1. *Cannady, J.* (1998) Applying Neural Networks to Misuse Detection. Proceedings of the 21st National Information Systems Security conference. P. 368 – 381.

2. *Абрамов Е.С., Макаревич О.Б., Бабенко Л.К., Пескова О.Ю.* Разработка архитектуры СОА на основе нейронной сети // Материалы VI Международной научно-практической конференции «Информационная безопасность», – Таганрог. – 2004. – С. 81 – 86.

3. *Райан Д., Менг-Джанг Лиин* Обнаружение атак с помощью нейросетей.- Режим доступа [http://neurnews.iu4.bmstu.ru/, свободный], 03.12.2009.

Абрамов Евгений Сергеевич
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: juic@mail.ru.
347928, г. Таганрог, пер. Некрасовский, 44.
Тел.: 8(8634)371-905.
Кафедра безопасности информационных технологий; доцент.

Abramov Eugene Sergeevich
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: juic@mail.ru.
44, Nekrasovskiy, Taganrog, 347928, Russia.
Phone: 8(8634) 371-905.
The Department of IT Security; associate professor.

Сидоров Игорь Дмитриевич
Технологический институт Федерального государственного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: idsidorov@gmail.com.
347928, г. Таганрог, пер. Некрасовский, 44.
Тел.: 8(8634)371-905.
Кафедра безопасности информационных технологий; ассистент.

Igor D. Sidorov
Taganrog Institute of Technology – Federal State-Owned Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: idsidorov@gmail.com.
44, Nekrasovskiy, Taganrog, 347928, Russia.
Phone: 8(8634) 371-905.
The Department of IT Security; assistant.

УДК 004.056.53

А.П. Росенко

ОБ ОДНОМ ПОДХОДЕ К ОПРЕДЕЛЕНИЮ ВЕРОЯТНОСТЕЙ ПОСЛЕДСТВИЙ ОТ ВОЗДЕЙСТВИЯ НА АИС УГРОЗ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

В работе предложен один из подходов к определению вероятностей последствий от воздействия на АИС угроз безопасности конфиденциальной информации. Показано, что процесс воздействия на АИС различных дестабилизирующих

факторов можно представить в виде логико-вероятностного процесса. Предложена математическая модель на основе Марковского случайного процесса с дискретными состояниями.

Внутренние угрозы; конфиденциальная информация; особое состояние; логико-вероятностная схема.

A.P. Rosenko

ONE APPROACH TO DETERMINING CONSEQUENCES PROBABILITIES OF EXPOSURE TO AIS INFORMATION SECURITY THREATS

In this paper we propose an approach to determining the probabilities of consequences from exposure to the AIS security threats by confidential information. It is shown that the process of impacts on AIS by various destabilizing factors can be represented in the form of logical-probabilistic process. A mathematical model based on Markov random process with discrete states.

Internal threats; confidential information; particular condition; logical-probabilistic scheme.

1. Актуальность проблемы

Известно, что на безопасность конфиденциальной информации (КИ), циркулирующей в автоматизируемой информационной системе (АИС), оказывают влияние многочисленные факторы [1,5]. В связи с этим для оценки безопасности КИ могут применяться различные подходы. В то же время, как показывает анализ [1–7], для такой оценки необходимо учитывать тот факт, что в результате воздействия на АИС угроз безопасности КИ она может переходить из одного, исходного состояния, в другое – особое состояние. Переход АИС из одного состояния в другое является следствием вполне конкретных причин. Однако возникают они, как правило, в произвольный момент времени, поэтому их появление случайно.

Каждая особая ситуация может привести как к благополучному, так и неблагополучному исходу для КИ с учетом успешности или не успешности действий собственника информации ограниченного распространения по парированию различных по природе происхождения деструктивных факторов.

В работе предлагается методика определения вероятностей последствий от воздействия на АИС угроз безопасности конфиденциальной информации.

2. Постановка задачи

Пусть на АИС воздействует внутренняя угроза, приводящая к возникновению особой ситуации. Обозначим вероятность возникновения i-й особой ситуации через q_i, условную вероятность парирования её последствий - через r_i, а вероятность не парирования – через $\bar{r}_i$. Тогда для определения вероятностей p_i и q_i представим последовательность переходов АИС от одного (исходного) состояния к другому марковским случайным процессом со счетным множеством состояний и дискретным временем. Сущность метода расчета вероятностей p_i и q_i при использовании марковского процесса состоит в том, что неизвестные вероятности определяются из решения матрицы состояний, которая описывает этот процесс.

Последствия от воздействия внутренних угроз на безопасность КИ могут быть различными. Наиболее распространенными из них являются [1]: кража КИ; подмена (модификация) КИ; уничтожение (разрушение) КИ; нарушение нормаль-

ной работы АИС; ошибки и проступки персонала при работе с КИ; перехват КИ. Определение вероятностей таких случайных состояний АИС осуществляется с учетом того, что случайное проявление внутренней угрозы, как потенциально опасного события, а также не парирование особой ситуации сопровождается несанкционированным доступом к информации ограниченного распространения.

Анализ показывает, что процесс воздействия на АИС различных дестабилизирующих факторов целесообразно представить в виде логико-вероятностного процесса.

3. Логико-вероятностная схема возможных состояний АИС

Логико-вероятностная схема возможных состояний АИС представлена на рисунке 1. На рис. 1 обозначения следующие:

«0» – начальное (исходное) состояние АИС;

«БИ» – угроза безопасности КИ с вероятностью $p_{ву}$ не проявилась;

«ОС» – угроза безопасности КИ с вероятностью $q_{ос} = 1 - p_{ву}$ проявилась, что привело к возникновению особой ситуации;

– особая ситуация с вероятностью $r_{ос}$ парирована;

– особая ситуация с вероятностью $\overline{r_{ос}} = 1 - r_{ос}$ не парирована, что привело к перерастанию особой ситуации в несанкционированный доступ к КИ;

– вероятности $q_{кр}, q_{ун}, q_{пер}, q_{под}, q_{аис}, q_{п}, q_{нд}$ – соответственно кражи, уничтожения (разрушения), ошибки и проступки персонала, подмены (модификации), нарушения нормальной работы АИС, перехват и нарушения доступа к КИ.

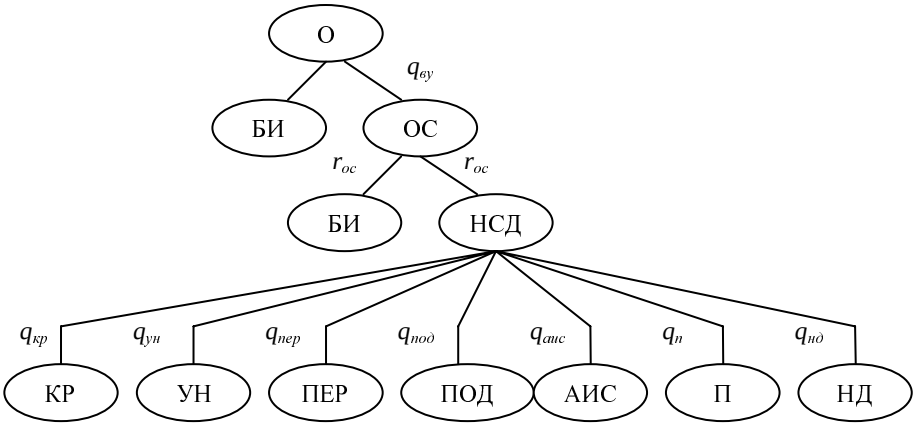

Рис. 1. Логическая схема возможных состояний АИС

4. Вероятности последствий от воздействия на АИС внутренних угроз

В соответствии с рис. 1 вероятности последствий от воздействия угроз безопасности КИ определяются следующим образом:

вероятность благополучного исхода от воздействия на АИС угроз безопасности КИ

$$P_{би} = p_{ву} + q_{ву} r_{ос}; \quad (1)$$

вероятность противоположного события, то есть вероятность неблагополучного исхода от воздействия на АИС дестабилизирующих факторов

$$Q_{би} = q_{ву}\overline{r_{ос}}; \qquad (2)$$

вероятность кражи КИ

$$p_{кр} = Q_{би}q_{к}; \qquad (3)$$

вероятность уничтожения (разрушения) КИ

$$p_{ун} = Q_{би}q_{он}; \qquad (4)$$

вероятность ошибок и проступков персонала

$$p_{пер} = Q_{би}q_{пер}; \qquad (5)$$

вероятность подмены (модификации) КИ

$$p_{под} = Q_{би}q_{под}; \qquad (6)$$

вероятность нарушения нормальной работы АИС

$$p_{аис} = Q_{би}q_{аис}; \qquad (7)$$

вероятность перехвата КИ

$$p_{п} = Q_{би}q_{п}; \qquad (8)$$

вероятность нарушения доступа к КИ

$$p_{нд} = Q_{би}q_{нд}. \qquad (9)$$

Так как вероятности $P_{би_i}$ и $Q_{би_i}$ составляют полную группу событий, то при практическом использовании выражений (3–9) необходимо для проверки компетентности полученных результатов, использовать выражение

$$P_{би_i} + Q_{би_i} = 1.$$

Это связано с тем, что для ветвящегося процесса сумма вероятностей последующих состояний АИС, исходящих из предшествующих, равна единице.

Выражение (1) позволяет определить вероятность благополучного, а выражение (2) – неблагополучного исхода в целом от воздействия на АИС дестабилизирующих факторов. Выражения (3–9) позволяют определить уровень безопасности КИ по видам последствий от воздействия на АИС дестабилизирующих факторов различной природы.

5. Выводы

Предложенная методика позволяет определять вероятности перехода системы в различные состояния с учетом воздействия на АИС внутренних и внешних неблагоприятных факторов. Однако, как показывают исследования, трудности заключаются в том, что для её применения необходимо располагать априорными исходными данными. В связи с тем, что в настоящее время такие данные отсутствуют, наиболее предпочтительными методами получения исходных данных являются методы экспертных оценок.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Росенко А.П.* Теоретические основы анализа и оценки влияния внутренних угроз на безопасность конфиденциальной информации [Текст] / А.П. Росенко // Монография – М.: Гелиос АРВ, 2008. – 154 с.

2. *Росенко А.П.* Марковские модели оценки безопасности КИ с учетом воздействия на автоматизированную информационную систему внутренних угроз [Текст] / А.П. Росенко // Вест. Став. гос. ун-та. – Ставрополь: Изд-во СГУ, 2005. № 43. – С. 34-40.

3. *Росенко А.П.* Математическое моделирование влияния внутренних угроз на безопасность конфиденциальной информации, циркулирующей в автоматизированной информационной системе [Текст] /А.П. Росенко // Известия ЮФУ. Технические науки. – 2008. – № 8 (85). – С. 71-81.

4. *Росенко А.П.* О выборе критерия оценки эффективности функционирования системы защиты информации [Текст] / А.П. Росенко, Е.С. Клименко // Первая международная научно-техническая конференция «Инфотелекоммуникационные технологии в науке, производстве и образовании». – Ставрополь: Изд-во Сев.- Кав. гос. тех.ун-т, 2004. – С. 46 – 47.

5. *Росенко А.П.* Научно-теоретические основы исследования влияния внутренних угроз на безопасность КИ, циркулирующей в автоматизированных информационных системах [Текст] / А.П. Росенко // Известия ТРТУ. Тематический выпуск. “Информационная безопасность”. – 2005. – № 4(48). – С. 19-30.

6. *Росенко А.П.* Математическое моделирование процесса воздействия внутренних угроз на безопасность КИ [Текст] / А.П. Росенко, Е.С. Клименко // Сборник материалов Седьмой международной конференции «Информационные технологии и безопасность. Менеджмент информационной безопасности», 27сентября – 2 октября. Вып. 10. – Киев: Ин-т проблем регистрации информации НАН Украины, 2007. – С. 40-45.

7. *Росенко А.П.* Марковская модель оценки влияния внутренних угроз на безопасность конфиденциальной информации [Текст] / Е.С. Клименко, А.П. Росенко // Известия ТРТУ. Технические науки. Тематический выпуск. «Информационная безопасность». – 2007. – № 1 (76). – С. 123–126.

Росенко Александр Петрович
Ставропольский государственный университет.
E-mail: rosenko@stavsu.ru.
355010, г.Ставрополь, ул. Беличенко, 2, кв.21.
Тел.: 8 (8652) 94-13-81.
Заведующий кафедрой компьютерной безопасности.

Rosenko Aleksander Petrovich
Stavropol State University
E-mail: rosenko@stavsu.ru.
App 21, 2, Belichenko str., Stavropol, 355010, Russia.
Phone: 8 (8652) 94-13-81.
Head of the department “Computer Security”.