести механизм вывода, содержащий три входные переменные, которыми являются: возможный ущерб от инцидента, эффективность защиты и потенциал угрозы (рис.2.7) .

Рис.2.7 - Оценка риска по трем входным переменным

В данном случае вероятность возникновения инцидента непосредственно не является входной величиной, поэтому она не представлена на рис.2.7, однако, она будет использована для логического обоснования правил продукционного вывода.

Ниже рассмотрим методы оценки эффективности защиты.

Для оценки эффективности защиты целесообразно использовать требования международного стандарта ISO/IEC 27002:2005 «Практические правила управления информационной безопасностью». В стандарте определены следующие десять направлений, по каждому из которых сформулированы требования к системе защиты информации:

a) политика безопасности;

b) организация защиты;

c) управление ресурсами;

d) безопасность персонала;

e) физическая безопасность;

f) администрирование компьютерных систем и вычислительных сетей;

g) управление доступом;

h) разработка и сопровождение информационных систем;

i) планирование бесперебойной работы;

j) контроль выполнения требований политики безопасности.

Положения, содержащиеся в стандарте ISO/IEC 27002:2005, позволяют по каждому из указанных направлений получить оценку соответствия системы защиты информации предъявляемым требованиям. В данном случае мы сознательно опускаем вопрос оценивания технической эффективности системы защиты информации, считая, что выполнение базовых технических требований обеспечивается политикой безопасности предприятия.

Общая оценка складывается из «взвешенных» оценок по отдельным направлениям. «Вес» для каждого направления определяется экспертом-аналитиком на этапе обследования предприятия. При этом учитывается

различие в требованиях к защите информации в государственных, финансово-кредитных, коммерческих, телекоммуникационных и других организациях. Учитывается также стадия жизненного цикла, на которой находится информационная система: проектирование, ввод в действие или эксплуатация.

Рассмотрим оценку потенциала угрозы. Угрозы различаются по степени опасности. Очевидно, что нарушители (источники угроз) обладают разными возможностями для реализации своих замыслов и имеют разную степень заинтересованности в достижении цели. Методы нечеткой логики позволяют увеличивать число учитываемых параметров и таким образом включать в процесс обработки многопараметрические модели нарушителей. Однако следует иметь ввиду, что при этом увеличивается число и сложность продукционных правил.

Для того чтобы сделать механизм вывода, по возможности, более простым и одновременно эффективным, целесообразно производить предварительную группировку входных данных. При этом полезными оказываются локальные модели нарушителей, отражающие специфику и конкретные условия проявления угроз.

В данном случае целесообразно ввести локальную модель нарушителя, учитывающую его объективные возможности и степень заинтересованности, а в качестве обобщенной характеристики угрозы, исходящей от этого нарушителя использовать «потенциал угрозы» (табл. 2.3).

Локальная модель нарушителя, вытекающая из таблицы 2.3, является достаточно простой и прозрачной: потенциально опасным признается только тот нарушитель, который имеет и высокие объективные возможности и высокую степень заинтересованности в преодолении защиты.

Таблица 2.3

Определение «потенциала угрозы»

Степень заинтересованности нарушителя	Объективные возможности нарушителя				
	1	2	3	4	5
1	1	1	1	1	1
2	1	2	2	2	2
3	1	2	3	3	3
4	1	2	3	4	4
5	1	2	3	4	5

Существует модель нарушителя более общего вида, которая позволяет включить в процесс обработки большее количество информации о характере и особенностях проявления угроз. В качестве такой модели можно рассмотреть четырехкомпонентную модель, включающую (рис.2.9):

a) организацию нападения на информационный ресурс (зависит от заинтересованности нарушителя, связей и принадлежности нарушителя к криминальной группе);

b) технологию доступа к информационному ресурсу (определяется квалификацией нарушителя, возможностями технологического планирования атаки и используемыми методами);

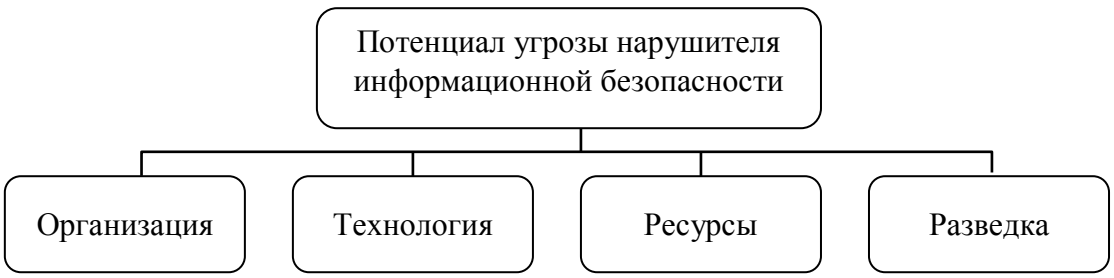

Рис.2.9 - Общая модель нарушителя информационной безопасности

c) технические и интеллектуальные ресурсы (определяются технической оснащенностью и сторонней поддержкой);

d) разведку параметров и уязвимостей (определяется способами получения исходных сведений).

Оценку потенциала нарушителя на основе этой модели можно выполнить по составляющим компонентам с последующей «весовой обработкой». При этом все оценочные процедуры будут относиться к предварительной обработке. Для механизма нечеткого вывода входной переменной по-прежнему будет оценка «потенциала угрозы».

Таблица 2.4

Шкала ущерба

Уровень ущерба	Описание воздействия
5. катастрофический	Приводит к разрушительным последствиям и невозможности ведения бизнеса.
4. критический	Наносится значительный урон репутации компании и ее интересам, что может представлять угрозу для компании и продолжения ее бизнеса.
3. большой	Приводит к большим потерям материальных активов или ресурсов или наносится большой урон репутации компании и ее интересам.
2. заметный	Приводит к заметным потерям материальных активов, существенному влиянию на репутацию компании или существенному ущемлению ее интересов.
1. малый	Приводит к незначительным потерям материальных средств и ресурсов, которые быстро восполняются, или незначительному влиянию на репутацию.

Шкалы оценок ущерба и риска. Предположим, что для оценки ущерба используется качественная пятиуровневая шкала, представленная в табл. 2.4.

В общем случае оценки ущерба могут носить как качественный, так и количественный характер. Однако качественные оценки являются более универсальными и могут быть использованы даже тогда, когда для оценки

ущерба нет количественных показателей (нанесение ущерба авторитету компании, раскрытие перспективных планов развития и т.д.).

Аналогичная шкала задается для измерения риска (табл.2.5).

Таблица 2.5

Шкала риска

Уровень риска	Описание риска
Недопустимый (Нд)	Уровень риска очень большой и является недопустимым для организации, что требует прекращение эксплуатации системы и принятии радикальных мер по уменьшению риска.
Критический (К)	Уровень риска такой, что бизнес процессы находятся в неустойчивом состоянии. Необходимо незамедлительно принять меры по уменьшению риска.
Высокий (В)	Уровень риска не позволяет стабильно работать. Имеется настоятельная необходимость в корректирующих действиях, изменяющих режим работы в сторону уменьшения риска. Система может продолжать работу, но корректирующий план действий необходимо применить как можно быстрее.
Средний (С)	Уровень риска позволяет работать, но имеются предпосылки к нарушению нормальной работы. Необходимо разработать и применить план корректирующих действий в течении приемлемого периода времени.
Низкий (Н)	Если сведения расцениваются как низкий риск, необходимо определить существует ли необходимость в корректирующих действиях или есть возможность принять этот риск.

Введенные уровни ущерба и риска используются при формировании правил вывода. Для формирования правил вывода необходимо определить в качестве промежуточной величины вероятность успешной атаки. Допустим, что для представления вероятности несанкционированного доступа (НСД), используется рассмотренная выше пятиуровневая шкала, содержащая уровни:

a) A – событие практически никогда не происходит;

b) B – событие случается редко;

c) C – событие вполне возможно;

d) D – событие, скорее всего, произойдет;

e) E – событие обязательно произойдет.

При обосновании правил вывода будем исходить из следующих предположений. Предположим, что, если эффективность защиты выше потенциала нарушителя, то вероятность успешной атаки соответствует уровню *A*. Если эффективность защиты равна потенциалу нарушителя, то вероятность успешной атаки соответствует уровню *B*. Наконец, если эффективность защиты меньше потенциала нарушителя, то вероятность НСД будет тем выше, чем больше превышение потенциала нарушителя над эффективностью защиты (уровни *C*, *B* и *F*).

Представленная логическая модель позволяет оценить вероятность успешной атаки в зависимости от потенциала угрозы и эффективности защиты (табл.2.6).

Определенная таким образом вероятность успешной атаки определяет функцию риска как свертку шкал вероятности и ущерба (табл.2.7).

Таблица 2.6

Вероятность успешной атаки на информационные ресурсы

Эффективность защиты	Потенциал угроз				
	1	2	3	4	5
1	B	C	D	E	E
2	A	B	C	D	E
3	A	A	B	C	D
4	A	A	A	B	C
5	A	A	A	A	B

Таблица 2.7

Шкала оценок риска

Ущерб	Вероятность реализации угроз				
	A	B	C	D	E
1	H	H	H	C	C
2	H	H	C	B	B
3	H	C	B	B	K
4	C	B	B	K	K
5	C	B	K	K	Нд

2.3 Разработка методики использования нечеткой логики для оценки рисков информационной безопасности оптических сетей телекоммуникации

Механизм оценивания рисков на основе нечёткой логики, по существу, является экспертной системой, в которой базу знаний составляют правила, отражающие логику взаимосвязи входных величин и риска. В простейшем случае это «табличная» логика, в общем случае - более сложная логика, отражающая реальные взаимосвязи, которые могут быть формализованы с помощью продукционных правил вида «Если..., то».

Кроме того, механизм нечёткой логики требует формирования оценок ключевых параметров и представления их в виде нечётких переменных. При этом необходимо учитывать множество источников информации и качество самой информации.

Механизм нечёткого вывода можно представить в виде последовательности этапов, в каждом из которых используются результаты предыдущего этапа (рис.2.10):

а) Задание функций принадлежности входных переменных - предполагает определения вида функций принадлежности для каждой из входных лингвистических переменных на оси возможных значений этой переменной. Кроме этого, на данном этапе необходимо задать параметры выбранных функций принадлежности.

Среди многих методов определения функций принадлежности наибольшее распространение получил модифицированный метод парных сравнений Саати. Для реализации этого метода необходимо:

1) Задать лингвистическую переменную *X*. Для оценки риска необходимо задать следующие лингвистические переменные:

а) вероятность последствия воздействия нарушителя (инцидента);

b) ущерб от последствия воздействия нарушителя(инцидента);

2) Определить универсальное множество *U*, на котором задаётся переменная *X*:

а) для вероятности последствия воздействия нарушителя(инцидента) U={0;0,1;0,2;...;1};

b) для ущерба от инцидента U={0;1;2;...;8};

c) для риска U={0;1;2;...;8}

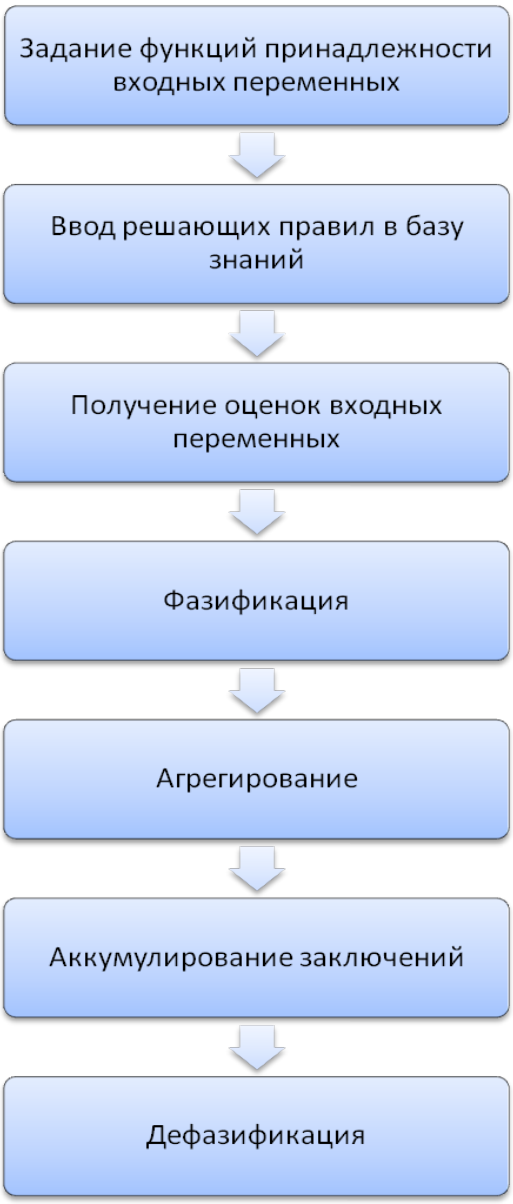

Рис.2.10 - Основные этапы механизма нечеткого вывода

3) Задать совокупность нечётких термов {S1,S2,...,Sm}, которые используются для оценки переменной *X*:

а) для вероятности инцидента зададим следующие термы:

- низкая - последствие практически никогда не происходит;

- средняя - последствие вполне возможно при определённом стечении обстоятельств;

- высокая - последствие скорее всего произойдёт при реализации атаки.

b) для ущерба от последствия воздействия нарушителя (инцидента):

- малый - приводит к незначительным потерям материальных средств и ресурсов, которые быстро восполняются, или незначительному влиянию на репутацию;

- заметный - приводит к заметным потерям материальных активов, существенному влиянию на репутацию компании, эксплуатирующей данную систему передачи данных, или существенному ущемлению её интересов;

- большой - приводит к заметным потерям материальных активов, существенному влиянию на репутацию компании, эксплуатирующей систему передачи данных, и её интересам.

c) для риска:

- низкий - если сведения расцениваются как низкий риск, необходимо определить, существует ли необходимость в корректирующих действиях или есть возможность принять этот риск;

- средний - уровень риска позволяет работать, но имеются предпосылки к нарушению нормальной работы системы передачи данных, необходимо разработать план корректирующих действий в течение приемлемого периода времени;

- высокий - уровень риска не позволяет стабильно работать. Имеется настоятельная необходимость в корректирующих действиях, изменяющих режим работы системы передачи данных в сторону уменьшения риска. Система может продолжать работу, но корректирующий план действий необходимо применить как можно быстрее.

4) Для каждого терма S_j, j=1,m сформировать матрицу (2.17)

$$A = \begin{bmatrix} 1 & \frac{r_2}{r_1} & \frac{r_3}{r_1} & \dots & \frac{r_n}{r_1} \\ \frac{r_1}{r_2} & 1 & \frac{r_3}{r_2} & \dots & \frac{r_n}{r_2} \\ \dots & \dots & \dots & \dots & \dots \\ \frac{r_1}{r_n} & \frac{r_2}{r_n} & \frac{r_3}{r_n} & \dots & 1 \end{bmatrix}, \qquad (2.17)$$

где $\frac{r_i}{r_j} = a_{ij,}\, i, j = \overline{1,n}$ - относительная оценка рангов r_i и r_j.

Для экспертных оценок элементов этой матрицы можно использовать девятибалльную шкалу Саати:

1 - при отсутствии преимущества r_j над r_i;

3 - при слабом преимуществе r_j над r_i;

5 - при существенном преимуществе r_j над r_i;

7 - при явном преимуществе r_j над r_i;

9 - при абсолютном преимуществе r_j над r_i;

2,4,6,8 - промежуточные сравнительные оценки.

5) Используя формулу (2.18) вычислить элементы функций принадлежности для каждого терма

$$\left.\begin{array}{l} \mu_1 = \left(1 + \frac{r_2}{r_1} + \frac{r_3}{r_1} + \cdots + \frac{r_n}{r_1}\right)^{-1} \\ \mu_2 = \left(\frac{r_1}{r_2} + 1 + \frac{r_3}{r_2} + \cdots + \frac{r_n}{r_2}\right)^{-1} \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ \mu_n = \left(\frac{r_1}{r_n} + \frac{r_2}{r_n} + \frac{r_3}{r_n} + \cdots + 1\right)^{-1} \end{array}\right\}, \qquad (2.18)$$

где M_i, i=1,n - степень принадлежности элемента $u_i \in U$ нечёткому множеству S. Нормирование найденных функций осуществляется путём деления на наибольшие степени принадлежности.

б) Ввод решающих правил в базу знаний - заключается в программировании базы знаний, то есть в представлении её в форме продукционных правил вида «Если..., то», отражающих логические взаимосвязи входных лингвистических переменных с величиной риска. Эти правила формируются на основе общих закономерностей поведения

исследуемой системы и позволяют «вложить» в механизм вывода логическую модель прикладного уровня.

в) Получение оценок входных переменных - является той процедурой, которая обеспечивает механизм вывода текущей информации, отражающей фактическое состояние защищённости исследуемой системы на данный момент времени. Для этого могут быть использованы оценки экспертов фактического состояния защищённости исследуемой системы. Оценки могут быть получены на основе заранее разработанных диагностических тестов, охватывающих различные аспекты проявления оцениваемых величин.

г) Фазификация оценок входных переменных - представляет собой процедуру нахождения конкретных значений функций принадлежности, соответствующих полученным значениям оценок входных переменных.

д) Агрегирование - является процедурой определения степени истинности условий по каждому из правил системы нечёткого вывода. Здесь значения функций принадлежности подвергаются преобразованиям типа нечёткая конъюнкция или нечёткая дизъюнкция в соответствие с продукционными правилами.

е) Аккумулирование заключений - представляет собой процедуру нахождения функции принадлежности для каждой из выходных лингвистических переменных заданной совокупности правил нечёткого вывода. Результат аккумуляции для каждой лингвистической переменной определяется как объединение нечётких множеств.

ж) Дефазификация - является процедурой нахождения чётких значений выходных переменных, в наибольшей степени отвечающих входным данным и базе продукционных правил.

В качестве базового механизма нечёткого логического вывода используют вывод Мамдани. При этом на этапе а) функции принадлежности могут определяться по методу статистической обработки экспертной информации, методу парных сравнений Саати и модифицированному методу

Саати, а этап г) можно выполнить, используя метод центра тяжести, медианы или центр максимумов.

Отличительной особенностью ОСТ является то, что помимо объективных законов в их функционировании существенную роль имеют субъективные представления. При оценке рисков безопасности ОСТ значительное количество информации о системе может быть получено от различных групп людей: а) имеющих опыт управления данной системой и представляющих её цели, но не знающих досконально особенности её функционирования; б) знающих особенности функционирования системы, но не имеющих полного представления о её целях; в) знающих теорию и практику организации защиты, но не имеющих чётких представлений о целях, задачах и особенностях функционирования системы в целом и т.п. Поэтому получаемая от них информация, как правило, носит субъективный характер, и её представление на естественном языке не имеет аналогов в языке традиционной математики и содержит большое число неопределённостей типа: «много», «мало» если речь идёт о вложении денежных средств в совершенствование системы защиты или об изменении количества персонала, занятого вопросами защиты; «маленькая», «средняя», «большая» - если речь идёт о возможности инцидента от воздействия нарушителя; «средний», «не очень большой», «большой» - при оценке ущерба по данному инциденту. Поэтому и описание подобной информации на языке традиционной математики обедняет математическую модель исследуемой реальной системы и делает её слишком грубой. Таким образом, при оценке рисков безопасности таких систем возникает необходимость использования нечёткой логики.

2.4 Выводы

На основании вышеизложенного множеств можно сделать следующие выводы.

1. Оценка информационной безопасности ОСТ должна производиться с целью проверки соответствия достигнутого уровня информационной безопасности ОСТ, заданному уровню в технических заданиях на разработку этих сетей. Причем эти оценки должны обладать свойствами сравнимости и повторяемости, чтобы быть доказательными при анализе альтернативных вариантов оценке уровня информационной безопасности на различных этапах их жизненного цикла.

2. Обычно применение метода количественной оценки риска требует больших затрат как на описание, так и на анализ бизнес-процессов, но неоспоримым преимуществом данного метода является гарантированная полнота определения перечня рисков.

При количественной оценке риска используются различные методы. Наиболее распространенными являются:

a) статистический метод;
b) табличный метод;
c) метод экспертных оценок;
d) аналитический метод;
e) метод анализа иерархий;
f) метод нечетких множеств.

3. Для повышения качества оценки рисков необходимо исследовать и реализовать, во-первых, механизмы представления нечетких и неполных данных (нечеткие механизмы), во-вторых, механизмы устранения субъективности нечетких и неполных данных и поиска оптимального решения задачи (эволюционные механизмы). Для указанных целей в настоящее время исследуются вопросы применения теории нечетких множеств.

4. Механизм получения оценок рисков безопасности на основе нечеткой логики позволяет учитывать качество входной информации и надежность (степень доверия) источников информации. Этот механизм

позволяет заменить приближенные табличные методы грубой оценки рисков современным математическим аппаратом.

5. Разработка методики оценки информационной безопасности предполагает наличие или разработку: модели объекта оценки, модели системы защиты, модели потенциального нарушителя.

В условиях динамичного развития ОСТ и возникновения новых угроз информационной безопасности важным становится анализ и управление рисками информационной безопасности.

В основу разработки методик положена оценка процессов управления рисками, которая требует построения полной модели ОСТ, включающей:

a) описание сетевых ресурсов;

b) описание и оценку существующих в них уязвимостей;

c) анализ и оценку возможных угроз;

d) описание возможных дестабилизирующих воздействий, способных реализовать угрозы;

e) оценку противодействия угрозам принятыми на ОСТ мерами обеспечения безопасности и реализованными механизмами безопасности.

3 МОДЕЛИРОВАНИЕ ПАРАМЕТРИЧЕСКИХ АЛГОРИТМОВ ОЦЕНКИ РИСКОВ БЕЗОПАСНОСТИ ОПТИЧЕСИКИХ СЕТЕЙ ТЕЛЕКОММУНИКАЦИИ

3.1 Анализ инструментальных средств для оценки рисков информационной безопасности

В настоящее время имеется большое разнообразие как методики анализа и оценка рисками, так и реализующие их программные средства, наиболее распространенными из которых является CRAMM, RiskWatch, COBRA, Кондор, Гриф, Авангард, OCTAVE [31-34].

Метод CRAMM был разработан службой безопасности Великобритании по заданию британского правительства. В основе методике CRAMM лежит комплексный подход к оценке рисков, сочетая количественные и качественные методы анализа. Концептуальная схема проведения обследования по методике CRAMM показано на рис.3.1.

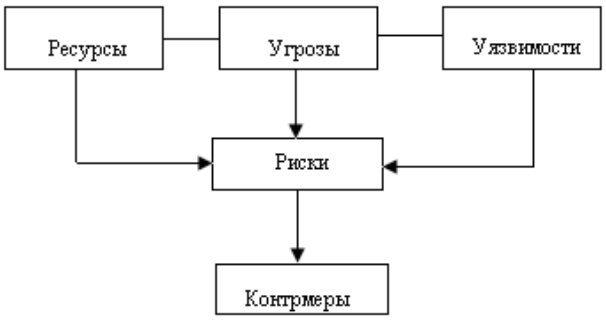

Рис.3.1 - Схема проведения обследования по методике CRAMM

CRAMM предполагает разделение всей процедуры анализа рисков на несколько последовательных этапов. На первом этапе идентификации и оценки ресурсов описывается и анализируется все, что касается идентификации и определения ценности ресурсов системы. Если по результатам проведения этого этапа установлено, что уровень критичности

ресурсов является очень низким и существующие риски заведомо не превысят некоторого базового уровня, то к системе предъявляется минимальный набор требований безопасности. В этом случае генерируется стандартный список контрмер для обеспечения соответствия базовому набору требований безопасности.

Стадия оценивания угроз и уязвимостей выполняется при проведении полного анализа рисков, при этап принимается во внимание все, что относится к идентификации и оценке уровней угроз для ресурсов и их уязвимостей.

Стадия анализа рисков позволяет оценить риски либо на основе сделанных оценок угроз и уязвимостей проведении полного анализа рисков, либо путем использования упрощённых методик для базового уровня безопасности.

Программное обеспечение RiskWatch, разработанное американской компаний RiskWatch Inc., помогает провести анализ рисков и сделать обоснованный выбор мер и средств защиты. Используемая в программных средствах методика состоит из четырех этапов. Первый этап – определение предмета исследования. Второй этап – внесение данных касающихся конкретных характеристик системе на этом этапе:

a) подробно описываются ресурсы, потери и классы инцидентов;
b) с помощью вопросника, база которого содержит более вопросов, выявляются возможные уязвимости;
c) задается частота возникновения каждой из выделенных угроз, степень уязвимости и ценность ресурсов.

Третий этап – оценка рисков. Сначала устанавливаются связи между ресурсами, потерями, угрозами и уязвимостями, выделенными на предыдущих этапах. Для рисков рассчитываются математические ожидания потерь за год по формуле (3.1):

$$m = p \times \vartheta \quad , \tag{3.1}$$

где р – частота возникновения угрозы в течение года, $Э$-стоимость ресурса, который подвергается угрозе.

Четвёртый этап - генерация отчетов.

Система COBRA, разработанная компанией Risk Associates, является средствам анализа рисков и оценки соответствия информационной системы (ИС) стандарту ISO 17799. COBRA реализует методы количественной оценки рисков, а также инструменты для консалтинга и проведения обзоров безопасности. Анализ рисков, выполняемый данным методом, отвечает базовому уровню безопасности, т е уровни рисков не определяются. Достоинство методики – в её простоте. Необходимо ответить на несколько десятков вопросов, затем автоматически формируется отчёт.

Программный продукт Кондор позволяет специалистам по ИБ проверить политику ИБ системы на соответствие требованием ISO 17799. Кондор включает в себе более 100 вопросов, ответив на которые специалист получает подробный отчёт о состоянии существующей политики безопасности, а также модуль оценки уровня рисков соответствие требованием ISO 17799. В отчёте отражаются все положения, политики безопасности, которые соответствуют и не соответствуют стандарту, а также существующий уровень риска невыполнения требований политики безопасности в соответствии со стандартом. Элементам, которые не выполняются, даются комментарии и рекомендации экспертов. Все варианты отчётов для большей наглядная система реализует метод качественном оценки рисков по уровневой шкале рисков: высокий, средний, низкий.

Гриф – это программный комплекс анализа и контроле рисков информационных систем. Данный комплекс делает оценку рисков по различным информационным ресурсом, подсчитывает суммарный риск, а также ведёт подсчёт соотношения ущерба и риска выдаёт недостатки существующей политики безопасности.

Отчётная система программного комплекта Гриф состоит из трёх частей: первая «Информационные риски ресурсов», вторая «Соотношение ущерба и риска», третья «Общий вывод о существующих рисках информационной системы».

Экспертная система «Авангард» включает два программных комплекса: «Авангард – Анализ» и «Авангард – Контроль», каждый из которых базируется на своей методике оценки рисков.

В первом предполагается оценка рисков на основе расчета риско образующих потенциалов компонентов оцениваемой системы. При этом под рискообразующим потенциалом понимается та часть совокупного риска, связанного с системой, которая может быть отнесена на счёт этого компонента. При расчёте рискообразующих потенциалов сначала отроятся модели событий рисков, содержащие по возможности подробное неформальное описание этих событий и перечень угроз, которые могут привести к ним. Далее по каждой модели события риска рассчитывается оценка риска - как произведение оценки вероятности события риска. При этом оценки, как вероятности событий риска, так и степени опасностей событий, предлагается получать с помощью ранговых шкал вероятности имеет фиксированный размер от 0 до 100 (от нулевой до 100 – процентной вероятности возникновения события риска). Нижняя граница отсутствует, по этому шкала строится по следующему принципу. Сначала на неё наносятся те риски, все опасности которых сводится к материальному ущербу и может быть выражена в денежных единицах. В результате получается базовая шкала опасности событий рисков. Далее пользователям предлагается абстрагироваться от «денежной» метрики и воспринимать шкалу как выражающую лишь относительную степень опасности отдельных событий и указывать на ней события рисков путём сравнения степени их нежелательности или недопустимости.

Методика предлагает, что любое событие риска происходит в результате реализации некоторого множества угроз, причём каждая из них может быть определена как угроза безопасности какого-либо компонента оцениваемой системы. Таким образом удаётся определить рискообразующий потенциал каждой из угроз в зависимости от её «вклада» в событие риска, а также рискообразующие потенциалы тех компонентов, к которым эти угрозы относятся, и рассчитать риски по всем структурным составляющим оцениваемой системы и по системе в целом.

Методика комплекса «Авангард - Контроль» посвящена рискам, являющимся результатом невыполнения требований обеспечения безопасности оцениваемой системы и её компонентов, поэтому для применения этого комплекса необходимо для каждого компонента оцениваемой системы иметь полный набор требований, выполнение которых означает нулевой риск нарушения безопасности системы.

Методология OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) была разработана в Институте программной инженерии при Университете Карнеги—Меллона и предусматривает активное вовлечение владельцев информации в процесс определения критичных информационных активов и ассоциированных с ними рисков.

Ключевые элементы OCTAVE:

a) идентификация критичных информационных активов;

b) идентификация угроз для критичных информационных активов;

c) определение уязвимостей, ассоциированных с критичными информационными активами;

d) оценка рисков, связанных с критичными информационными активами.

OCTAVE предусматривает высокую степень гибкости, достигаемую путем выбора критериев, которые предприятие может использовать при адаптации методологии под собственные нужды. Методология разработана для применения в крупных компаниях, а ее растущая популярность привела к

созданию версии OCTAVE-S для небольших предприятий. Имеются коммерческие программные продукты, реализующие положения OCTAVE.

Методология CORAS разработана в рамках программы Information Society Technologies. Ее суть состоит в адаптации, уточнении и комбинировании таких методов проведения анализа рисков, как Event-Tree-Analysis, цепи Маркова, HazOp и FMECA. CORAS использует технологию UML и базируется на австралийском/новозеландском стандарте AS/NZS 4360: 1999 Risk Management и ISO/IEC 17799-1: 2000 Code of Practice for Information Security Management. В этом стандарте учтены рекомендации, изложенные в документах ISO/IEC TR 13335-1: 2001 Guidelines for the Management of IT Security и IEC 61508: 2000 Functional Safety of Electrical/Electronic/Programmable Safety Related. В соответствии с CORAS информационные системы рассматриваются не только с точки зрения используемых технологий, но с нескольких сторон, а именно как сложный комплекс, в котором учтен и человеческий фактор. Правила данной методологии реализованы в виде Windows- и Java-приложений

Сравнение различных методик оценки рисков приведено в таблице 3.1.

Таблица 3.1

Сравнение оценки рисков информационной безопасности оптические сети телекоммуникаций на базе программных продуктов

Методика	Область применения		Достоинства	Недостатки
	Базовый уровень	Полный анализ рисков		
1	2	3	4	5
CRAMM		+	Является хорошо структурированной и широко о пробированной методикой анализа, позволяющей получать реальные практические	Требует специальной подготовки и высокой квалификации аудитор. В большей степени подходят для аудита уже существующих информационных систем, находящихся на

Продолжение таблицы 3.1

1	2	3	4	5
			результаты. В основе программного продукта лечит достаточно объемная база знании по контрмерам в области ИБ, базирую на рекомендациях стандарта В ISO 17799	стадии эксплуатации. Не позволяет создавать собственные шаблоны отчётов и модифицировать имеющиеся.
Risk – Watch		+	Простота, малая трудоёмкость, возможность создания собственных профилей. Упрошённый подход к описанию модели информационной системы и оценке рисков.	Высокая стоимость
COBRA	+		Простота методики, возможность использование различных баз знаний.	Возможность внесения дополнений в базу знаний не доступно пользователям.
Кондор	+		Возможность генерации отчётов по одному или нескольким разделам стандарта ISO 17799	Небольшая градация шкала риска
Гриф		+	Простота в использовании, возможность оценки рисков по различным информационным ресурсам	Генерирует большое количество бумажной документации, которое не всегда оказывается полезной на практике.
Авангард		+	Возможность построения модели рисков и оценка остаточного риска	Достаточно трудоёмкий процесс аудита.
OCTAVE		+	методологией оценки рисков, которая включает выполнение всех фаз по определению и оценке критичных активов, угроз и уязвимостей	Отсутствует оценка рисков на техническим уровне.

Продолжение таблицы 3.1

1	2	3	4	5
CORAS		+	CORAS является то, что программный продукт, реализующий эту методологию, распространяется бесплатно и не требует значительных ресурсов для установки и применения.	В CORAS не предусмотрена периодичность проведения оценки ИТ-рисков и обновление их величин, что свидетельствует о том, что методология пригодна для выполнения разовых оценок и не годится для регулярного использования.

3.2 Моделирование параметрических алгоритмов оценки рисков информационной безопасности оптических сетей телекоммуникации на основе методе нечеткой логики

Механизмы оценки рисков на основе нечеткой логики включают в себя последовательность этапов, в каждом из которых используются результаты предыдущего этапа. Последовательность этих этапов обычно следующая:

a) ввод правил программирования в виде продукционных правил («ЕСЛИ,… ТО»), отражающих взаимосвязь уровня входных данных и уровня риска на выходе;

b) Задание функции принадлежности входных переменных (как пример - с помощью специализированных программ вроде "Fuzyy logic" — в данном примере мы использовали MatLab).

c) Получение первичного результата оценок входных переменных.

d) Фазификация оценок входных переменных (нахождение конкретных значений функций принадлежности).

e) Агрегирование (подразумевает проверку истинности условий путем преобразований функций принадлежности через нечеткую конъюнкцию и нечеткую дизъюнкцию).

f) Активизация заключений (нахождение весовых коэффициентов по каждому из правил и функций истинности).

g) Аккумуляция заключений (нахождение функции принадлежности для каждой из выходных переменных).

h) Дефазификация (нахождение четких значений выходных переменных).

3.2.1 Моделирование параметрических алгоритмов оценки рисков информационной безопасности на основе теории нечетких множеств с использованием MATLAB

3.2.1.1 Моделирование двухпараметрического алгоритма оценки риска с трехуровневыми шкалами входных параметров

Таблица 3.2

Оценка риска по трехуровневым шкалам

Вероятность	Ущерб		
	«Большой»	«Средний»	«Низкий»
«Большая»	Б	С	Н
«Средняя»	С	С	Н
«Низкая»	Н	Н	Н

Продукционные правила, соответствующие таблице 3.2, можно представить следующим образом:

а) ЕСЛИ Вероятность «Большая» И Ущерб «Большой», ТО Риск = «Большой» (Б);

b) ЕСЛИ Вероятность «Большая» И Ущерб «Средний», ТО Риск = «Средний» (С);

c) ЕСЛИ Вероятность «Большая» И Ущерб «Низкий», ТО Риск = «Низкий» (Н);

d) ЕСЛИ Вероятность «Средняя» И Ущерб «Большой», ТО Риск = «Средний» (С);

e) ЕСЛИ Вероятность «Средняя» И Ущерб «Средний», ТО Риск = «Средний» (С);

f) ЕСЛИ Вероятность «Средняя» И Ущерб «Низкий», ТО Риск = «Низкий» (Н);

g) ЕСЛИ Вероятность «Низкая» И Ущерб «Большой», ТО Риск = «Низкий» (Н);

h) ЕСЛИ Вероятность «Низкая» И Ущерб «Средний», ТО Риск = «Низкий» (Н);

i) ЕСЛИ Вероятность «Низкая» И Ущерб «Низкий», ТО Риск = «Низкий» (Н).

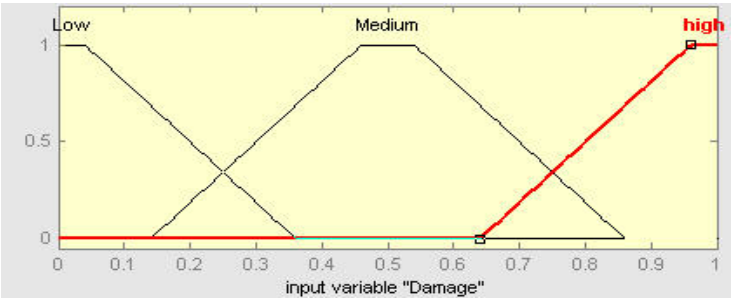

Рис. 3.2 - Трапециевидные функции принадлежности трехуровневой шкалы "ущерба"

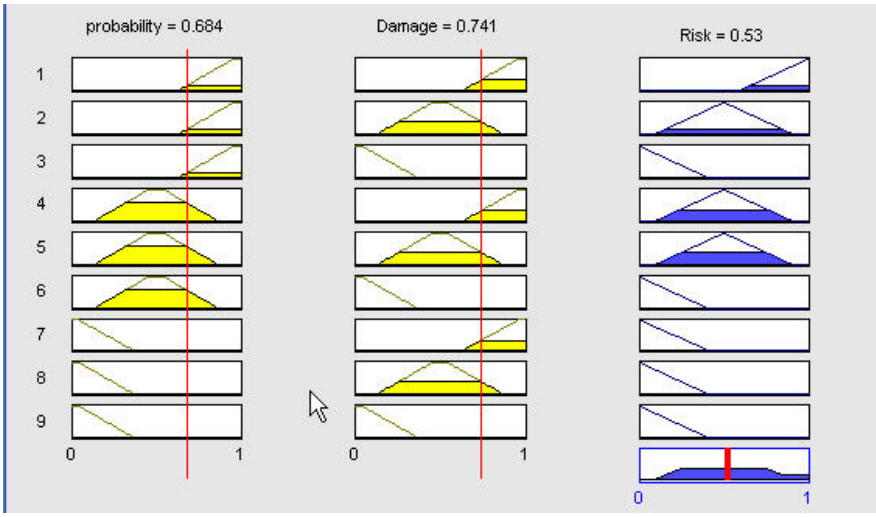

Рис. 3.3 - Ввод оценок входных переменных в механизм вывода

Для определенности положим, что на основе предварительного обследования получены некоторые оценки вероятности инцидента и ущерба, например, 0,683 и 0,741, которые введем в окно Input графического интерфейса (рис. 3.3).

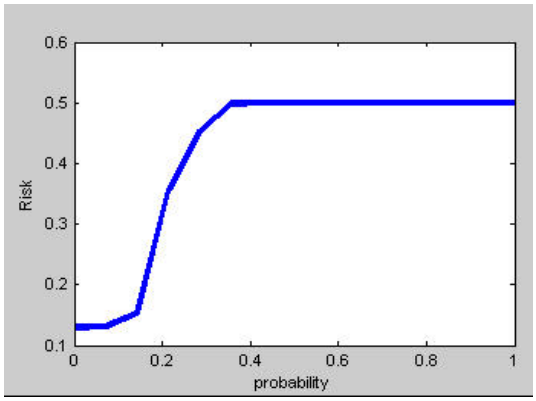

Рис.3.4 - Кривая вывода для трехуровневых входных шкал

График «кривой вывода» – зависимости величины риска от вероятности инцидента, построенный с помощью интерфейса Fuzzy Logic Toolbox представлен на рисунок 3.4. Наглядное графическое представление позволяет оценить адекватность свойств механизма вывода предъявляемым требованиям. В данном случае «кривая вывода» свидетельствует о том, что

механизм вывода можно использовать только в области низких значений вероятности, т.е. при вероятности меньше 0,5.

3.2.1.2 Моделирование двухпараметрического алгоритма оценки риска с пятиуровневыми шкалами входных параметров

Рассмотрим двухпараметрический алгоритм с пятиуровневыми шкалами. Предположим, что алгоритм остается двухпараметрическим, но для измерения входных параметров используются пятиуровневые шкалы. Шкала вероятности содержит следующие уровни:

a) A – событие практически никогда не происходит;

b) B – событие случается редко;

c) C – вероятность события за рассматриваемый промежуток времени приблизительно равна 0,5 (событие вполне возможное при соответствующем стечении обстоятельств);

d) D – скорее всего событие произойдет (при организации атаки);

e) E – событие, вероятнее всего, произойдет (при организации атаки).

Шкала ущерба содержит также пять уровней:

a) N (Negligible) – ущерб, которым можно пренебречь;

b) Mi (Minor) – незначительный ущерб, последствия которого легко устранить;

c) Mo (Moderate) – умеренный ущерб;

d) S (Serious) – серьезный ущерб, ликвидация которого возможна, но связана со значительными затратами;

e) C (Critical) – критический ущерб, который ставит под сомнение возможность устранения его последствий.

Шкала для оценки риска может быть задана в виде последовательности чисел от 0 до 8, включительно. Зависимость риска от вероятности ущерба приведена в табл.3.3.

Таблица 3.3

Шкала оценки риска по пятиуровневым шкалам

Вероятность	Ущерб				
	N	Mi	Mo	S	C
A	0	1	2	3	4
B	1	2	3	4	5
C	2	3	4	5	6
D	3	4	5	6	7
E	4	5	6	7	8

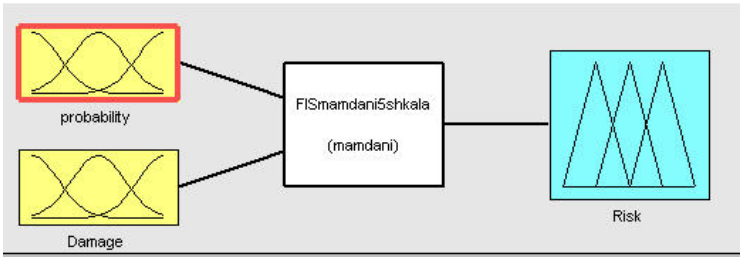

Рис.3.5 – Двух параметрический система нечеткого вывода

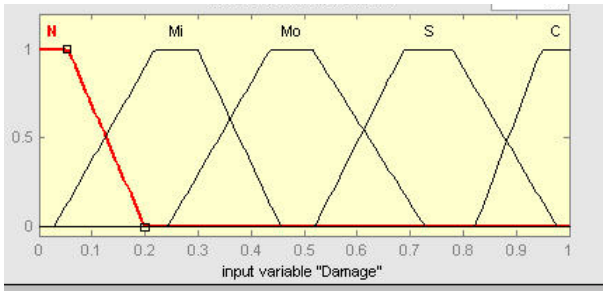

Рис.3.6 - Функции принадлежности на пятиуровневой шкале

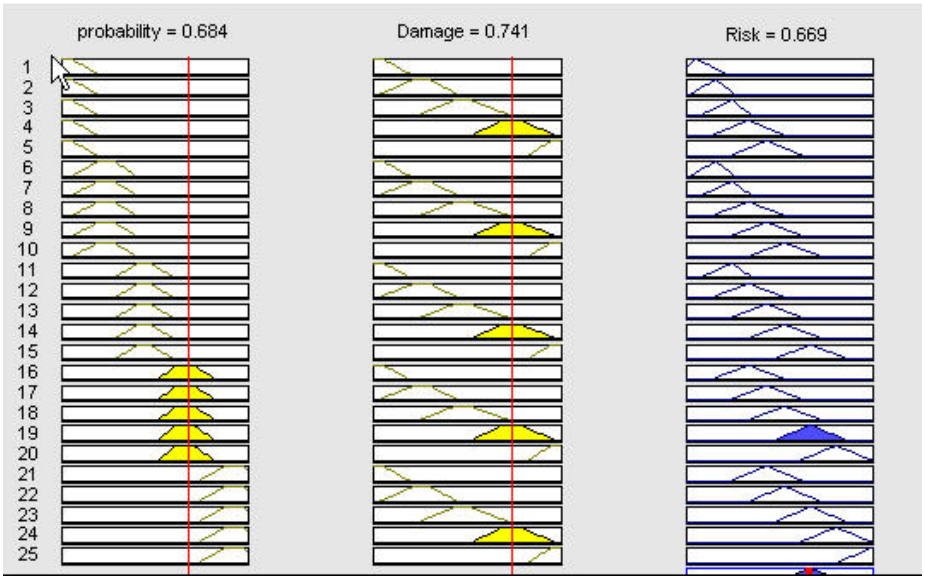

Рис.3.7 - Механизм вывода для пятиуровневых шкал

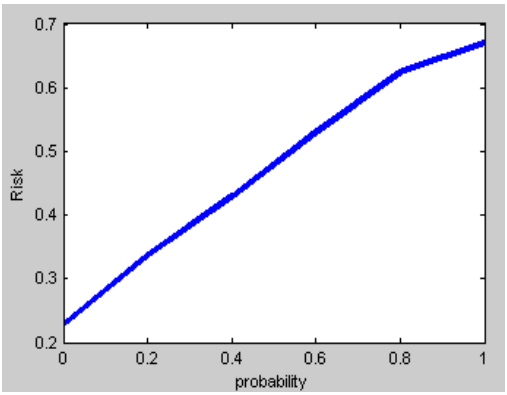

Рис.3.8 - Кривая вывода для пятиуровневых входных шкал

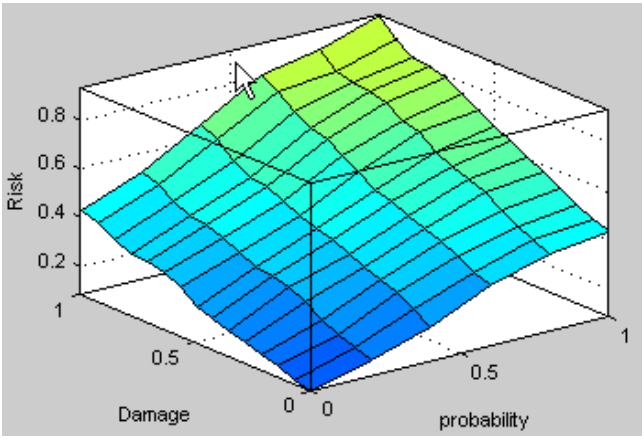

Рис. 3.9 - Поверхность нечеткого вывода для пятиуровневых шкал входных данных

Графический интерфейсе Fuzzy Logic Toolbox позволяет получить трехмерное изображение «поверхности системы нечеткого вывода» (рисунок 3.9). Гладкая и монотонная «поверхность вывода» гарантирует «качество» используемого алгоритма во всем диапазоне изменения входных переменных.

Функции принадлежности входных переменных, как и в предыдущем случае, зададим с помощью линейный функций. Число функций принадлежности на осях входных переменных в данном случае равно пяти. Параметры функций принадлежности определяются программой интерфейса. Для выходной переменной число функций принадлежности следует задать равным девяти. Предположим, как и ранее, что с помощью диагностических тестов или на основе экспертного обследования системы получены оценки входных переменных: вероятности инцидента и предполагаемого ущерба. Характерно, что полученный результат существенно отличается от оценки риска полученной в предыдущем примере для трехуровневых шкал входных величин, хотя входные переменные были одинаковыми. В последнем случае график "кривой вывода" имеет "завал" при вероятности большей 0.5, что и отражает низкую чувствительность трехуровневого алгоритма в области высоких значений вероятности.

3.3 Выводы

Из выше изложенного можно отметить следующее:

1. Разработан механизм получения оценок риска для практического использования. Данный механизм позволяет не только решить поставленные задачи, но и существенно расширить возможности указанных методик. Он позволяет снять ограничения на число учитываемых входных переменных и адекватно использовать качественные и количественные оценки входных параметров, исходящие от прикладных специалистов.

2. Механизм получения оценок риска на основе нечеткой логики позволяет учитывать качество входной информации и надежность (степень

доверия) источников информации. Он обладает широкими возможностями, позволяющими адаптировать его к разнообразным "профилям" прикладных систем и встраивать их в состав собственных разработок систем управления рисками.

3. Указанные обстоятельства и наличие открытых универсальных пакетов прикладных программ для обработки нечеткой информации в среде MATLAB и fuzzyTECH позволяют рекомендовать их для широкого использования.

ЗАКЛЮЧЕНИЕ

Результаты проведенных исследований позволяют отметить следующее:

1. В условиях широкого использования зарубежных технических средств телекоммуникаций и программного обеспечения необходимо проведение разумной технической политики, сочетающей в себе создание ОСТ с соблюдением требований по безопасности информации. Интенсивное внедрение зарубежных оптических технологий телекоммуникаций сопровождается появлением новых угроз и уязвимостей, которые существенно расширяют возможности нарушителей по негативному воздействию на информационную сферу ОСТ, поэтому требования к информационной безопасности ОСТ должны формироваться и устанавливаться с учетом последствий, к которым могут привести инциденты информационной безопасности, и тех затрат, которые необходимы для их устранения.

2. Международная практика показывает, что в настоящее время на операторов телекоммуникаций, как на непосредственных собственников ОСТ, возлагаются основные функции по обеспечению информационной безопасности, такие как защита от несанкционированного доступа к объектам телекоммуникаций, входящих в состав этих сетей, а также защита информации, передаваемой по этим сетям, и информации управления сетями.

3. Исследования показывают, что без использования специальных мер, методов обеспечения информационной безопасности и механизмов безопасности (средств защиты информации) ОСТ являются абсолютно уязвимыми перед угрозами информационной безопасности и что обеспечение информационной безопасности современных ОСТ является объективно необходимым.

4. Решение проблемы оценки информационной безопасности, возникающей при создании современных ОСТ, необходимо проводить на серьезной научной основе с учетом международного опыта, стандартов и рекомендаций.

5. Известно, что комплексную характеристику степени удовлетворения пользователя предоставляемыми услугами определяют параметры качества обслуживания, для определения которых необходимо использовать совокупность общих показателей. В новых международных стандартах и рекомендациях ISO, ITU-T, ETSI и др. информационная безопасность рассматривается как один из показателей качества обслуживания (Quality of Service, QoS) ОСТ.

6. В настоящее время информационная безопасность ОСТ не имеет количественной оценки, хотя большая часть других показателей качества обслуживания (достоверность, скорость и надежность) имеют, поэтому одной из важным и актуальным является проблема обеспечения качества обслуживания ОСТ в условиях преднамеренных информационных воздействий.

7. В основе формирования требований, определяющих необходимый уровень информационной безопасности, лежит анализ ОСТ как объектов оценки рисков информационной безопасности. Однако в настоящее время не существует общей методологии, методов и конкретных методик оценки рисков информационной безопасности, поэтому сравнение безопасности различных сетей безопасности чрезвычайно затруднительно.

8. Анализ показывает, что разработка методики оценки рисков информационной безопасности предполагает наличие или разработку: модели объекта оценки, модели системы защиты, модели потенциального нарушителя.

9. В условиях динамичного развития ОСТ и возникновения новых угроз информационной безопасности важным становится анализ и управление рисками информационной безопасности.

10. При использовании качественного метода оценки очень важно, насколько опытен, квалифицирован и компетентен человек, выполняющий оценку уровня риска. Риск оценивается качественно; тем не менее для более легкой интерпретации полученных результатов, а также для оценки риска, используется количественная форма.

Количественный метод требует значительно больше времени, так как каждому фактору риска присваивается конкретное значение; это даёт полную информацию о проведенном анализе ресурсов и объектов.

Применение метода количественной оценки риска требует больших затрат как на описание, так и на анализ бизнес-процессов, но неоспоримым преимуществом данного метода является гарантированная полнота определения перечня рисков.

11. Второе направление оценки информационной безопасности ОСТ основывается на определении числовых характеристик информационной безопасности технологий телекоммуникаций (количественные критерии). Методика количественной оценки рисков дает точные цифры возможных потерь при возникновении инцидента информационной безопасности.

12. Для повышения качества оценки рисков необходимо исследовать и реализовать, во-первых, механизмы представления нечетких и неполных данных (нечеткие механизмы), во-вторых, механизмы устранения субъективности нечетких и неполных данных и поиска оптимального решения задачи (эволюционные механизмы). Для указанных целей в настоящее время исследуются вопросы применения теории нечетких множеств.

13. Механизм получения оценок рисков безопасности на основе нечеткой логики позволяет учитывать качество входной информации и

надежность (степень доверия) источников информации. Этот механизм позволяет заменить приближенные табличные методы грубой оценки рисков современным математическим аппаратом.

14. Оценку риска можно провести как по двум, так и по трем параметрам: эффективность защиты, потенциал угрозы и возможные потери.

15. По сравнению с вероятностным методом, нечеткий метод позволяет резко сократить объем и время производимых вычислений, что, в свою очередь, способствует увеличению быстродействия нечетких систем, но не способствует повышению точности вычислений.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Muriel Médard, Distributed Algorithms for Attack Localization in All-Optical Networks IEEE Communications Magazine. November 1997, pp. 136-142 http:// web.mit.edu/medard/www/p2.pdf

2 Steven S. Lumetta, Classification of Two-Link Failures for All Optical Networks ECE Department, Optical Society of America 2000.
http:// ieeexplore.ieee.org

3 A.Sridharan, Kumar N. Sivarajan, Blocking in All-Optical Networks, 2006. http:// www.sprintlabs.com

4 Mohammed N. Islam, Information assurance and system survivability in all-optical networks, University of Michigan, 1999. http:// citeseerx.ist.psu.edu

5 Корченко, А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. / А. Г. Корченко — К.: «МК-Пресс», 2006. — 320 с.: ил.

6 Балашов П.А. Оценка рисков информационной безопасности на основе нечеткой логики. // Безопасность компьютерных систем. – 2003. - №5 (№6). – С. 56 – 59 (60 – 65).

7 Петренко С.А. Аудит безопасности Intranet. / С.А. Петренко, А.А. Петренко. - М.: ДМК Пресс, 2002. - 416 с.: ил.

8 Саати Т.Г. Принятие решений. Метод анализа иерархий. / Т. Г. Саати; пер. с англ. Р. Г. Вачнадзе. - М.: «Радио и связь», 1993. - 320 с.: ил.

9 Харитонов Е.В. Согласование исходной субъективной информации в методах анализа иерархий. / Е. В. Харитонов // Математическая морфология. т. 3, выпуск 2. - 1999. - с. 41 - 51.

10 Новиков А.А., Устинов Г.Н.; Под ред. Устинова Г.Н. Уязвимость и информационная безопасность телекоммуникационных технологий. – М.: Радио и связь, 2003.

11 Muriel Médard, Douglas Marquis, Attack Detection Methods for All-Optical Networks, IEEE Communications Magazine. 1998, pp. 107-122 http:// www.isoc.org/

12 Khurram Kazi, Optical Networking Standards: A Comprehensive Guide, USA 2007, springer.com p.840.

13 И.А. Булавкин, Вопросы информационной безопасности сетей PON г. 2004.

14 А. В. Боос, О. Н. Шухардин, Анализ проблем обеспечения безопасности информации, передаваемой по оптическим каналам связи, и путей их решения Журнал «Информационное противодействие угрозам терроризма» 5–2005

15 Манько А., Каток В., Задорожний М.. Защита информации на волоконно-оптических линиях связи от несанкционированного доступа. http://bezpeka.com/files/lib_ru/217_zaschinfvolopt.zip

16 Гришачев В.В., Кабашкин В.Н., Фролов А.Д.. Физические принципы формирования каналов утечки информации в ВОЛС. http://it4business.ru/itsec/

17 International Telecommunication Union, ITU-T recommendations. http:// www.itu.int/itu-t

18 В. В. Крухмалев, В. Н. Гордиенко, А. Д. Моченов и др.; Под ред. В. Н. Гордиенко и В. В. Крухмалева. Основы построения телекоммуникационных систем и сетей: Учебник для вузов - М.: Горячая линия - Телеком, 2004. - 510 с

19 И.А.Каримов, Мировой финансово-экономический кризис, пути и меры по его преодолению в условиях Узбекистана, Ташкент, март 2009.

20 O'z DSt ISO/IEC 15408-1:2007 – Информационная технология – Методы и средства обеспечения безопасности – Критерии оценки безопасности информационных технологий – Часть 1: Введение и общая модель.

21 O'z DSt ISO/IEC 15408-2:2008 – Информационная технология – Методы и средства обеспечения безопасности – Критерии оценки безопасности информационных технологий – Часть 2: Функциональные требования безопасности.

22 O'z DSt ISO/IEC 15408-3:2008 – Информационная технология – Методы и средства обеспечения безопасности – Критерии оценки безопасности информационных технологий – Часть 3: Требования доверия к безопасности.

23 O'z DSt ISO/IEC 27001:2009 – Информационная технология – Методы обеспечения безопасности – Системы управления информационной безопасностью - Требования.

24 O'z DSt ISO/IEC 27002:2008 – Информационная технология – Методы обеспечения безопасности – Практические правила управления информационной безопасностью.

25 Леоненков А.В. Нечеткое моделирование в среде MATLAB и fyzzyTECH.-СПб.:БХВ-Петербург, 2005. – 736с.

26 http://www.ietf.org

27 http://www.etsi.org

28 http://www.oiforum.com

29 http://www.iso.org

30 http:// www.cramm.com/

31 http://www.cert.org/octave/

32 http:// www.riskwatch.com/

33 http://www.riskworld.net/

34 http://www.digitalsecurity.ru/

ПРИЛОЖЕНИЕ