

АЛГОРИТМ КОМПЛЕКСНОЙ ОЦЕНКИ УГРОЗ НСД К ИНФОРМАЦИИ ПРИ ПРОЕКТИРОВАНИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ КРИТИЧЕСКОГО ПРИМЕНЕНИЯ

Р.А. Залогин

Разработан алгоритм комплексной оценки угроз несанкционированного доступа к информации при проектировании автоматизированных систем критического применения (АСК). Предложенный алгоритм оценки угроз несанкционированного доступа к информации позволяет точно оценить уязвимости проектируемой автоматизированной системы критического применения с точки зрения информационной безопасности

Ключевые слова: информационная безопасность, алгоритм, автоматизированная система

С точки зрения системного анализа АСК представляет собой сложную организационно-техническую систему, характеризующуюся большим количеством параметров. Анализ функций, принципов построения различных АСК позволяет построить структурную и функциональную модель типовой АСК. Процесс проектирования таких АСК характеризуется большим количеством этапов, включает в себя целый ряд процедур, характерных как для процесса проектирования в целом, так и решающих специфические задачи исследования отдельных систем АСК с целью обеспечения максимально возможного уровня защиты информации, обрабатываемой данной АСК.

Процесс алгоритмизации комплексной оценки угроз НСД к информации в АСК заключается в объединении алгоритмов оценки частных угроз НСД к информации, а также сведению частных показателей угроз в один общий комплексный показатель.

На рис. 1. представлен алгоритм комплексной оценки угроз НСД к информации в АСК и включает следующие блоки.

Блок 1. Ввод вероятностей распределения между угрозами НСД в АСК, полученных из статистики угроз аналогичных систем, либо с учетом имеющейся статистики, накопленной при функционировании данной системы, переход в блок 2.

Блок 2. Аналогично блоку 1, производится ввод вероятностей распределения атак при реализации конкретного вида угрозы, осуществляется переход в блок 3.

Блок 3. Ввод вероятностей, определяемых исходя из функционирующих в АСК служб, протоколов, технологий передачи данных, переход в блок 4.

Блок 4. Блок организации циклов с указанием количества испытаний, или проходов цепи, описывающей процесс реализации угроз НСД в АСК. Количество проходов цепи выбирается исходя из требуемой погрешности результатов, и

определяется при организации вычислительного эксперимента, переход в блок 5.

Блок 5. Определение вида угрозы производится с помощью генератора случайных чисел в соответствии с вероятностями, введенными в блоке 1, осуществляются переходы в блок 6-8.

Блок 6. Генерация угрозы нарушения конфиденциальности без конкретизации вида атаки, либо иного воздействия на систему или информацию, переход в блок 9.

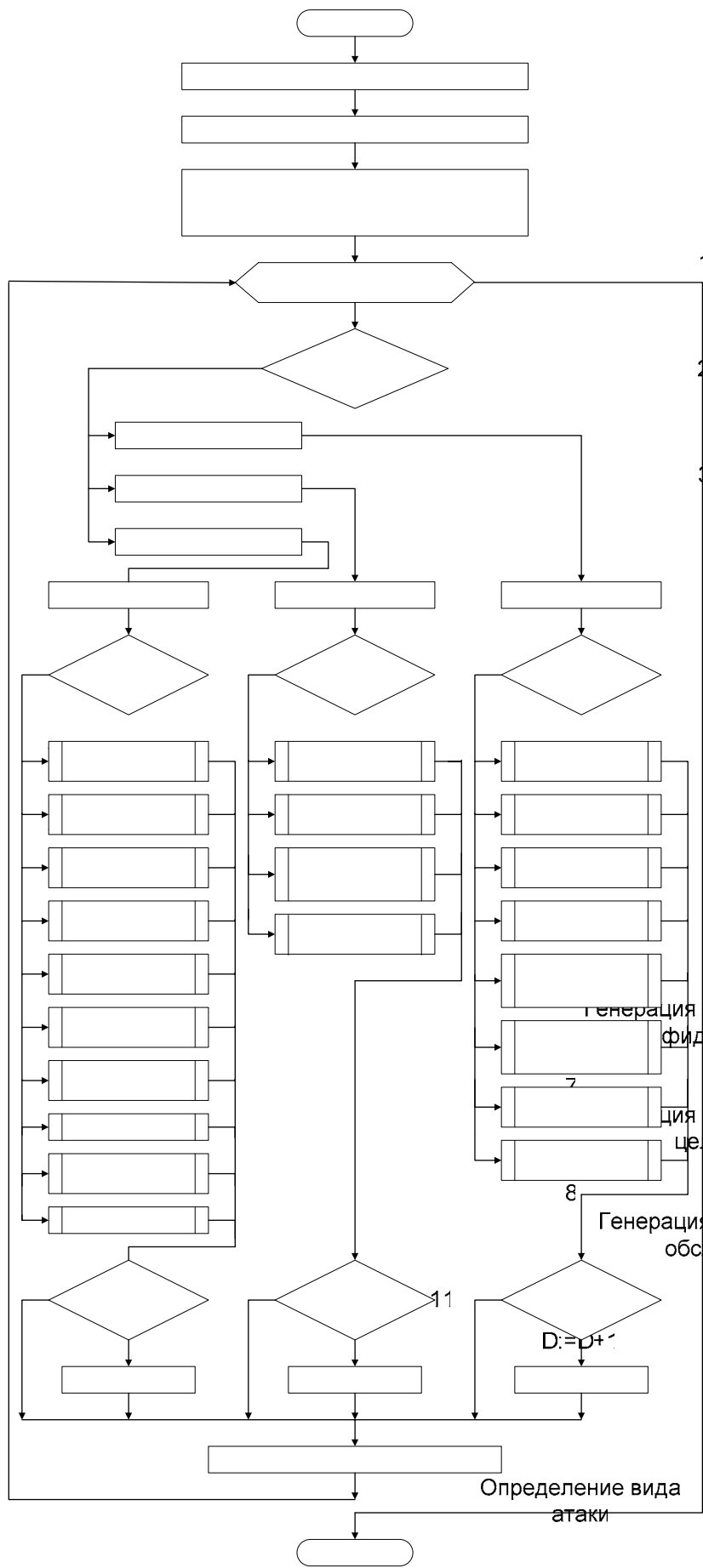
Блок 7. Генерация угрозы нарушения целостности без конкретизации вида атаки, либо иного воздействия на систему или информацию, переход в блок 10.

Блок 8. Генерация угрозы отказа в обслуживании без конкретизации вида атаки, либо иного воздействия на систему или информацию, переход в блок 11.

Блок 9-11. Учет сгенерированных угроз с учетом их вида, осуществляется увеличением переменной на 1: $D:=D+1$, $C:=C+1$, $K:=K+1$, где D – количество сгенерированных угроз отказа в обслуживании, C – количество сгенерированных угроз нарушения целостности, K – количество сгенерированных угроз нарушения конфиденциальности, далее осуществляется переход в блоки 12-14.

Блок 12-14. Определение вида атаки в соответствии с вероятностями, введенными в блоке 2. Вид атаки определяется исходя из того, какая угроза была сгенерирована и определяется графом переходов. Далее производится переход в блоки 15-22 для произведения моделирования атак, свойственных реализации угрозе нарушения конфиденциальности, в блоки 23-26 для моделирования атак угрозы нарушения целостности, в блоки 27-36 для моделирования атак угрозы отказа в обслуживании.

Блок 15-18, 23-24. Моделирование атак подменой адреса канального, сетевого уровня, подменной адреса на протокол ARP, подменой доменного имени. Далее с учетом сгенерированной угрозы производится переход в блоки 37-39.



Алгоритм расчета комплексной оценки угроз НСД.

27
 28
 Моделирование атаки
 исполнением SQL-
 сценариев

На

Ввод вероятност

Ввод вероятностей $P_{2.5} - P_{2.12}$

Определение перечня плани
 служб и определение вероят
 $P_{29.30} P_{29.31} P_{32.33} P_{32.34} P_{41.42}$
 $P_{54.55} P_{54.56} P_{57.58} P_{57.59} P_{60.61}$

4

i:=

5

Определ
 угр

Генерация угрозы нарушения
 конфиденциальности

Генерация угрозы нарушения
 целостности

Генерация угрозы отказа в
 обслуживании

10

C:=

13

Определ
 ат

23

Моделиров
 подмной
 протоко

24

Моделир

Блок 19. Моделирование атаки навязыванием ложного маршрута. Далее производится переход в блок 37.

Блок 20-21, 25. Моделирование атаки методом подбора пароля к учетным записям, криптографическим анализом на защищаемую информацию. Далее производится переход в блок 37, 38.

Блок 22, 26-27. Моделирование атак удаленным исполнением SQL-сценариев. Далее с учетом сгенерированной угрозы производится переход в блоки 37-39.

Блок 28-32, 34-35. Моделирование атак методом генерации ложных TCP-пакетов, генерация ложных UDP-пакетов, генерации ложных ICMP-ответов, создания ложных DHCP-клиентов, сброса TCP-соединения, способом Ping of Death, принуждением к ускоренной передачи данных. Далее с учетом сгенерированной угрозы производится переход в блок 39.

Блок 33. Моделирование атаки методом навязывания длинной сетевой маски. Далее производится переход в блок 39.

Блок 36. Моделирование случайных отказов. Далее производится переход в блок 39.

Блок 37-39. Определение реализации атаки на информацию, обрабатываемую в АСК. Если атака заканчивается удачей, то соответственно и угроза считается реализованной, осуществляется переход в блоки 40-42.

Блок 40-42. Учет реализованных атак, угроз с учетом их вида, осуществляется увеличением переменной на 1: $N_d := N_d + 1$; $N_c := N_c + 1$; $N_k := N_k + 1$; $K := K + 1$, где K – общее число реализованных атак или воздействий (случаев реализации угрозы), N_d – количество реализованных угроз отказа в обслуживании, N_c – количество реализованных угроз нарушения целостности, N_k – количество реализованных угроз нарушения конфиденциальности, далее осуществляется переход в блок 43.

Блок 43. Расчет комплексного показателя реализации угроз НСД в соответствии с расчетными соотношениями: $P_{c(нсд)} = K/N$; $P_{c(конф)} = N_k/K$; $P_{c(ц)} = N_c/C$; $P_{c(отк)} = N_d/D$, где $P_{c(нсд)}$ – комплексный

показатель реализации угроз НСД к информации в АСК, $P_{c(конф)}$, $P_{c(ц)}$, $P_{c(отк)}$ – показатели реализации угроз нарушения конфиденциальности, целостности, отказа в обслуживании, N – общее количество проходов цепи при проведении испытаний, K – общее количество реализованных угроз НСД, N_k , N_c , N_d – количество реализованных угроз нарушения конфиденциальности, целостности, отказа в обслуживании соответственно.

Таким образом, в результате проведения исследований были получены следующие результаты:

1. Разработан алгоритм произведения условных переходов в графе переходов при произведении имитационного моделирования процесса функционирования АСК с целью расчета комплексного показателя угроз НСД к информации.

2. Разработан алгоритм комплексной оценки угроз НСД к информации при АСК, обеспечивающий расчет комплексного показателя оценки угроз НСД.

3. Разработаны алгоритмы расчета частных показателей угроз НСД к информации при проектировании АСК, что позволяет производить проектирование оптимальной телекоммуникационной и информационной подсистемы, а также производить подбор наиболее оптимальных СЗИ для проектируемой АСК с целью обеспечения максимального уровня защищенности обрабатываемой в них информации.

Литература

1. К вопросу о количественной оценке угроз несанкционированного доступа к информации в автоматизированных системах критических применений / О.Е. Работкина, Р.А. Залогин // Вестник ВГТУ, Том 4, №5, 2008.

2. Классификация угроз НСД в автоматизированных системах управления критического применения / Рогозин Е.А., Махинов Д.В., Залогин Р.А., Ланкин О.В., Багаев М.А. // Проблемы обеспечения надежности и качества приборов, устройств и систем: Межвуз. сб. науч. тр. Воронеж: ВГТУ, 2006.

Воронежский государственный технический университет

ALGORITHM FOR ESTIMATION INFORMATION SECURITY THREATS WHEN DESIGNING CRITICAL APPLICATION AUTOMATED SYSTEMS

R.A. Zalogin

The column describes algorithm for estimation information security threats when designing critical application automated systems

Key words: information security, algorithm, automated systems