КОМП'ЮТЕРНІ ЗАСОБИ, МЕРЕЖІ ТА СИСТЕМИ

УДК 612.4

В.А. ЧЕРНОМОРЕЦ, С.К. ГОРБУНОВ, Н.С. СТАШКОВА

АНАЛИЗ УГРОЗ ТЕХНОГЕННЫМ ОБЪЕКТАМ

Приведено формально-логическое определение угроз системе. Анализируются методы идентификации и оценки реальных и потенциальных угроз техногенным объектам.

1.1. Определение понятия «угроза»

Сложившиеся определения понятия «угрозы» техногенным объектам заключаются в том, что таковыми считаются любые события или обстоятельства, которые могут стать причиной нанесения ему ущерба или вызвать нарушение нормального функционирования [1]. Иными словами, содержание понятия «угроза» (u) соответствуют описанию логических условий реализации причинно-следственных связей в системе «объект–среда», заданных в форме импликаций типа – если произойдет определенное событие (s), то $E(Q)$ – эффективность функционирования объекта Q уменьшится.

Здесь по умолчанию принимаются следующие аксиомы.

1. Многообразие ситуаций в системе «объект–среда» можно соотнести со значениями логической переменной «угрозы» U, аргументами которой являются значения предметных переменных «время» t, «события» S и «объект» Q.

2. Любое событие $s \in \{S\}$ представляет угрозу u объекту Q (т.е. $s \approx u$) только в тех случаях, когда:

а) атрибуты события s в момент его реализации t являются адекватными характеристикам объекта $X(Q)$;

в) атрибуты события s ухудшают показатели эффективности функционирования объекта Q, т.е. $E(Q) \to \min$.

То есть, констатация факта наличия угроз объекту основана на логически непротиворечивой согласованности следующих предпосылок снижения эффективности его функци-

онирования: t – момент появления события $s \in \{S\}$; A – атрибуты события s (тип физического носителя, амплитудно-частотная характеристика, продолжительность и т.д.); $x \in \{X\}$ – подмножество характеристик объекта, адекватных атрибутам события s.

Обобщением этих и подобных неформальных соглашений являются условия реализации неоднородного, многоместного, многозначного предиката эффективности функционирования объекта, содержание которого можно сформулировать следующим образом: «существуют такие события s и такой момент времени t, когда адекватность атрибутов этих событий характеристикам объекта $F(x, s, t)$, вызывает уменьшение показателей эффективности его функционирования ($E(Q) \to \min$)».

Формальная запись этого предиката имеет вид

$$(S \approx U) = \exists s \, \exists t \, (\, \forall x \, ((F(x, s, t)) \to (\, E(Q) \to \min)). \qquad (1)$$

Отсюда следует, что в зависимости от t момента появления связей вида $F(x, s, t)$ угрозы можно разграничить на реальные, потенциальные и мнимые.

Реальные угрозы – это достоверные события, атрибуты которых являются адекватными имеющимся характеристикам объекта в момент времени $t = t_i$, $F(x, s, t_i)$.

Потенциальные угрозы – события, атрибуты которых могут стать адекватными будущим характеристикам объекта, т.е. $F(x, s, t_{i+k})$.

Мнимые угрозы – события, для которых эти связи маловероятны или невозможны в рамках существующих гипотез о принципах их порождения, т.е. $P(F(x, s, t_{i+k})) \to 0$, где P – вероятность.

Современные исследования в области повышения безопасности техногенных объектов фактически направлены на решение различных прикладных задач связанных с управлением условиями реализации этого предиката. В зависимости от акцентов в отношении вклада в условия его реализации конкретных предметных переменных, многообразие существующих в этом отношении подходов базируется на двух методологиях.

Методология необходимости ориентирована на управление условиями адекватности характеристик объекта и событий $F(x, s, t)$ путем совершенствования характеристик объекта. Это предполагает идентификацию его «уязвимых» мест, оценку последствий нежелательных воздействий и другие процедуры, направленные в итоге на сохранение паспортной эффективности функционирования данного объекта при реализации всех разновидностей ожидаемых угроз.

Методология достаточности ориентирована на управление адекватностью $F(x, s, t)$ путем парирования атрибутов одиночных угроз. Это связано с идентификацией причинно-следственных связей в среде порождающих события, которые представляют угрозу объекту, прогнозированием моментов их появления и точек приложения, а также других характеристик, параметры которых могут быть заблаговременно учтены при проектировании объекта или при организации адресной защиты его подсистем.

В настоящее время преимущественно развиваются методы первого типа, связанные с идентификацией угроз и анализом последствий их реализации.

1.2. Идентификация событий, представляющих угрозу объекту

В отношении методов идентификации угроз наиболее показательными являются подходы, развиваемые в рамках теории потенциальной эффективности сложных систем, теории катастроф и теории защиты информационных ресурсов в компьютерных системах.

1. Проблема угроз техногенным объектам впервые начала рассматриваться в рамках **теории потенциальной эффективности сложных систем** в контексте описания взаимодействия двух систем, имеющих различные цели, т.е. в конфликтных ситуациях [2]. Считается, что в этом случае стратегической целью поведения каждой системы является снижение эффективности функционирования другой путем захвата ее ресурсов.

В свою очередь, вероятность достижения этой цели определяется вероятностями достижения тактических целей, описанных в терминах различных качественных свойств системы (например, надежность, управляемость, помехоустойчивость и пр.).

Эффективность такого противостояния в каждой системе описывается целевым функционалом, экстремум которого определяется формой ее защитного поведения. То есть, взаимные угрозы конфликтующих систем рассматриваются как разновидность их активной защиты.

2. **Теория катастроф и теория устойчивости** рассматривают угрозы объекту как неизбежное следствие особенностей характеристик процессов, лежащих в основе его функционирования. По разным причинам в диапазонах вариаций переменных его состояния могут существовать области, в которых при гладком изменении параметров управлений параметры этих переменных изменяются скачком. Для исследования данных областей и соответствующих им управлений используются аналитические и топологические методы [3].

Проблема угроз в этом случае решается комплексно – путем повышения устойчивости характеристик объекта вблизи этих областей и ввода ограничений на соответствующие им параметры управлений.

3. Наиболее полно проблемы угроз проработаны в связи с **защитой информационных ресурсов**.

В этом случае исходят из того, что задачи идентификации угроз и защиты от них являются взаимосвязанными. Так, согласно стандартам США [4], для организации «правильной» циркуляции информационных потоков в информационных системах необходимо предварительно синтезировать формальную модель системы защиты. Такая модель должна включать полную систему аксиом и иметь формальные доказательства теорем для свойств необходимости и достаточности сохранения состояния защищенности информации при всех переходах в пространстве состояний. Это позволяет сформировать список запрещенных

каналов доступа к информации ограниченного пользования, относительно которых и требуется организовать защитные мероприятия.

При практической реализации этой идеи возникают сложности, обусловленные следующими причинами.

1. При анализе «уязвимых» мест защищаемой системы предполагается, что угрозы будут возникать на «старых» принципах. Имеется в виду, что теоретическая модель защиты строится исходя из системы аксиом и допущений, основанных на обобщении существующих принципов проектирования элементной базы и разработки матобеспечения. На момент создания системы часть этих постулатов становятся неадекватными новым технологическим и программным возможностям.

2. Реализация теоретической модели защищенной системы предполагает целенаправленное проектирование ее архитектуры и контроль на всех этапах технологического цикла, связанного с ее изготовлением. В результате , на момент создания, стоимость такой системы защиты превышает стоимость информации, которую она призвана защищать. Поиск экономических компромиссов приводит к тому, что в итоге появляются неучтенные запрещенные каналы.

3. Наибольшие сложности связаны с двойным назначением интерфейса такой системы. С одной стороны, он должен обеспечить дружелюбное взаимодействие с пользователем, а с другой – ограничить действия нарушителя, притом, что используются одни и те же каналы связи с системой обработки информации. Поскольку отсутствуют методы семантического анализа программ, целевую ориентацию их поведения можно разграничить только на последних этапах. Это дает множество возможностей для организации доступа к информации ограниченного пользования через служебные программы и недокументированные команды процессора.

В итоге, все это реализуется в многообразии форм проявления угроз, различиями во внутренней организации, жизненном цикле, среде формирования и пр. Поэтому современные классификаторы угроз компьютерным системам строятся путем их группировки по характерным признакам в зарегистрированных прецедентах, что скорее обобщает личный опыт исследователя в этой области.

4. Анализ способов идентификации угроз можно продолжить в рамках психологии общения и конфликтологии, где под ними понимаются недружелюбные намерения одного лица в отношении другого.

Общим недостатком этих методов идентификации и классификации угроз является стремление установить некие закономерности на уровне их первичных признаков или в лучшем случае сценариев, хотя достаточно очевидно, что на этом уровне угрозы и «правильные действия» не различимы.

1.3. Методы оценки угроз техногенным объектам

Для оценки угроз в настоящее время существует различные подходы, основанные на анализе априорных или апостериорных оценок функционирования объекта в случае их реализации.

Для определения **априорных оценок последствий** одна из первых методик была предложена специалистами фирмы *IBM* относительно оценок угроз информационным системам и заключалась в определении ожидаемого ущерба R_i от i-й угрозы:

$$R_i = 10(S_i + V_i - 4), \qquad (2)$$

где S_i – частота возникновения i-й угрозы, V_i – ожидаемые потери в случае реализации этой угрозы. Соответственно, ожидаемый ущерб от всех угроз $R = \sum R_i$.

Предполагается, что величина S_i принимает значения согласно шкале, учитывающей интервалы времени, в пределах которых можно ожидать их появления. Каждому из этих интервалов присваивается свой вес. Например, если событие случается один раз в 1000 лет, то оно имеет вес 1, три раза в день – 7.

Аналогично и показатель относительных потерь V_i оценивается по шкале стоимости ликвидации угроз, границами которой и весами являются 1 дол – 0, 10 000 000 дол. – 7.

Подобный подход с незначительными изменениями используется до настоящего времени и зафиксирован в национальном стандарте США *ISO* 13335 [5]. В ближайшее время этот же метод предполагается использовать и в национальном стандарте Украины ДСТУ «Информационные технологии. – Руководство по управлению безопасностью информационных технологий».

В последние годы для априорных оценок угроз все чаще используются измерения **фактора риска**. В общем виде эта величина определяется следующим образом:

$$F = P \cdot R_Q, \qquad (3)$$

где F – фактор риска; P – вероятность появления «нежелательного» события (угрозы); R_Q – ожидаемый ущерб от этой угрозы.

На основе (3) были предложения оценивать ожидаемый ущерб по так называемым нижним и верхним взвешенным значениям. При этом предполагается, что известны вероятности появления угроз, а также минимальное и максимальное значения ущерба при их появлении.

Попытка аналитического решения задачи оценки угроз приведена в [6]. Идея метода заключается в следующем. Пусть λ – средний показатель появления анализируемого типа угроз, причем он рассматривается как случайная переменная $\overline{\lambda}$ с распределением вероятностей $f(\lambda)$. Данный показатель определяется на основе фактов, имевших место в процессе функционирования данного объекта, или ему подобных. Если таких данных нет, то показатели появления угроз могут быть определены экспертным путем. Если r – число проявлений угроз в течение года, то случайной величине $\overline{r}$ будет соответствовать распределение вероятностей $f(r/\lambda)$. Если число проявлений угрозы зависит только от продолжительности периода измерений и среднего коэффициента проявления, то справедливым будет распределение Пуассона. Имея набор значений $r_1, r_2, \ldots, r_n$ значения λ могут быть определены на основе формулы гамма-распределения.

Получение полных оценок сопряжено с проведением сложных выкладок ввиду недостаточной определенности самого понятия ущерба. Тем не менее, это позволяет на стадии проектирования системы получить ориентировочные оценки защищенности системы от ожидаемых классов угроз.

Апостериорные оценки последствий используется при классификации опасных состояний объектов по совокупности конкретных признаков, оговоренных в ведомственных нормативных документах.

Так, при классификации происшествий на АЭС используется шкала МАГАТЭ, основанная на анализе влияния поврежденных подсистем на весь технологический цикл. Для классификации пожаров существует своя шкала, учитывающая объем возгорания и динамику его развития. Для оценки землетрясений – шкала Рихтера и т.д.

В технических приложениях для количественных описаний эффективности функционирования объекта используется соотношение между оценками критериев качества J его функционирования и затратами ресурсов на их достижение R_E в виде

$$E = J/R\ , \qquad (4)$$

где E – эффективность функционирования объекта; J – вектор критериев качества; R – вектор затрат ресурсов, необходимых для достижения J.

Такие оценки величины E позволяют множество возможных состояний объекта разграничить на три класса

– штатные – $E = F(J, \mathrm{R}) \rightarrow \max$;

– аварийные – $E(Q) = F(J, R) \rightarrow \min$;

– катастрофические – $E(Q) = F(J, R) \rightarrow 0$.

Реальные объекты обладают конечным множеством частных критериев качества $\{J\}$ и конечным множеством ресурсов $\{R\}$. Поэтому любое событие $u_i \in \{U\}$ является угрозой либо для конкретного качества $J_M \in \{J\}$, либо для конкретного ресурса $R_N \in \{R\}$.

Можно доказать, что угрозы компонентам вектора качества вызывают преимущественно обратимые изменения в состояниях объекта (аварии). Соответственно угрозы ресурсам приводят к необратимым изменениям характеристик объекта (катастрофам).

С этих позиций идентификация угроз заключается в том, что из всего множества событий в среде требуется выделить два подмножества:

$$\{U^X, U^R\} \in \{U\}, \qquad (5)$$

где U^X – подмножество угроз, вызывающих обратимые изменения характеристик объекта Q; U^R – подмножество угроз, вызывающих необратимые изменения характеристик объекта Q.

Если известна модель объекта Q и траектории его переходов в запрещенные состояния, то, при надлежащем выборе критериев, обратная задача решается с точностью до классов запрещенных управлений, т.е. до подмножеств угроз U^X, U^R. В многоуровневом объекте для любого из его уровней средой являются все события нижележащего уровня. Поэтому, понижая уровень анализа объекта, на

нижнем из них подобным образом можно определить параметры атрибутов угроз как элементарных событий во внешней среде [7].

Сложности в этом случае связаны с тем, что существует естественный дрейф характеристик элементной базы объекта, в результате чего могут появляться новые «уязвимые места» и, соответственно, новые типы угроз.

Поэтому нынешние тенденции в работах данного направления заключаются в поисках методов идентификации принципов порождения потенциально уязвимых характеристик объекта в течение всего его жизненного цикла. Здесь может быть использован следующий подход.

Будем считать, что основной причиной появления «уязвимых мест» объекта является конфликт между параметрами его структурных и качественных характеристик или рассогласование их проектных параметров.

Содержательно характеристики структуры объекта относятся к законам формирования связей между его отдельными подсистемами, которые в итоге определяют их способность к совместному поддержанию нового качественного свойства. Поэтому структурные характеристики описываются терминами надежность, живучесть, ресурсопотребление и пр.

Качественные характеристики объекта отражают внешние проявления процесса его функционирования и описываются в терминах отклонения этого процесса от заданных целей в виде точности, быстродействия, безопасности и пр.

Нештатные режимы возникают в тех случаях, когда способы организации взаимодействия между подсистемами объекта становятся неадекватными проектным требованиям к параметрам его качественных характеристик. Для описания этих способов представим каждое текущее значение независимой переменной в виде ее соотношения с границами собственного диапазона вариаций и своим дополнением до границы этого же диапазона.

Такая нормировка позволяет перейти от описания структур конкретных объектов к анализу их инвариантов, отражающих общие принципы структурообразования систем независимо от природы их материальной основы [8].

Среди множества разновидностей таких инвариантов структур систем существует два экстремальных типа. Один из них характеризуется как структурная гармония и соответствует максимально достижимой согласованности структурообразующих связей подсистем между собой и с диапазонами вариаций параметров управлений. В этом случае обеспечивается достижение наивысших параметров качественных характеристик объекта при заданной элементной базе.

Другой предельный тип – структурная дисгармония – это предельно возможная несогласованность характеристик структурообразующих элементов, в результате чего все качественные характеристики объекта имеют минимальные показатели.

В системах естественного происхождения гармонические структуры определяющие, поскольку являются формой накопления их положительного эволюционного опыта. Дисгармонические структуры появляются как пробные направления эволюции биообъектов либо как результат их прижизненных повреждений.

В техногенных объектах выраженная дисгармоническая структура возникает при рассогласовании исходных связей подсистем в результате асинхронной деформации их характеристик, в частности, в связи с дрейфом характеристик элементной базы. Каждый из этих типов структур можно чисто формальными методами разграничить на последовательность классов в соответствии с внутренней шкалой их возможных трансформаций [9]. При таком подходе идентификация потенциальных угроз объекту сводится к определению параметров шкал эволюции его структуры в течение жизненного цикла

1. *Белов В.М., Выходцев В.Р, Грищенко В.И., Кабикин В.Е., Котова А.Б., Кифоренко С.И., Волков Ю.И., Пустовойт О.Г.* Методология конструирования системно-иерархического классификатора чрезвычайных ситуаций. – Киев, 1998. – 32 с. – (Препр. / НАН Украины, Междунар. науч.-уч. центр информ. технологий и систем; 98–1).
2. *Флейшман Б.С.* Основы системологии. – М.: Сов. радио, 1982. – 368 с.
3. *Арнольд В.И.* Теория катастроф. – М.: Наука, 1990. – 128 с.
4. CSC–STD – 001 – 83 «Trusted System Evaluation Criteria». National Computer Security Center, 1983. – 112 p.
5. ISO/IECTR 13335–1: 1996 (E) «Information technology–Guidelines for the management of it Security». – ISO/IEC, 1996. – Part 1. – 132 p.
6. Security Protection. – 1978. – 10, N 2. – P. 23–40.
7. *Галиуллин А.С.* Методы решения обратных задач динамики. – М.: Наука, 1986. – 224 с.
8. *Сороко Э.М.* Структурная гармония систем. – Минск: Наука и техника, 1984. – 263 с.
9. *Черноморец В.А.* Модель генезиса соразмерных отношений между частями биологического целого // Кибернетика и вычисл. техн. – Киев: Наук. думка, 1997. – Вып. 114. – С. 108–115.

Получено 26.12.2001