ПОДХОДЫ К КОЛИЧЕСТВЕННОЙ ОЦЕНКЕ ЗАЩИЩЕННОСТИ РЕСУРСОВ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

***Казарин Олег Викторович**, доктор технических наук, старший научный сотрудник, г. Москва*
***Кондаков Сергей Евгеньевич**, г. Москва*
***Троицкий Игорь Иванович**, кандидат технических наук, доцент, г. Москва*

В работе проанализированы традиционные качественные показатели защищенности ресурсов автоматизированных систем. Обосновано, что для оценки защищенности информационных и программных ресурсов автоматизированных систем необходимо применять количественные показатели. Предложен подход перехода от качественных показателей защищенности к количественным показателям. Обоснован математический аппарат, основный на теории надежности и теории массового обслуживания. Предложены расчетные выражения для оценки количественных показателей защищенности информации в автоматизированных системах.

***Ключевые слова**: защищенность автоматизированных систем, показатели защищенности, руководящие документы, защита информации*

APPROACHES TO MEASURING OF INFORMATION SECURITY RESOURCES OF AUTOMATED SYSTEMS

***Oleg Kasarin**, Doctor of Science (Comp), Associate Professor, Moscow*
***Sergey Kondakov**, Moscow*
***Igor Ttoitskii**, Ph.D., Associate Professor, Moscow*

Abstract. This paper analyzes the traditional qualitative indicators of security resources automated systems. It is proved that for the evaluation of security of information and software resources necessary to apply the system quantitative indicators. The approach for transition from qualitative to quantitative indicators is offered. The mathematical apparatus by use the reliability theory and queuing theory are justified. The settlement expressions for evaluating quantitative data protection in automated systems are proposed.

***Keywords**: automated systems security, information security indicators, guidance documents, information security*

Введение

В настоящее время для оценки защищенности автоматизированных систем в соответствии с действующими нормативными правовыми актами применяется система качественных показателей [1,2]. Данная оценка учитывает особенности автоматизированных систем, группы и классы защищенности информации от несанкционированного доступа (НСД) в этих системах, перечень требований по обязательному использованию рекомендуемых средств (механизмов) защиты информации или объектов, содержащих информационный ресурс, а также объектов, через которые нарушитель может получить доступ к информации.

Для количественной оценки защищенности информационных и программных ресурсов АС

необходимо применять количественные показатели, использование которых обеспечивает более объективную оценку.

Выбор количественных показателей защищенности

Решение этой задачи предполагает разработку подхода для определения количественного показателя уровня защищенности информационных и программных ресурсов АС, перевод (трансформация) в количественные значения качественного показателя заданного уровня защищенности и проведение оценки адекватности полученных результатов. Для получения количественной оценки показателя защищенности информационных и программных ресурсов АС могут быть использованы аппарат теории вероятности, теории массового обслуживания и теории надежности, позволяющие с достаточной точностью описывать (моделировать) процессы, протекающие в защищенной информационной системе [1].

Защищенность информационных и программных ресурсов АС складывается из обеспечения её основных свойств: целостности, доступности и конфиденциальности. Если количественно задать требования к ним, то уровень защищенности можно рассматривать как агрегированный (интегральный) показатель

$$P_{защ} = F(P_{цел}, P_{дос}, P_{кнф}), \quad (1)$$

где: $P_{цел}$ - вероятность обеспечения целостности информации, хранимой и обрабатываемой в АС;

$P_{дос}$ - вероятность обеспечения доступности информации, хранимой и обрабатываемой в АС;

$P_{кнф}$ - вероятность сохранения конфиденциальности информации.

Выражения для показателей автоматизированных систем

Анализ ряда работ [1-8], содержащих количественный расчет показал, что более проработанными, на наш взгляд, являются рекомендации ГОСТ 51987. Приведенные в нем выражения имеют четкий физический смысл, достаточно просты и вычисляемы [2, с.85]. Поэтому при определении некоторых показателей защищенности будут использоваться положения ГОСТ 51987 или их модификации.

Для оценки вероятности обеспечения целостности информационных и программных ресурсов АС используем модель на основе профилактической диагностики целостности системы.

Будем считать: целостность информационных и программных ресурсов АС не нарушена, если к началу периода и в течение всего периода $T_{зад}$ источники угроз либо не проникают в систему, либо не происходит их активизации (инициирующего события).

Моделируемая технология защиты основана на профилактической диагностике целостности информационных и программных ресурсов АС. Диагностика осуществляется периодически. Предполагается, что существуют не только средства диагностики, но и способы восстановления необходимой целостности информационных и программных ресурсов при выявлении проникших вредоносных источников или следов их негативного воздействия. Выявление нарушений целостности возможно лишь в результате диагностики. Достижение требуемой целостности информационных и программных ресурсов АС является следствием достаточно частого диагностирования АС при ограничениях на допустимое ухудшение показателей ВВХ. Результатом применения очередной диагностики является полное восстановление нарушенной целостности информационных и программных ресурсов АС и подтверждение целостности при отсутствии ее нарушения. При очередной диагностике все проникшие, но не активизировавшиеся источники опасности формально считают нейтрализованными.

Существование средств гарантированного выявления источников опасности или следов их воздействия и существование способов восстановления нарушений целостности информационных и программных ресурсов АС являются необходимыми условиями обеспечения безопасности её функционирования.

Для описания процессов защиты АС введем обозначения:

λ - интенсивность воздействия на АС, осуществляемой с целью внедрения источника опасности;

β - среднее время активизации проникшего в АС источника опасности;

$T_{диаг}$ - период диагностики целостности информационных и программных ресурсов АС;

$T_{зад}$ - задаваемый период непрерывного безопасного функционирования АС.

Возможны два варианта:

вариант 1 - заданный период безопасного функционирования $T_{зад}$ меньше периода диагностик ($T_{зад} < T_{диаг}$);

вариант 2 - заданный период безопасного функционирования больше или равен периоду диагностик ($T_{зад} \geq T_{диаг}$), т.е. за это время заведомо произойдет одна или более диагностик.

Для варианта 1 вероятность $P_{цел(1)} = F(\lambda, \beta, T_{диаг}, T_{зад})$ отсутствия опасного воздействия в течение периода $T_{зад}$ при экспоненциальной аппроксимации временных характеристик проникновения и активизации источников опасности и независимости исходных характеристик вычисляют по формуле:

$$P_{цел\,(1)} = \begin{cases} (\lambda - \beta^{-1})^{-1} \{\lambda\, e^{-Tзад/\beta} - \beta^{-1}\, e^{-\lambda\, Tзад}\}, \text{ если } \lambda \neq \beta^{-1}, \\ e^{-\lambda\, Tзад}[1+\lambda\, Tзад], \text{ если } \delta = \beta^{-1} \end{cases} \quad (2)$$

Эту формулу используют для оценки вероятности отсутствия опасных воздействий без какой-либо диагностики в предположении, что к началу $T_{зад}$ целостность информационных и программных ресурсов АС обеспечена.

Для варианта 2 при условии независимости исходных характеристик и периодов между диагностиками вероятность отсутствия опасного воздействия в течение периода $T_{зад}$ при экспоненциальной аппроксимации временных характеристик проникновения и активизации источников опасности и независимости исходных характеристик вычисляют по формуле:

$$P_{цел(2)} = P_{ов\,t} + P_{ов\,k}, \quad (3)$$

где $P_{ов\,t}$ - вероятность отсутствия опасного воздействия в течение всех периодов между диагностиками, целиком вошедшими в $T_{зад}$. С учётом доли этих периодов $N\, T_{диаг}/T_{зад}$ в общем заданном периоде $T_{зад}$, расчёт осуществляют по формуле:

$$P_{ов\,t} = (N\, T_{диаг})\, /T_{зад}\, [P^{N}_{ов\,(1)}\, (\lambda, \beta, T_{диаг})], \quad (4)$$

где N -число периодов между диагностиками, которые целиком вошли в пределы времени $T_{зад}$, с округлением до целого числа, $N = T_{диаг}/T_{зад}$ - целая часть;

$P^{N}_{ов(1)} = \mathrm{F}\,(\lambda, \beta, T_{диаг})$ - вероятность того, что источники опасности не будут воздействовать за один период между диагностиками, целиком вошедший в пределы времени, вычисляют по формуле (2);

$P_{ов\,к}$ - вероятность отсутствия опасного воздействия после последней диагностики (в конце $T_{зад}$). С учётом доли остатка $T_{ост} = T_{зад} - N\, T_{диаг}$ в общем заданном периоде $T_{зад}$ и независимости исходных характеристик расчёт осуществляется по формуле:

$$P_{ов\,к} = (T_{ост} / T_{зад})\, P_{ов\,(1)}\, (\lambda, \beta, T_{диаг}).$$

Значение $P_{ов(1)} = \mathrm{F}\,(\lambda, \beta, T_{диаг}, T_{зад})$ вычисляют по формуле (3).

Таким образом, вероятность отсутствия опасного воздействия $P_{ов}$ в течение заданного периода функционирования системы $T_{зад}$ определяется аналитическими выражениями (2) и (3) в зависимости от варианта соотношений между исходными данными.

Необходимые для моделирования пределы исходных значений $T_{зад}$, λ, β задаются в ТЗ на АС или в постановках функциональных задач при указании сценариев возможного опасного воздействия, а значение $T_{диаг}$ указывают в эксплуатационной документации.

Вероятность сохранения конфиденциальности информации вычисляют по формуле:

$$P_{кнф} = 1 - \prod_{m=1}^{k} P_{пр\,кнф\,m},$$

где k – количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к информации;

$P_{пр\ кнф\ m}$ – вероятность преодоления нарушителем m-ой преграды до истечения периода объективной конфиденциальности информации $T_{кнф}$.

Для экспоненциальной аппроксимации распределений исходных характеристик при их независимости $P_{пр\ кнф\ m}$ равна:

$$P_{пр\,кнф\,m} = \frac{T_{кнф} f_m}{T_{кнф} f_m + u_m f_m + u_m T_{кнф}},$$

где f_m – среднее время между соседними изменениями параметров защиты m-ой преграды;

u_m – среднее время преодоления (вскрытия значений параметров защиты) m-ой преграды.

$T_{кнф}$ – средняя длительность периода объективной конфиденциальности информации.

Необходимые для моделирования исходные количество преград k и пределы значений u_m определяют в результате дополнительного моделирования, натурных экспериментов, учитывающих специфику системы защиты и возможные сценарии действий нарушителей или сравнения с аналогами. Диапазон возможных значений $T_{кнф}$ задают в ТЗ.

Вероятность обеспечения доступности информации, хранимой и обрабатываемой в АС - $P_{дос}$, это свойство системы при санкционированном запросе в любой момент времени выдать потребителю информацию, т.е. её готовность системы, надежность [3]. На наш взгляд, наиболее системным показателем надежности является коэффициент готовности.

Общее выражение для определения коэффициента готовности, а следовательно и $P_{дос}$, имеет вид:

$$P_{дос} = T_0/(T_0 + t_в), \quad (7)$$

где T_0 – время наработки на отказ системы;

$t_в$ – время восстановления системы после отказа.

Для оценки времени наработки на отказ системы составляется укрупненная структурная схема надежности (ССН).

Коэффициент готовности $P_{дос}$ в период времени τ, определяется как:

$$P_{дос} = \frac{\tau}{\tau - t_в \ln P_{бр}(\tau)}, \quad (8)$$

где: τ – период времени, за который определяется $K_г$ (задается);

$t_в$ – время восстановления (задается);

$P_{бр}(\tau)$ – вероятность безотказной работы АС за время τ (вычисляется).

Таким образом, определены основные составляющие выражения (1), поэтому финальное выражение для количественной оценки уровня защищенности АС, с учетом подходов, представленных в [4, 5], имеет вид:

$$P_{защ} = P_{цел} b_{цел} + P_{дос} b_{дос} + P_{кнф} b_{кнф},$$

где $b_{цел}$, $b_{дос}$, $b_{кнф}$ - весовые коэффициенты свойств защищенности информации, при условии $b_{цел} + b_{дос} + b_{кнф} = 1; b_{цел} = b_{дос} = b_{кнф}$.

Выводы

В рамках данной статьи представлен подход к количественной оценке уровня защищенности, все представленные выражения достаточно просты и вычисляемы. Адекватность полученных количественных оценок защищенности АС легко определяется на базе аппарата теории вероятности, теории массового обслуживания и теории надежности.

Данный подход может использоваться для формирования показателей безопасности комплексов средств автоматизации [] и может быть рекомендован для формирования требований к критическим системам [].

Литература:

1. Жуков И.Ю., Зубарев И.В., Костогрызов А.И. и др. Методическое руководство по оценке качества функционирования информационных систем. М.: Изд-во 3 ЦНИИ МО РФ, 2003. 352 с.
2. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. М.: Радио и связь, 2012. 192 с.
3. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ДиаСофт, 2002. 688 с.
4. Мельников В.В. Защита информации в компьютерных системах. - М.: Финансы и статистика, 1997. 368 с.
5. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. М.: Наука и техника, 2004. 384 с.
6. Акулов О.А., Баданин Д.Н., Жук Е.И., Медведев Н.В., Квасов П.М., Троицкий И.И. Основы информационной безопасности: Учеб. пособие. М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. 161 с.
7. Математические основы информационной безопасности / Басараб М. А., Булатов В. В., Булдакова Т. И. и др.; под ред. В. А. Матвеева; НИИ РиЛТ МГТУ им. Н.Э. Баумана, 2013. - 244 с.
8. Разработка систем информационно-компьютерной безопасности / Зима В.М., Котухов М.М., Ломако А.Г., Марков А.С., Молдовян А.А. - СПб: ВКА, 2003. - 327 с.
9. Кондаков С.Е. Анализ и синтез комплекса средств защиты информации // Вопросы кибербезопасности. 2013. № 2. С. 20-24.
10. Кондаков С.Е. Модель оценки обоснованности выбора варианта КСА // Известия Института инженерной физики. 2013. Т. 4. № 30. С. 44-46.
11. Кондаков С.Е. Обоснование выбора варианта системы защиты информации с показателями различной природы, размерности и вектора полезности // Труды международного симпозиума Надежность и качество. 2014. Т. 1. С. 314-315.
12. Чобанян В.А., Шахалов И.Ю. Анализ и синтез требований к системам безопасности объектов критической информационной инфраструктуры // Вопросы кибербезопасности. 2013. № 1(1). С.17-27.

References

1. Zhukov I.Yu., Zubarev I.V., Kostogryzov A.I. and etc., Metodicheskoe rukovodstvo po otsenke kachestva funktsionirovaniya informatsionnykh system, M.: Izd-vo 3 TsNII MO RF, 2003, 352 p.
2. Markov A.S., Tsirlov V.L., Barabanov A.V. Metody otsenki nesootvetstviya sredstv zashchity informatsii, M.: Radio i svyaz', 2012, 192 p.
3. Domarev V.V. Bezopasnost' informatsionnykh tekhnologiy. Metodologiya sozdaniya sistem zashchity. – K.: DiaSoft, 2002, 688 p.
4. Mel'nikov V.V. Zashchita informatsii v komp'yuternykh sistemakh. - M.: Finansy i statistika, 1997, 368 p.
5. Shcheglov A.Yu. Zashchita komp'yuternoy informatsii ot nesanktsionirovannogo dostupa. M.: Nauka i tekhnika, 2004. 384 p.
6. Akulov O.A., Badanin D.N., Zhuk E.I., Medvedev N.V., Kvasov P.M., Troitskiy I.I. Osnovy informatsionnoy bezopasnosti: Ucheb. posobie. M.: Izd-vo MGTU im. N.E. Baumana, 2008, 161 p.
7. Matematicheskie osnovy informatsionnoy bezopasnosti / Basarab M. A., Bulatov V. V., Buldakova T. I. end etc.; by ed. V. A. Matveeva; NII RiLT MGTU im.N.E.Baumna, 2013, - 244 p.
8. Razrabotka sistem informatsionno-komp'yuternoy bezopasnosti / Zima V.M., Kotukhov M.M., Lomako A.G., Markov A.S., Moldovyan A.A. - SPb: VKA, 2003, - 327 p.
9. Kondakov S.E. Analiz i sintez kompleksa sredstv zashchity informatsii, Voprosy kiberbezopasnosti, 2013, N 2, pp. 20-24.
10. Kondakov S.E. Model' otsenki obosnovannosti vybora varianta KSA, Izvestiya Instituta inzhenernoy fiziki, 2013, Vol. 4, N 30, pp. 44-46.
11. Kondakov S.E. Obosnovanie vybora varianta sistemy zashchity informatsii s pokazatelyami razlichnoy prirody, razmernosti i vektora poleznosti, Trudy mezhdunarodnogo simpoziuma Nadezhnost' i kachestvo, 2014, Vol. 1, pp. 314-315.
12. Chobanyan V.A., Shakhalov I.Yu. Analiz i sintez trebovaniy k sistemam bezopasnosti ob"ektov kriticheskoy informatsionnoy infrastruktury, Voprosy kiberbezopasnosti, 2013, N 1(1), pp.17-27.