УДК 681.322

СИСТЕМА АНАЛИЗА И ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АСУ

А.М. БАКУРЕНКО

Военная академия Республики Беларусь
Минск, 220057, Беларусь

Поступила в редакцию 17 июля 2008

Предложена структура системы анализа и оценки информационной безопасности автоматизированных систем управления. Приведены формальные модели процесса информационного взаимодействия и оцениваемой системы в контексте информационной безопасности.

Ключевые слова: автоматизированная система управления, информационная безопасность, угрозы, модель, оценка.

Введение

Высочайшая степень информатизации, к которой стремится современное общество, ставит его безопасность в зависимость от защищенности информационных технологий, обеспечивающих благополучие и даже жизнь множества людей. Сегодня компьютерные системы и телекоммуникации во многом определяют надежность систем обороны и безопасности страны, обеспечивая хранение конфиденциальной информации, ее обработку, доставку и представление потребителям. Массовое применение компьютерных систем, позволившее решить задачу автоматизации процессов обработки постоянно нарастающих объемов информации, сделало эти процессы чрезвычайно уязвимыми по отношению к агрессивным информационным воздействиям и поставило перед потребителями современных технологий новую проблему — проблему информационной безопасности.

Современные системы управления — это сложные системы, включающие в свой состав большое количество подсистем, которые, в свою очередь, также являются сложными системами. Автоматизированные системы управления (АСУ) кроме главной функции (управление объектом или процессом) выполняют множество вспомогательных функций, используя для этого различные технические средства. Зачастую результат выполнения главной функции зависит от того, выполнены ли (или насколько качественно выполнены) дополнительные функции.

В таких условиях резко возрастают требования к устойчивости функционирования АСУ и безопасности обрабатываемой в них информации. Под информационной безопасностью (ИБ) понимается состояние защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуре [1]. Критичными для закрытых АСУ, АСУ специального назначения являются угрозы целостности, конфиденциальности, доступности.

Постановка задачи

В современных АСУ затраты на обеспечение информационной безопасности достигают затрат на создание и эксплуатацию самой системы и, по мнению экспертов, имеют устойчивую тенденцию к дальнейшему увеличению. Злоумышленные воздействия или информационные угрозы состоят в преднамеренном или случайном нарушении свойств конфиденциальности, целостности и доступности вычислительной системы. Под угрозой информационной безопасности АСУ понимаются воздействия (пути воздействия) на систему (на активы и ресурсы, связанные с АСУ), которые прямо или косвенно могут нанести ущерб ее безопасности. Принято выделять три типа угроз: нарушение конфиденциальности, целостности и доступности (отказ в обслуживании) обрабатываемой, хранящейся и передаваемой информации) [2, 3].

Угрозы могут возникать в результате как преднамеренных действий, так и случайно; существуют классификации угроз и уязвимостей. Связь между видом опасности (уязвимостью) и возможной угрозой состоит в месте, времени и типе атаки, реализующей угрозу [2]. Цель системы защиты — противодействие угрозам безопасности. "Безопасная АСУ" — это система, обладающая средствами защиты, успешно и эффективно противостоящая информационным угрозам [2–4]. Однако для построения экономически эффективной системы защиты необходимо решить задачу оптимального выбора набора средств реализации системы защиты от комплекса возможных угроз ИБ, удовлетворяющих заданным ограничениям (стоимость всей системы, общий уровень безопасности, скорость работы и т.п.). Необходимо разработать методики анализа и оценки ИБ АСУ с тем, чтобы было возможно получить количественную оценку уровня защищенности по рассматриваемому критерию и получить возможность сравнивать различные комплексы средств защиты. Кроме того, сегодня все реже говорят о средствах обеспечения гарантированной защиты, а чаще — о средствах, препятствующих атаке, замедляющих процесс ее реализации с целью увеличения времени на принятие ответных действий или действий по предотвращению угрозы безопасности.

Система анализа и оценки информационной безопасности

Отличительной особенностью АСУ специального назначения является то, что они функционируют постоянно. Поэтому, в случае нарушения ИБ, постоянно требуется анализировать состояние ИБ и принимать решения, направленные на недопущение или предотвращение реализации угроз. Для выполнения функций анализа и оценки ИБ АСУ должна быть разработана система анализа и оценки (САО) ИБ, которая, в свою очередь, может входить в состав системы защиты информации (СЗИ). Кроме того, в целях повышения объективности проводимого анализа (например, в тех случаях, когда СЗИ подверглась атакам или нарушено ее функционирование), такая система может функционировать отдельно, независимо от СЗИ. САО ИБ должна реализовывать методики анализа и оценки информационной безопасности.

Структурно в состав САО ИБ должны входить модули (рис. 1), реализующие функции:

– анализа угроз;

– анализа уязвимостей

– принятия решения об уровне ИБ;

– управления процессом анализа и оценки ИБ.

Под анализом угроз понимается всестороннее изучение возможных угроз ИБ и способов их реализации. Анализ уязвимостей — комплекс мероприятий по всестороннему изучению свойств АСУ, способных привести к нарушению ИБ.

Как правило, анализ угроз и уязвимостей проводится для конкретной АСУ с учетом ее применения, условий эксплуатации, с построением модели вероятного нарушителя, учитывающей стратегию поведения нарушителя, уточняющей характер угроз, источником которых он является [5]. Необходимость наличия этой модели обусловлена также тем, что закрытые АСУ, АСУ специального назначения, являясь режимными объектами, разрабатываются и эксплуатируются в условиях, отличных от тех, в которых разрабатываются и функционируют другие системы.

Рис. 1. Система анализа и оценки ИБ

Функция принятия решения об уровне ИБ предполагает наличие процесса, реализующего на основе методики оценки ИБ оценку общего уровня ИБ АСУ. Входными параметрами для данной методики будут являться результаты анализа угроз и уязвимостей.

Очевидно, что предложенная САО ИБ АСУ в процессе функционирования будет использовать вычислительные ресурсы всей системы. Поэтому к САО предъявляются требования, направленные на недопущение снижения общей производительности АСУ:

– применение преимущественно пассивных методов анализа (например, наблюдение за сетевыми интерфейсами вместо отправки запросов на получение информации об их состоянии);

– выбор оптимальной частоты выполняемых проверок;

– в случае выполнения в виде отдельной подсистемы, использование преимущественно собственных вычислительных ресурсов и др.

Модели анализа и оценки информационной безопасности

Разработка методик анализа и оценки ИБ представляется возможной только после построения модели АСУ в контексте ИБ. Рассмотренные в литературе по данной тематике модели не позволяют адекватно и полно описать информационные процессы, происходящие в АСУ. Кроме того, не существует единой модели, комплексно охватывающей три основных направления обеспечения безопасности, каждая из них описывает один из аспектов защиты: конфиденциальность, целостность или доступность.

Учитывая, что оценка каждого из указанных аспектов возможна по нескольким критериям, а также то, что столь сложную систему невозможно полно охарактеризовать с помощью единственного показателя, оценка ИБ в общем случае является задачей многокритериальной оценки.

Существуют два основных подхода к многокритериальной оценке эффективности сложных систем [6, 7]. Первый так или иначе связан со сведением множества частных показателей $\{W_i\}$ к единственному интегральному показателю W_o. Второй используется при наличии значительного числа частных показателей эффективности, приблизительно одинаково важных, и предполагает использование методов теории многокритериального выбора и принятия решений. Цель функционирования СЗИ — поддержание заданного уровня защищенности. Поэтому показатели эффективности должны характеризовать динамические свойства СЗИ и позволять оценивать ее как характеристики адаптивной системы.

Для получения таких показателей на основе анализа существующих формальных моделей безопасности [3, 6–8] и стандартов информационной безопасности должна быть разработана адекватная модель АСУ с имеющейся в ее составе СЗИ (в контексте информационной безопасности), устраняющая выявленные недостатки в исследованных моделях и стандартах. Первостепенной задачей создания подобной модели является адекватное формальное описание информационных процессов, происходящих в АСУ специального назначения. Преимуществом формального описания является отсутствие противоречий в политике безопасности и возможность теоретического доказательства безопасности системы при соблюдении всех условий политики безопасности.

Данную модель можно разработать на основе адаптации субъектно-объектной модели, предложенной А.А. Грушо [2]. В данных исследованиях вводится понятийный аппарат рассмотрения вычислительной системы в виде субъектов и объектов, взаимодействующих посредством операций; разрешение взаимодействия определяется доступом, при взаимодействии образуется информационный поток. Субъектно-объектная модель описывает состояния системы, позволяет разделять безопасное состояние от небезопасного, сформулировать положения, при выполнении которых система останется в безопасном состоянии при осуществлении любых переходов. Использование субъектно-объектной модели разрешает формализовать описание политики безопасности и построить защищенную систему.

В общем случае процесс информационного взаимодействия представляется следующим образом: U — множество участников информационного процесса, осуществляющих доступ к информации, ее обработку и обменивающихся информацией; I — множество информационных объектов, хранящих информацию.

С точки зрения безопасности информационные процессы моделируются с помощью отношений информационных потоков, определенных на этих базовых множествах. Под информационным потоком понимается событие, приведшее к появлению в точке назначения потока информации, находящейся перед этим событием в точке исхождения потока. Существуют два вида потоков:

$\text{Stream}^W \subseteq U \times I$ — отношение, описывающее потоки от пользователей к объектам;

$\text{Stream}^R \subseteq I \times U$ — отношение, описывающее потоки от объектов к пользователям.

В результате проведенных исследований были выявлены сущности и операции:

1. Для каждой информации существует по крайней мере один пользователь, являющийся ее достоверным источником:

TrustSrc: $I \rightarrow U$.

2. Для каждого пользователя известен набор информации, для которой он является уполномоченным потребителем:

Autority: $U \rightarrow$I

В каждый момент времени информационное взаимодействие характеризуется следующими отношениями между пользователями и информацией:

1. Know $\subseteq U \times I$ — отношение известности, которое определяет, какой пользователь какую информацию знает;

2. Create $\subseteq U \times I$ — отношение порождения, которое определяет, какой пользователь какую информацию предоставляет.

Конфиденциальность обеспечивается тогда, когда отношение известности не противоречит функции авторизации Know$\subseteq$Autority, а целостность — когда отношение порождения не противоречит функции доверенного источника Create$\subseteq$TrustSrc.

Полученная субъектно-объектная модель описания состояний системы, отражающая схему информационных потоков и правила управления ими, после своего развития может быть положена в основу модели анализа информационной безопасности, отражающую заданный порядок обработки информации и формальное доказательство ее безопасности. Формальные модели широко используются при построении систем защиты, так как с их помощью можно доказать безопасность системы, опираясь при этом на объективные доказуемые математические постулаты. Целью построения модели является получение формального доказательства безопасности системы при соблюдении определенных условий, а также определения достаточного критерия безопасности.

Формальные модели позволяют обосновать практическую пригодность системы, определяют ее базовую архитектуру и используемые технологические решения при ее построении. При функционировании АСУ в ней происходит взаимодействие между ее компонентами, порождаются информационные потоки. Основная цель создания политики безопасности и описания ее в виде формальной модели — это определение условий, которым должно подчиняться поведение системы. Формальный подход заключается в описании свойств компонент АСУ и потоков в ней, а также СЗИ. Свойство безопасности трактуется не как количественное, а как качественное состояние системы.

Система считается безопасной в соответствии с моделью, если [3]:

– ее исходное состояние удовлетворяет критериям безопасности модели;

– системный механизм контроля доступа реализует правила контроля доступа модели;

– все состояния модели, достижимые из исходного, соответствуют критериям безопасности.

Вычисление множества достижимых состояний и оценка их соответствия критериям безопасности называется разрешением проблемы безопасности [3]. Там же показано, что разрешение проблемы безопасности может быть реализовано для каждой конкретной системы, находящейся в заданном состоянии. Поскольку абсолютное большинство систем реализуют дискреционные модели, разрешение проблемы безопасности является актуальной задачей для процесса оценки безопасности.

Проблема безопасности может быть формализована следующим образом:

Система Σ в общем виде представляет собой машину состояний: $\Sigma = S^{\Sigma}, T, S_0^{\Sigma}, Q$, где S^{Σ} — множество состояний системы; Q — множество запросов, обрабатываемых системой; T — функция перехода из состояния в состояние, $T : Q \times S^{\Sigma} \to S^{\Sigma}$. Функция T в ответ на запрос q переводит систему из состояния S_1^{Σ} в следующее $S_{i+1}^{\Sigma} = T\ q, S^{\Sigma}$; S_0^{Σ} — начальное состояние системы.

Состояние S^{Σ} достижимо в системе $\Sigma = S^{\Sigma}, T, S_0^{\Sigma}, Q$ тогда и только тогда, когда существует последовательность $< q_0, S_0^{\Sigma}\ , ..., \ q_0, S_n^{\Sigma} >$, в которой $S_0^{\Sigma} = S^{\Sigma}$, а $S_{i+1}^{\Sigma} = T\ \ q, S_i^{\Sigma}\ \ , 0 \le i < n.$

Модель безопасности M — это кортеж множеств $M=\{S, R, C\}$, где S — множество состояний для данной модели; R — множество состояний для данной системы, сформулированных в форме логических предикатов вида $r(s_1, s_2)$, определяющих допустимость перехода из состояния s_1 в состояние s_2; C — множество критериев безопасности, сформулированных в виде $c(s)$, определяющих безопасность состояния s с точки зрения модели.

Состояние $s \in S$ является безопасным тогда и только тогда, когда для него истинны все критерии $c(s) \in C$, т.е. $\forall c \in C : c(s) =$"истина".

Для оценки безопасности всех достижимых состояний для данной системы $\sum$ в состоянии S_0^{Σ} необходимо:

оценить заданное состояние системы на соответствие критериям безопасности;

доказать, что механизм контроля доступа, реализованный в системе, соответствует правилам контроля доступа;

вычислить множество состояний, достижимых из заданного, и оценить их безопасность.

Развитие данного подхода возможно с применением теории графов для получения аналитических выражений метрик ИБ. Построенная на основе этой теории модель реализации угроз ИБ представляет собой направленный граф (рис. 2). Вершины графа — состояния системы, соответствующие попытке реализации злоумышленником некоторой угрозы информации.

Состояние системы S_0 является начальным, т. е. таким, при котором еще ни одна из угроз информации не реализована и выполняются критерии $c(s) \in C$. Состояние S_j соответствует

попытке реализации *j*-й угрозы. В случае ее успешной реализации осуществляется переход к следующему состоянию системы, в противном случае (при штатном реагировании СЗИ, службы безопасности системы) осуществляется переход к состоянию S_{f+1}, где $f=1, 2, \ldots, F$ — номера целей, преследуемых злоумышленником. Состояние S_f является конечным и соответствует достижению злоумышленником *f*-й цели. Дуги графа соответствуют направлениям переходов между состояниями. Каждая дуга характеризуется значением вероятности перехода между соответствующими состояниями системы. Пунктиром обозначены дуги, соответствующие переходу из данного состояния в состояние S_{f+1}.

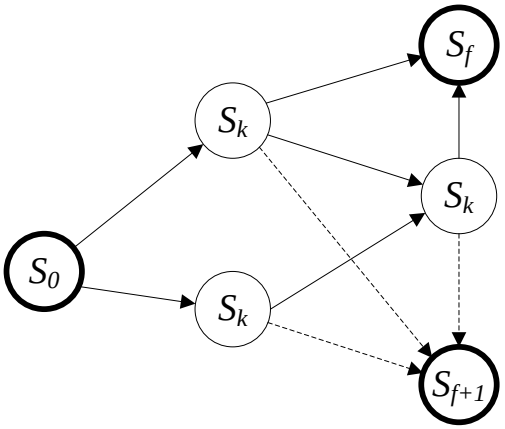

Рис. 2. Реализации угроз ИБ

При этом вероятность реализации нарушителем *f*-й цели будет определяться выражением:

$$P_f = \sum_{k=1}^{f-1} p_k p_{kf}$$

На основе составленных таким образом графов для каждого из аспектов ИБ формируются частные показатели. При этом к ним предъявляются требования [6]: соответствия характеризуемому качеству системы, полноты, измеримости, ясности физического смысла, неизбыточности, чувствительности.

Частные показатели могут быть сведены в комплексные, характеризующие, соответственно, целостность, конфиденциальность или доступность, а также в один обобщенный показатель ИБ. Однако введение обобщенного показателя является весьма сложной и не всегда нужной задачей.

Заключение

Предложенные модели являются основой для разработки методик анализа и оценки информационной безопасности АСУ. Необходимо также учесть, что уровень информационной безопасности, обеспечиваемый системой защиты, определяется наиболее слабым ее звеном. Использование методик анализа и оценки ИБ должно позволять осуществить комплексный подход к выбору средств защиты и получению сбалансированного набора защитных средств, что при тех же затратах позволяет достичь более высокого уровня защищенности с точки зрения системы защиты в целом.

ANALYSIS AND ESTIMATION SYSTEM INFORMATION SAFETY OF THE MANAGEMENT INFORMATION SYSTEM

A.M. BAKURENKO

Abstract

The structure of system of the analysis and an estimation of information safety of the automated control systems is offered. Formal models of process of information interaction and estimated system in a context of information safety are resulted.

Литература

1. *Ярочкин В.И.* Информационная безопасность. Учебное пособие для студентов непрофильных вузов. М., 2000.
2. *Грушо А.А., Тимонина Е.Е.* Теоретические основы защиты информации. М., 1996.
3. *Зегжда Д.П., Ивашко А.М.* Основы безопасности информационных систем. М., 2000.
4. *Мельников В.В.* Безопасность информации в автоматизированных системах. М., 2003.
5. Критерии оценки безопасности компьютерных систем МО США ("Оранжевая книга") TCSTC [Departament of Defense Trusted Computer System Evaluation Criteria. DoD 5200.28-STD. 19831].
6. *Анфилатов В.С., Емельянов А.А., Кукушкин А.А.* / Под ред. А.А. Емельянова. Системный анализ в управлении: Учеб. пособие М., 2002.
7. *Домарев В.В.* Безопасность информационных технологий. Методология создания систем защиты. Киев, 2002.
8. *Анищенко В.В., Криштофик Л.М.* // Наука и военная безопасность. 2005. № 1. С. 30–34.