П.9 Модели комплекса «Уязвимость»

Общая схема развития ситуации в условиях террористических угроз отражена на рис.П.9.1. Логика анализа уязвимости следующая. В системе создаются изначальные условия безопасности, т.е. полагается, что система характеризуется целостностью (способностью выполнять множество возложенных на нее функций в соответствии с целевым назначением). Тем самым считается, что при создании и в начале эксплуатации обеспечивается требуемая безопасность (или приемлемый уровень уязвимости) системы. Для выявления уязвимостей и поддержания безопасности на необходимы сбор и обработка информации, они должны быть эффективными – для этого предлагается подсистема «Риск ошибочных аналитических выводов». Далее: на систему оказываются негативные воздействия, для оценки эффективности мониторинга и контроля предлагается подсистема «Риск скрытного внедрения и воздействия источника опасности». Для противодействия опасностям вырабатываются последовательные меры противодействия, они также должны быть эффективными – см. подсистему «Риск преодоления преград». Все эти меры требуют затрат, но несмотря на них, возможны ущербы – для оценки рисков и потенциальных ущербов с учетом затрат предлагается подсистема «Интегральная уязвимость системы». Наконец, для анализа комплексной уязвимости для системы сложной структуры, для элементов которой могут по-разному использоваться, а могут и вовсе не использоваться меры контроля и мониторинга и контроля, предлагается подсистема «Риск нарушения комплексной безопасности». Последняя подсистема вынесена на первое место, т.к. для интегрального анализа именно ее применение является приоритетным. После формирования интегральных условий и требований имеет смысл переходить к остальным подсистемам, позволяющим детализировать оценки на уровне отдельных элементов.

Рис. П.9.1 Схема развития критичных воздействий

Анализ выявленных тенденций позволил сформулировать цепочку логических зависимостей для оценки риска уязвимости системы (см. в подразделе 2.3 рис.2.3.1). Расчет рисков осуществляется на основе математического моделирования.

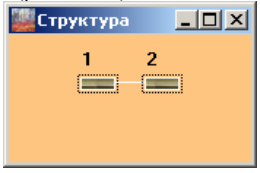
П.9.1 Модель «Риск нарушения комплексной безопасности»

Анализ «Модели процессов выполнения функций системой в условиях ненадежности комплексируемых компонентов» и «Комплекса моделей опасного воздействия на защищаемую системы» показал, что для расчетов предложенных интегральных показателей безопасности функционирования систем ни одна из этих моделей не может быть использована без развития. Однако, совокупность моделей содержит все необходимые атрибуты и при доработке и адекватной комбинации моделей потенциально возможно обеспечить анализ возможностей контроля, мониторинга и поддержания целостности систем сложной структуры.

Основные идеи развития состоят в следующем.

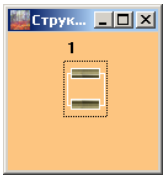
1-я идея. Поскольку модели математические, то путем смыслового переобозначения исходных данных и, соответственно, расчетных показателей, возможно использование одних и тех же моделей для оценки разных показателей. Идея не нова, она упомянута лишь для понимания дальнейшей логики в построении комплексных моделей.

2-я идея. Существующие модели надежности не учитывают на уровне функции распределения возможностей управления процессами. Зато «Модель процессов выполнения функций системой в условиях ненадежности комплексируемых компонентов» (см. подраздел П.1) может быть использована для комплексной оценки показателей в приложении к системам сколь угодно сложной параллельно-последовательной структуры. Сложность оценивается количеством составных элементов. Для этого достаточно знать наработку на отказ каждого из элементов. Рассмотрим простейшую структуру из двух элементов, соединенных последовательно (рис. П.9.1) или параллельно (рис. П.9.2).



ФР времени наработки на отказ $B(t) = 1-[1-B_1(t)][1-B_2(t)]$

Рис. П.9.1 Система из последовательно соединенных элементов



ФР времени наработки на отказ $B(t) = B_1(t)B_2(t)$

Рис. П.9.2 Система из параллельно соединенных элементов

Обозначив для i-го элемента функцию распределения (ФР) времени наработки на отказ через $B_i(t)=P(\tau_i \le t)$, получим:

1) для последовательно соединенных независимых элементов время выхода системы из строя равно минимуму из двух времен τ_i: выхода из строя 1-го или 2-го элементов (т.е система переходит в состояние отказа, когда откажет либо 1-й, либо 2-й элемент). В этом случае для системы в целом

$B(t) = P(\min(\tau_1, \tau_2) \le t) = 1 - P(\min(\tau_1, \tau_2) > t) = 1 - P(\tau_1 > t)P(\tau_2 > t) = 1 - [1 - B_1(t)][1 - B_2(t)]$.

При экспоненциальной аппроксимации

$B(t) = 1 - [1 - B_1(t)][1 - B_2(t)] = 1 - \exp(-t/T_{нар1})\exp(-t/T_{нар2}) = 1 - \exp(-t/(1/T_{нар1} + 1/T_{нар2}))$.

Среднее время наработки системы на отказ $T_{нар}$ равно

$$T_{нар} = 1/(1/T_{нар1} + 1/T_{нар2});$$

2) для параллельно соединенных независимых элементов при горячем резервировании (когда оба элемента находятся в рабочем состоянии и при выходе одного из них другой продолжает функционировать) время выхода системы из строя равно максимуму из двух времен τ_i: выхода из строя 1-го или 2-го элементов (т.е система переходит в состояние отказа, когда откажут оба - и 1-й и 2-й элементы). В этом случае ФР наработки на отказ для системы в целом

$$B(t) = P(\max(\tau_1, \tau_2) \le t) = P(\tau_1 \le t)P(\tau_2 \le t) = B_1(t)B_2(t).$$

При экспоненциальной аппроксимации

$$B(t) = B_1(t)B_2(t) = [1 - \exp(-t/T_{нар1})][1 - \exp(-t/T_{нар2})] =$$
$$= 1 - \exp(-t/(1/T_{нар1})) - \exp(-t/(1/T_{нар2})) + \exp(-t/(1/T_{нар1} + 1/T_{нар2})).$$

Среднее время наработки системы на отказ $T_{нар}$ равно

$$T_{нар} = T_{нар1} + T_{нар2} - 1/(1/T_{нар1} + 1/T_{нар2});$$

3) для параллельно соединенных независимых элементов при холодном резервировании (когда резервный элемент находится в нерабочем состоянии и начинает использоваться лишь после выхода из строя основного элемента) время выхода системы из строя при пренебрежении временем замены равно сумме двух времен τ_i , соответственно ФР представляет собой свертку $B(t) = B_1(t) * B_2(t)$.

Применяя приведенные рекуррентные соотношения, можно получать соответствующие оценки для сколь угодно сложной логической структуры с параллельно-последовательным соединением компонентов. Именно эти соотношения реализованы в предлагаемых программных моделях.

3-я идея. Существующий «Комплекса моделей опасного воздействия на защищаемую системы» применим лишь к системе, свернутой до одного элемента, но также может быть использован самостоятельно в приложении к каждому из независимых элементов. На выходе – вероятность безопасного функционирования в течение заданного времени, дополнение до 1 – это риск нарушения безопасности. Если для каждого элемента просчитать эту вероятность для всех точек $T_{зад.}$ от нуля до бесконечности, то получится траектория ФР времени безопасного функционирования каждого из элементов системы в зависимости от реализуемых мер контроля, мониторинга и поддержания целостности. В свою очередь, известный вид этой ФР (построенной по точкам с использованием указанных выше моделей) позволяет традиционными методами математической статистики определить среднее время безопасного функционирования каждого из элементов системы. А это – необходимые исходные данные для применения предложенной выше модифицированной «Модели процессов выполнения функций системой в условиях ненадежности комплексируемых компонентов» и, соответственно, оценки безопасности функционирования системы параллельно-последовательной структуры любой степени сложности.

Применяя идею 1, предлагается модифицировать и развить исходный «Комплекс моделей опасного воздействия на защищаемую систему» в комбинации с «Моделью процессов выполнения функций системой в условиях ненадежности комплексируемых компонентов» в другой терминологии исходных данных и с переобозначением расчетных показателей (в дальнейшем по тексту их будем называть модифицированными моделями).

Смысл развития предлагаемой модифицированной модели в следующем:

- на уровне переобозначения исходных данных «Комплекса моделей опасного воздействия на защищаемую систему»:

σ – вместо частоты воздействия на систему, осуществляемого с целью внедрения источника опасности, в модифицированной модели - это обратная величина наработки на ухудшение функционирования компонента с начала эксплуатации или момента восстановления (обозначается как $1/T_{к\ ухудш.}$ при решении задач оценки качества функционирования) или частота возникновения угроз системе ($Ч_{угроз}$ при решении задач оценки безопасности);

β – вместо среднего времени активизации проникшего в систему источника опасности в модифицированной модели - это наработка на нарушение приемлемого качества с начала ухудшения функционирования компонента ($T_{к\ наруш.}$ при решении задач оценки качества функционирования) или стойкость меры к реализации угроз ($T_{к\ стойкость}$ – при решении задач оценки безопасности);

$T_{меж}$ – вместо времени между окончанием предыдущей и началом очередной диагностики целостности системы в модифицированной модели - это период между моментами восстановления приемлемого качества компонента при решении задач оценки качества функционирования или период между системными контролями целостности при решении задач оценки безопасности ($T_{к\ между,}$ т.е по сути смысл практически не изменился);

$T_{диаг}$ – длительность диагностики, включая восстановление целостности системы - в модифицированной модели это время полагается учтенным в $T_{меж}$ (при необходимости учета на практике рекомендуется использование исходной модели);

$T_{зад}$ – вместо задаваемого периода непрерывного безопасного функционирования системы в модифицированной модели понимается задаваемый период для оценки (т.е. по сути смысл не изменился).

Добавляется среднее время наработки средств мониторинга на ошибку из исходной модели.

4-я идея. На основе реализации идей 1-3 создана интегральная модель «Риск нарушения комплексной безопасности», комбинирующая существующие модели надежности (не учитывающих возможностей управления процессами контроля, мониторинга и поддержания целостности, но позволяющих проведение комплексных оценок для сложных структур) и защищенности от опасных воздействий (учитывающих влияние контроля, мониторинга и поддержания целостности, но не позволяющих проведение комплексных оценок).

Суть предлагаемого метода расчета интегральных показателей (среднего времени безопасного функционирования как показатель ее стойкости к реализации угроз и риска нарушения безопасного функционирования системы в течение заданного периода времени) для сложных структур в условиях потенциальных угроз отражена на рис. П.9.3. При этом наработка мониторируемых элементов на безопасное функционирование увеличивается за счет поддержания целостности мониторируемых элементов.

Алгоритм расчета среднего времени безопасного функционирования как показатель ее стойкости к реализации угроз и риска нарушения безопасного функционирования системы в течение заданного периода времени приведен на рис. П.9.4.

Для формирования исходных данных согласно функциональной структуре анализируемой системы составляется моделируемая логическая схема системы с точки зрения обеспечения безопасности. Каждый составной комплекс состоит из соединяемых последовательно и/или параллельно функциональных элементов. Принимается во внимание, что каждый элемент обладает стойкостью к реализации угроз, кроме того, в отношении него могут осуществляться меры контроля и мониторинга (а могут и не осуществляться – тогда о его выходе из строя можно узнать лишь по факту свершения, а не в процессе контроля или мониторинга). Выход элементов из строя возможен в результате воздействий угроз, например, со стороны нарушителей санкционированного доступа.

Контроль целостности элементов анализируемой системы осуществляется периодически. Выявленные недостатки оперативно исправляются, чем и достигается восстановление функциональных возможностей системы, т.е поддержание ее целостности. Между периодическими контролями качества элемента, процесса или системы может осуществляться мониторинг их целостности, т.е непрерывное отслеживание их состояния. В отличие от мониторинга полагается, что реализуемый контроль состояния неизбежно

приводит к выявлению начавшегося ухудшения функционирования или фактов нарушенного качества. То есть, полагается, что в результате контроля обеспечивается поддержание целостности, а в процессе мониторинга между контролями целостность системы может оказаться нарушенной. Преимуществом мониторинга является наличие возможности отслеживания готовности между соседними контролями. Если же мониторинг совсем не используется, то скрытные нарушения безопасности, произошедшие в промежутке между контролями, смогут быть выявлены лишь в момент очередного контроля.

Рис. П.9.3 Суть логики предлагаемого расчета интегральных показателей для сложных структур в интересах повышения безопасности систем

Для оценки комплексной безопасности функционирования системы исходными данными являются:
системные характеристики:
структура архитектурного построения системы безопасности (с параллельно-последовательным соединением компонентов);
время восстановления системы;
задаваемый период для оценки;
характеристики к-й меры (компонента) системы:
частота возникновения угроз системе;
среднее время преодоления меры (компонента) в условиях реализации угроз (стойкость меры);
наработка на ошибку средств мониторинга компонента (если таковые имеются в наличии);
период между системными контролями целостности;
затраты на обеспечение функционирования компонента.

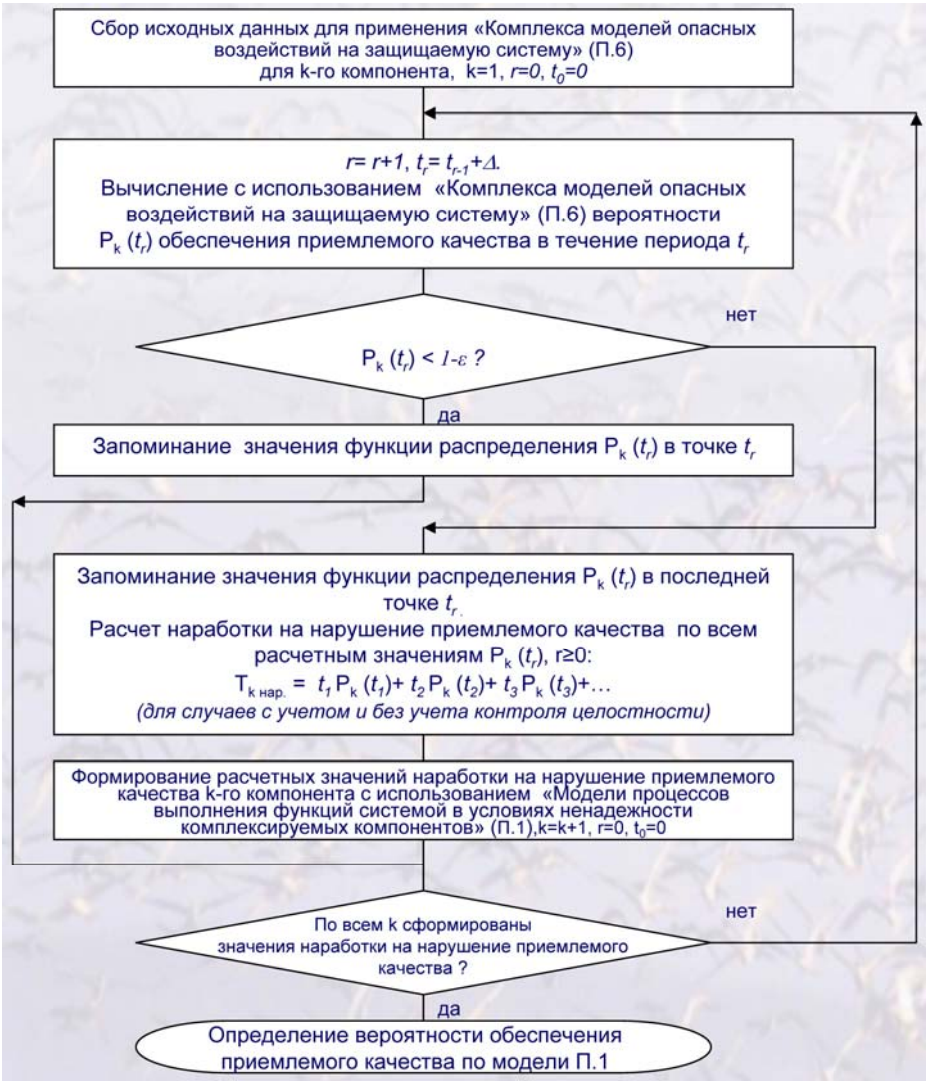


Рис. П.9.4 Алгоритм расчета показателей по модели «Риск нарушения комплексной безопасности»

В результате расчетов оцениваются:

среднее время безопасного функционирования системы без контроля и мониторинга, только с контролем и при использовании системного контроля и мониторинга между моментами контроля;

риск нарушения комплексной безопасности системы в течение задаваемого периода времени без контроля и мониторинга, только с контролем и при использовании системного контроля и мониторинга между моментами контроля с учетом затрат.

П. 9.2 Модель «Риск ошибочных аналитических выводов»

Модель основана на модифицированном применении модели П.5 «Модель процессов анализа объектов (информации, образцов, событий и др.)» с точностью до смыслового переопределения исходных данных. В качестве исходных данных используются:

объём информации о подозрительных событиях;

относительная часть принципиальной информации, объективно имеющей отношение к подготовке террористических актов;

скорость формирования аналитических выводов;

частота ошибок анализа 1-го рода, когда безопасные события воспринимаются аналитиком как имеющие отношение к подготовке террористических актов;

наработка на аналитическую ошибку (2-го рода), т.е. до момента когда аналитиком пропускаются события, имеющие объективное отношение к подготовке террористических актов;

период непрерывной работы аналитика;

допустимое время анализа информации.

В результате расчетов оцениваются риск ошибочных аналитических выводов (R).

П. 9.3 Модель «Риск скрытного внедрения и воздействия источников опасности»

Модель основана на модифицированном применении модели П.6 «Комплекс моделей опасных воздействий на защищаемую систему» с точностью до смыслового переопределения исходных данных. Полагается, что формально для обеспечения защищённости периодически осуществляется профилактическая диагностика целостности системы. Предполагается, что существуют не только средства диагностики, но и способы восстановления необходимой целостности системы при выявлении проникновения источников опасности в систему или следов негативного воздействия. Целостность системы в период между диагностиками отслеживают сменяющие друг друга операторы. Выявление проникших источников опасности и нарушений целостности возможно либо во время безошибочного мониторинга, либо в результате диагностики, после чего сразу осуществляется восстановление целостности. В случае, когда время наработки оператора на ошибку близко к нулю, практически осуществляется лишь профилактическая диагностика

целостности системы. Если же оператор способен выявлять опасности в режиме реального времени (т.е. при задании исходных данных для расчета наработка оператора на ошибку отлична от нуля), моделируется реализуемая технология мониторинга безопасности Опасные воздействия на систему осуществляются поэтапно: сначала источник опасности проникает (внедряется) в систему, а по прошествии свойственного ему периода активизации начинает воздействовать. До активизации проникшего источника опасности функциональная целостность системы не нарушается. Опасность считается реализованной лишь после реального воздействия проникшего источника опасности. Именно с начала такого воздействия целостность системы полагается нарушенной.

В качестве исходных данных используются:

возможная частота воздействия на систему с целью внедрения источника опасности;

среднее время активизации источника опасности, проникшего в систему (прогнозируемое);

время от окончания до начала очередной диагностики целостности системы;

длительность диагностики, включая восстановление целостности;

наработка оператора на ошибку между диагностиками целостности (при мониторинге она больше нуля; задаваемое значение 0 означает, что в качестве меры защиты используется лишь диагностика целостности без непрерывного мониторинга);

задаваемый период для оценки безопасности системы.

В результате расчетов оценивается риск скрытного внедрения и воздействия источников опасности в течение задаваемого периода времени (R) .

П. 9.4 Модель «Риск преодоления преград»

Модель основана на модифицированном применении модели П.7.2 «Комплекс моделей процессов несанкционированного доступа к ресурсам системы» с точностью до смыслового переопределения исходных данных. В качестве исходных данных используются:

количество защитных преград (в зависимости от возможных сценариев реализации угроз);

период между сменами параметров m-й преграды;

длительность террористической атаки как задаваемый период для оценки безопасности системы.

В результате расчетов оценивается риск преодоления защитных преград (R).

П. 9.5 Модель «Интегральная уязвимость системы»

Модель позволяет рассчитать интегральную уязвимость системы в течение задаваемого времени. В дополнение к исходным данным моделей П.9.2-9.4 задаются интересующие варианты развития событий:

вариант 1 – опасное воздействие на систему и преодоление защитных преград в течение заданного периода из-за невыявления подозрительных событий в режиме реального времени;

вариант 2 – опасное воздействие на систему и преодоление защитных преград в течение заданного периода из-за ошибочных аналитических выводов, несмотря на своевременное выявления подозрительных событий

вариант 3 – опасное воздействие на систему и преодоление защитных преград в течение заданного периода, несмотря на своевременное выявления подозрительных событий и корректные аналитические выводы.

Для каждого из трех вариантов свои исходные данные:

количество преград;

время преодоления каждой преграды;

время между сменой параметров;

длительность террористической атаки.

В результате расчетов оцениваются:

риск возможного опасного воздействия на систему и преодоления защитных преград в течение заданного периода из-за невыявления подозрительных событий в режиме реального времени (R1);

риск возможного опасного воздействия на систему и преодоления защитных преград в течение заданного периода из-за ошибочных аналитических выводов, несмотря на своевременное выявления подозрительных событий (R2);

риск возможного опасного воздействия на систему и преодоления защитных преград в течение заданного периода, несмотря на своевременное выявления подозрительных событий и корректные аналитические выводы (R3);

интегральная уязвимость системы (R=R1+R2+R3).