4.1. Стратегии нападения и защиты

В процессе развития конфликта между СИБ и "нарушителем" следует иметь в виду следующие свойства конфликтных зависимостей:

- возможность скачка (катастрофы). При некоторых условиях, особенно при переходе от тактических целей реализации ПЗ к стратегическим, интенсивность взаимодействия и возможные (потенциальные) потери изменяются скачкообразно;

- многоэкстремальность. В процессе взаимодействия конфликтующих сторон их цели могут иметь несколько максимумов и минимумов, как тактических, так и стратегических;

- неоднозначность. Интенсивность конфликта может иметь различную зависимость из-за реализации политики нападения и системы защиты;

- неопределенность. В одних и тех же пределах взаимодействия конфликтующих сторон интенсивность и последствия могут принимать неопределимые значения.

Рассмотрим классификацию конфликта с точки зрения интенсивности взаимодействия СИБ и "нарушителя". Следует выделить следующие возможные подходы [60]:

1. Критериальная классификация. В случае, если противодействующие стороны обладают полной информацией о ситуации и интенсивность взаимодействия равна нулю, то системы нападения и защиты нейтральны, взаимодействия и конфликта нет, их цели независимы. Под влиянием взаимодействия системы изменяют свое поведение и изменяются сами, что является основой критериальной классификации. Изменение интенсивности взаимодействия с противоположными целями может привести к противодействию, затем развиться антагонизм, нестрогое соперничество (нестрогий конфликт), строгое соперничество (строгий конфликт).

Следует отметить, что в результате конфликта может измениться не только характер взаимодействия, но форма и содержание самой СИБ и АИС. Другими словами, интенсивное взаимодействие может совмещать черты антагонизма и симбиоза и подобный конфликт называют конфликтом эксплуатации. Различают следующие виды эксплуатации (рис.291):

- "доброжелательная", когда обе соперничающие стороны выигрывают в

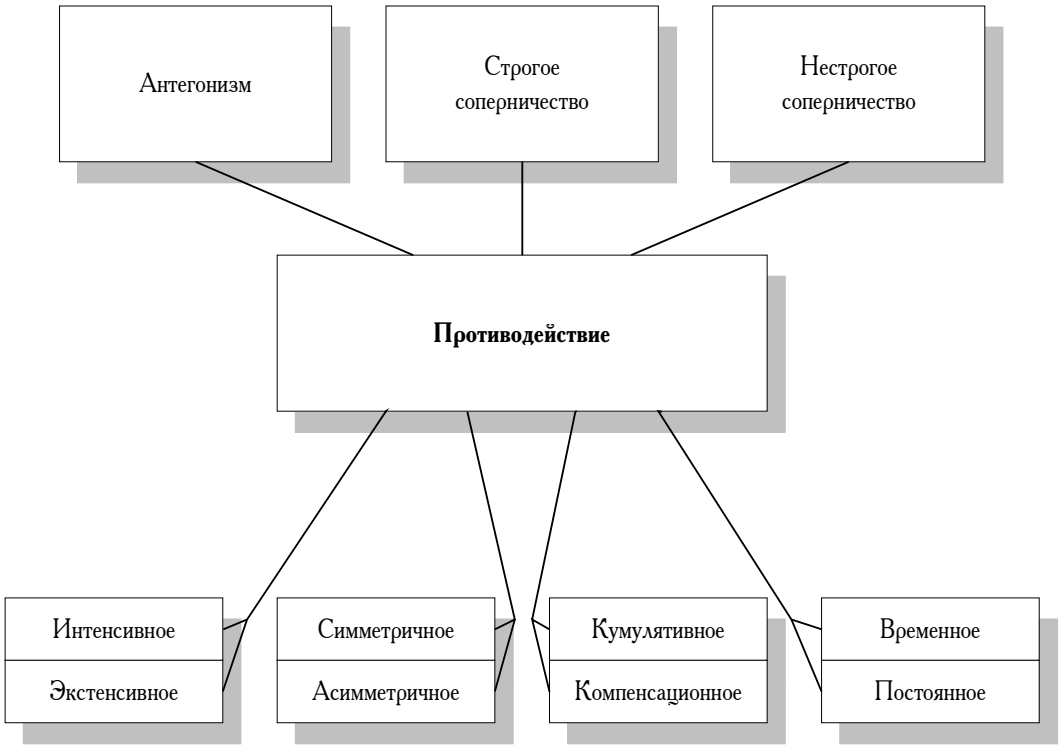

Рис. 29. Схема классификации конфликтов

конфликте, но одна больше другой. Например, при преодолении СИБ нарушителю становятся известны только пароли доступа и дальнейшие попытки проникновения прекращаются. Конфликт эксплуатации остается "доброжелательным", поскольку, с одной стороны, нарушитель получил необходимую информацию, а с другой - после попытки несанкционированного доступа следует смена паролей. Таким образом, противодействующие стороны оказались в ситуации выигрыша;

- "нормальная", когда одна сторона выигрывает за счет другой. Продолжая рассматривать приведенный пример, данный вид эксплуатации характеризует взаимодействие конфликтующих сторон с постоянным выигрышем;

- "злобная", если обе стороны проигрывают, но одна сторона меньше. В данном случае меньший проигрыш должен обеспечить противоположной конфликтующей стороне проигрыш значительно больший.

2. Функциональная классификация. Противодействующие стороны характеризуются видом и составом собственных функций управления:

- если обе функции либо одна из них имеют явную зависимость от времени, то конфликт является нестабильным;

- если функции не зависят явно от времени, то конфликт является стабильным;

- конфликт между системами может быть при обоюдном непрерывном или дискретном управлении;

- в зависимости от используемых ПЗ могут быть конфликты нарастающие, а при использовании соответствующих элементов СИБ - затухающие и периодические.

3. Информационная классификация. Данный вид классификации характеризует объем и характер осведомленности противодействующих сторон. С этой точки зрения выделяют:

- открытый конфликт, когда все функции управления заданы и полностью известны обеим сторонам. Открытые конфликты при преодолении СИБ не встречаются, поскольку открытое противодействие фиксируется и пресекается организационно-техническими средствами;

- односторонний конфликт, наиболее часто встречающаяся систуация "угроза-защита". В данном случае осведомленная сторона (СИБ) не знает как представляет ее противоположная неполно оведомленная сторона.

Реальный конфликт в АИС, с точки зрения реализации ПЗ, далеко не всегда распознаваем. Даже внешние проявления конфликта преобразуются (маскируются) таким образом, что производят не только отдаленное, но и противоположное впечатление. Кроме того, замаскированный, нестрогий конфликт может усиливаться, разрастаться и достичь антагонизма.

Предпримем попытку описать реальный конфликт в АИС. В отличие от абстрактного с безразмерными величинами, в реальном конфликте фигурируют физические измеримые величины, оцениваемые по условным шкалам. Дополнительные трудности возникают при описании математических операций над ресурсами (трудовыми, вычислительными и т. д.), поскольку противостояние ПЗ зависит от уровня добросовестности и моральной устойчивости персонала. Поэтому описание реального конфликта требует тщательного обоснования не только в формальном, но и морально-этическом аспектах.

Кроме того, восприятие конфликта не должно быть сведено только к противодействию. Во-первых, определить класс конфликта без подробного его исследования невозможно, так как внешние проявления не могут полностью характеризовать ПЗ. Во-вторых, классы конфликтов, как и классы ПЗ не

вполне стабильны. В-третьих, при делении конфликтов на “полезные” и “вредные”, результаты определяются интервалом оценки (временное противодействие типа “нестрогое соперничество” может являться стимулом для эволюции системы безопасности).

Охарактеризуем основные положения реального конфликта [64];

- при полной информации сторон, симметричном конфликте и одинаковых ресурсах исход конфликта определяется рациональностью распределения ресурсов сторон;
- при полной информации сторон, симметричном конфликте, одинаковых ресурсах, в зависимости от действий сторон конфликт может перейти из любого критериального класса в любой другой критериальный класс;
- при полной информации, симметричном (кроме управления запаздываением) конфликте и одинаковых ресурсах преимущество имеет сторона с меньшим запаздыванием управлений;
- при неполной информации сторон существует экстремум относительной оперативности управления и количества информации;
- в исследуемой системе конфликта должен соблюдаться закон “исключенного третьего”;
- если описание конфликта несводимо к единой системе величин, то конфликт многокритериальный;
- многокритериальные конфликты оптимально неразрешимы.

Исследование конфликта требует решение большого количества вопросов, поскольку каждая сторона владеет только своими описаниями и решает конфликт для себя. В рамках СИБ должны проводиться системные исследования относительно решения конфликта за каждую сторону и приниматься решения о достижении возможных целей каждой стороной в складывающейся ситуации.

Интересным является подход В.И. Ярочкина в [156], где представлен сценарий действий нарушителя. При этом выделяются три основных этапа при реализации нарушения:

- информационно-разведывательный этап - сбор необходимой информации об объекте управления и АИС;
- подготовительный этап - создание условий для реализации замысла;
- реализация преступного замысла.

Представляется возможным развить представленный подход и выделить в рамках конфликтов следующие основные циклы:

- *обоснование замысла.* Проводится анализ и оценка потенциальных угроз (или целей нападения), средств и времени, сопоставление тактических и стратегических задач, моделирование ситуации, формирование вариантов замысла (разведка, маскировка, дезинформация), моделирование вариантов и оценка эффективности;
- *разработка замысла.* Подробная разработка и детализация модели действий и противодействий с уточнением оценки эффективности;
- *принятие решения.* На основе предыдущего этапа принимается решение относительно целесообразности осуществления замысла;
- *подготовительный этап.* В соответствии с принятым решением реализуется комплекс организационно-технических мероприятий и осуществляется контроль результатов. На основании новой информации (потенциальные угрозы) повторно выполняются предыдущие этапы.
- *основной этап.* Моделирование конфликта с учетом поступления новой информации.
- *оценка результатов.* Дальнейшее уточнение модели конфликта с определением реальных событий и внесением корректировок.

В соответствии с представленными этапами развития конфликта предлагается стратегия развития конфликта нарушителем и СИБ.

Процесс развития конфликта со стороны нарушителя осуществляется в четырех этапах: аналитического, исследовательского, разработки и реализации (рис. 30).

В рамках аналитического этапа осуществляется постановка задачи, осуществляется декомпозиция задачи, анализируются тактические и стратегические цели, осуществляется уточнение условий и требований, после чего осуществляется обратное агрегирование задачи.

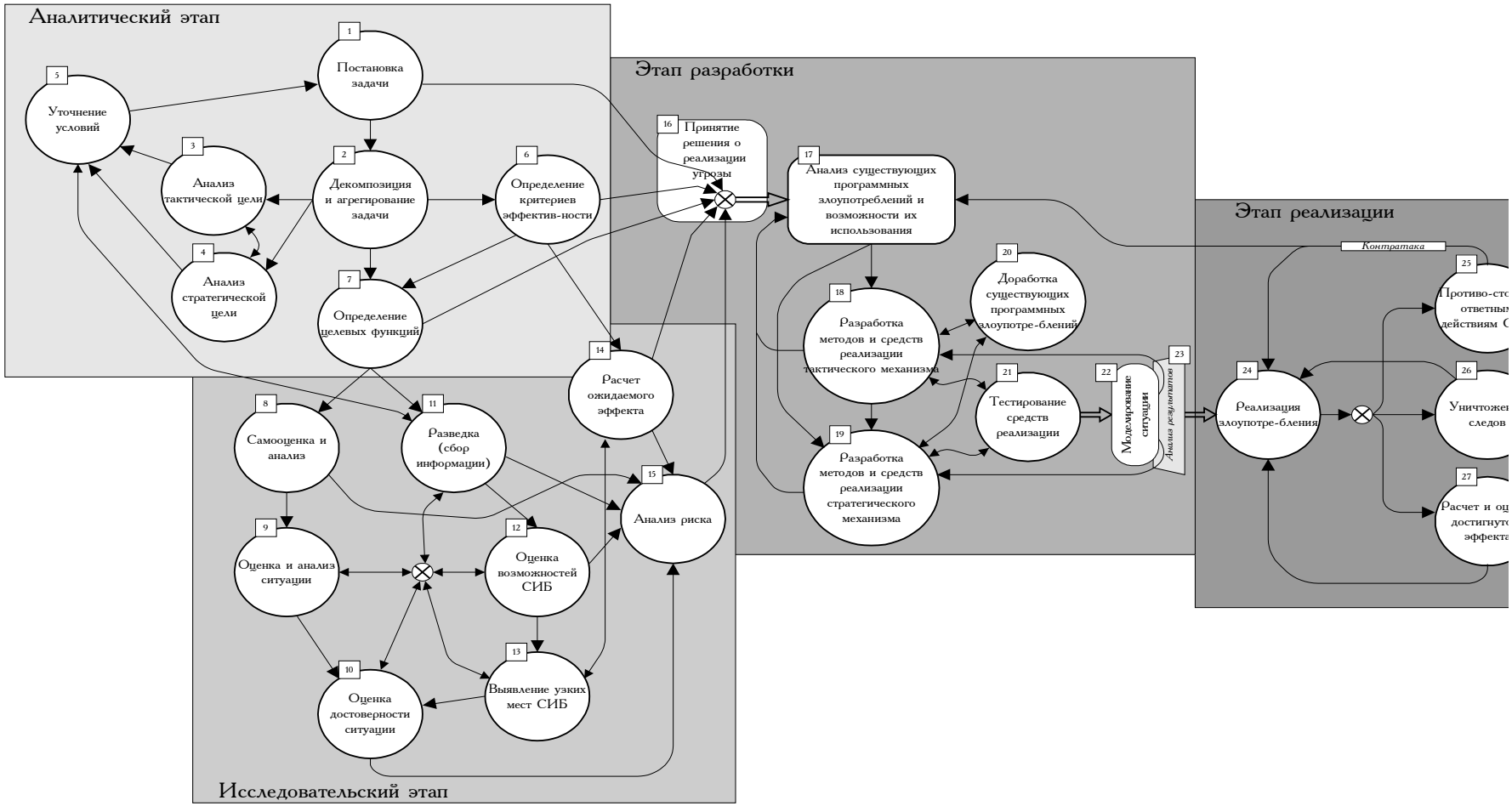

Рис. 30 Стратегия развития конфликта со стороны нарушителя

После декомпозиции и агрегировании определяются критерии эффективности нарушения, на основе чего определяются целевые функции разрабатываемого наушения.

В рамках исследовательского этапа осуществляется самооценка и анализ возможностей реализации угрозы, после чего производится анализ ситуации и ее достоверности. Сбор информации является важной частью реализации угрозы. На основе полученной информации и результатов анализа ситуации осуществляется оценка возможностей реализации угрозы, выявление узких мест СИБ. На основе результатов проведенной работы расчитывается ожидаемый эффект от реализации угрозы. Оценка риска является основным аргументом для принятия решения о разработке и реализации угрозы.

В рамках этапа разработки исследуются и анализируются существующие программные злоупотребления и определяется возможность их применения. На основе проведенного анализа определяется состав программных злоупотреблений, позволяющих достичь тактические и стратегические цели, после чего осуществляется их разработка или доработка существующих. После разработки осуществляется тестирование полученных компонентов программных злоупотреблений, их агрегирование в полиморфное программное злоупотребление. Полученное полиморфное программное злоупотребление тестируется и моделируются ситуации воздействий. Последним шагом в рамках данного этапа является анализ полученных результатов, на основе которых принимается решение о доработке или реализации программного злоупотребления.

Реализация атаки осуществляется одновременно с дополнительным анализом ситуации, риска и др. В случае, если атака завершилась успешно, осуществляется уничтожение следов (если это возможно) с тем, чтобы скрыть факт ее проведения. В случае, если атака была обнаружена, то принимается решении о продолжении атаки (посредством разработки или доработки других программных злоупотреблений) для обязательного достижения результатов.

Продолжением атаки может быть контратака (т.е. противодействие мерам защиты, направленным на обнаружение и ликвидацию результатов атаки программного злоупотребления), основной целью которой является выведение компонентов АИС из строя. Альтернативой атаки может быть прекращение воздействий, основной целью которой является сокрытие источников и средств

атаки. Последним шагом является расчет и оценка достигнутого эффекта от реализации угрозы.

На рис. 31 представлена стратегия развития конфликта (противостояния угрозам) системой информационной безопасности.

В рамках аналитического этапа осуществляется комплекс работ по сбору информации (разведка) из внешнего мира, на момент наличия достаточной информации разрабатывается постановка задачи и определяются целевые функции. После определения целевых функций определяются критерии эффективности. Определение необходимости достижения тактического опережения осуществляется на основе анализа сложившейся ситуации и риска, исходя из определенных целевых функций и критериев эффективности.

В случае, если принято решение о необходимости тактического опережения определяются цели тактического механизма и определяются основные задачи.

Работы по дезинформированию потенциальных злоумышленников должны проводиться на всех этапах развития стратегии разрешения конфликтов. Руководство АИС должны поддерживать работы, направленные на создание соответствующего иммиджа, распространение необходимой информации и т.п.

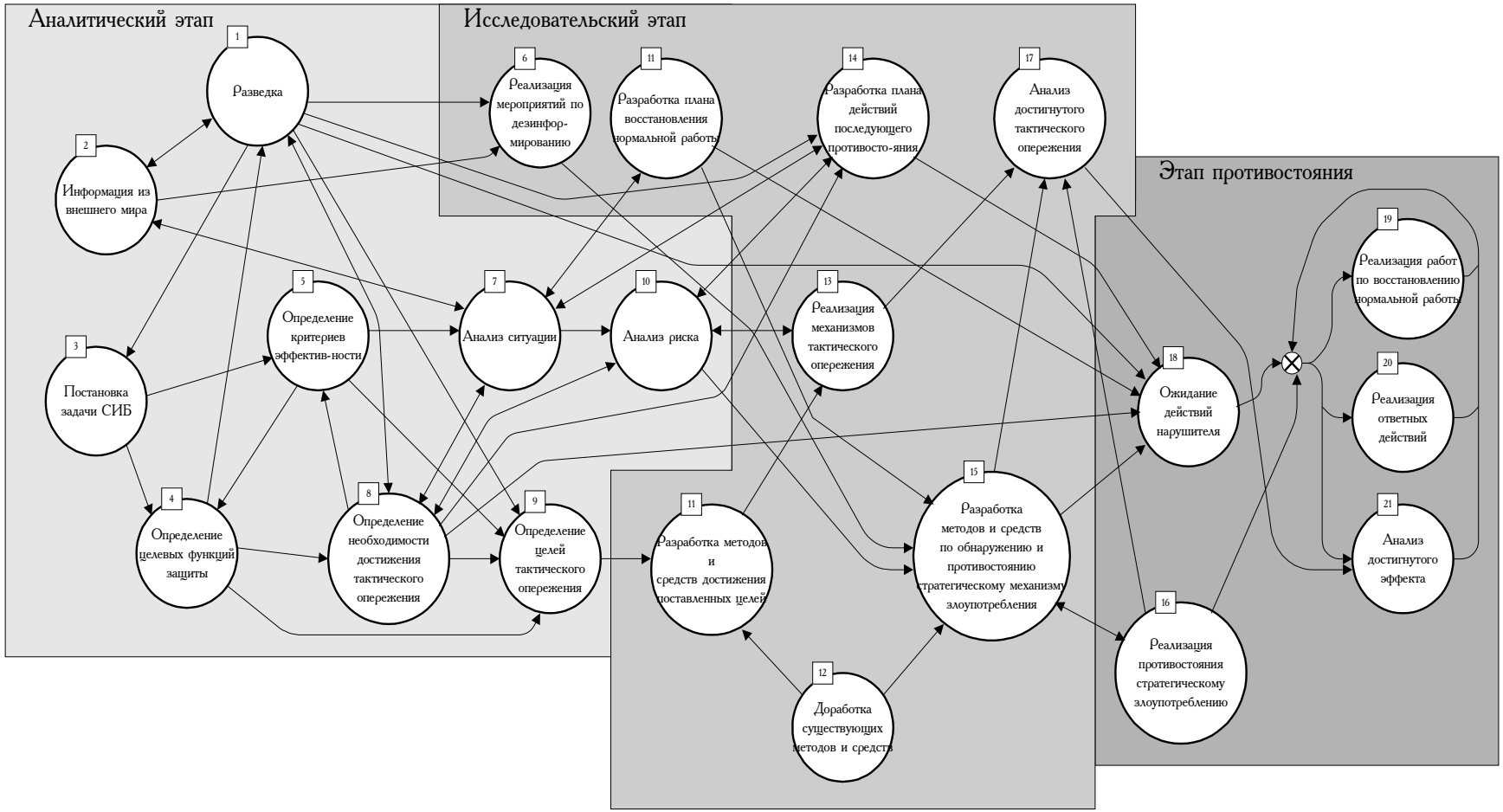

Рис. 31 Стратегия опережения и устранения конфликта системой информационной безопасности.

В рамках исследовательского этапа осуществляется разработка плана восстановления нормальной работы АИС.

В случае, если принято решение о тактическом опережении осуществляется разработка методов и средств достижения поставленных целей или доработка и адаптация уже существующих механизмов и средств, после чего реализуются мероприятия, обеспечивающие тактическое опережение. Также может приниматься решение о реализации ответных действий. На основе проведенных мероприятий осуществляется анализ достигнутого тактического опережения.

В случае, если принято решение об ожидании действий нарушителя, разрабатываются или дорабатываеются методы и средства по обнаружению и противостоянию стратегическому механизму злоупотребления, после чего ожидается первый шаг со стороны нарушителя. Следующим шагом является реализация противостояния стратегическому злоупотреблению. Отдельно может быть принято решение о реализации ответных действий в противовес нарушителю. На основе проделанных мероприятий осуществляются работы по восстановлению нормального функционирования АИС. Последним шагом является анализ эффективности СИБ.

На основе предложенных стратегий нарушителя и СИБ предлагается к рассмотрению ситуация взаимодействия АИС и противостоящей стороны (АИС, коллектив разработчиков, одиночки-изобретателя и др.). В качестве обхекта борьбы выступает ресурс (информация), за которую противостоящая сторона готова платить высокую цену. Доходы каждого $x_1(t)$ и $x_2(t)$ зависит от технического и технологического оснащения. Критерием эффективности является прибыль за время T. Следует отметить, что интервал времени является достаточным, чтобы была возможна реконструкция СИБ, введение технических новшеств. Часть дохода идет на процесс производства, а оставшаяся его часть составляет прибыль.

Скорость изменения доходов x_i конфликтующих сторон описывается следующими уравнениями:

$$x_1(t)=\alpha_1(u_{11},v_{21},t)\,x_2(t-t_2(u_{11}))-\beta_1 x_1(t)+u_{12}(t,{}'_1(T)) \qquad (4.1)$$

$$x_2(t)=\alpha_2(u_{21},v_{12},t)\,x_1(t-t_1(u_{21}))-\beta_2 x_2(t)+u_{22}(t,{}'_2(T)) , \qquad (4.2)$$

$$x_1(t)=j_1(t)$$

EMBED Equation.2 $x_2(t)=j_2(t)$

$$\$_1(T)=\int_0^T g_1(t)x_1(t)\,dt-w_1(u_{11},u_{12},v_{12}) \qquad (4.3)$$

$$\$_2(T)=\int_0^T g_2(t)x_2(t)\,dt-w_2(u_{21},u_{22},v_{21}) , \qquad (4.4)$$

где u_{11},u_{21} - управленческие действия, направленные на получение информации о другой стороне;

$t_2(u_{11}),t_1(u_{21})$ - запаздывания;

u_{12},u_{22} - управления, направленные на улучшение и развитие собственных средств защиты и доступа;

v_{12},v_{22} - управления, направленные на противодействия получения другой стороной информации;

w_1,w_2 - ресурсы, затраченные на управление;

j_1,j_2 - фазы конкурирующих процессов.

Полагая, что $u_{ij}=|u_{ij}|$, получаем

$$\alpha_1(t)=\frac{k_{11}u_{11}(t)+d_1}{k_{22}v_{21}(t)+e_1}-p_1\alpha_1(t) , \qquad (4.5)$$

$$\alpha_2(t)=\frac{k_{21}u_{21}(t)+d_2}{k_{12}v_{12}(t)+e_2}-p_2\alpha_2(t) ; \qquad (4.6)$$

или

$$\alpha_1(t)=k_{11}u_{11}(t)+k_{22}v_{21}(t)+d_{12}-p_1\alpha_1(t) \qquad (4.7)$$

$$\alpha_2(t)=k_{21}u_{21}(t)+k_{12}v_{12}(t)+d_{21}-p_2\alpha_2(t) \qquad (4.8)$$

где $\beta_{1,}\beta_2,k_{ij},d_1,d_2,e_1,e_2,p_1,p_2$ - коэффициенты;

$u_{11}\grave{I}u_1,u_{12}\grave{I}u_2,u_{21}\grave{I}u_2,u_{22}\grave{I}u_2,v_{12}\grave{I}v_1,v_{21}\grave{I}v_2$

Соответственно, ресурсы, затраченные на управление составит:

$$w_1=\int_0^T(\alpha_1u_{11}(t)+b_1u_{12}(t)+c_1v_{12}(t))\,dt=\int_0^T u_1(t)\,dt \qquad (4.9)$$

$$w_2=\int_0^T(\alpha_2u_{21}(t)+b_2u_{22}(t)+c_2v_{21}(t))\,dt=\int_0^T u_2(t)\,dt \qquad (4.10)$$

Для учета новых ПЗ, быстро изменяющих доходы сторон необходимо:

$$x_i(t_j) - x_i(t_i) = w_i(t_j, t_i) x_i(t) Dt_i \qquad (4.11)$$

При $x_i(t) = 0$ и $t_i \le t \le t_j$

$$w_i = \int_0^T u_i(t)\, dt + w_i^{(i,j)} \qquad (4.12)$$

где $w_i^{(i,j)}$ - затраты на переоснащение СИБ