УДК 681.325.3

Моделирование процессов ввода информации и оценки показателей эффективности систем санкционированного управления

Ю. В. Александров, С. В. Елагин, В. Н. Фомченко

Предложена модель процесса ввода информации в ССУ, на основании анализа которой получены формализованные выражения для оценки показателей эффективности информационно-кодового управления. Произведены оценки влияния защитных механизмов на эффективность управления и определены зависимости основных вероятностных и временных характеристик, по результатам анализа которых обоснован выбор характеристик ССУ.

В настоящее время системы санкционированного управления (ССУ) широко внедряются в различные производственные сферы для обеспечения безопасности потенциально-опасных объектов (ПОО) и технологических процессов (ТП). ССУ должны обеспечивать, с одной стороны, требуемые уровни защищенности ППО и ТП, а с другой – оперативность управления ПОО и ТП с целью пресечения несанкционированных действий (НСД) и предотвращения опасных событий. В связи с этим к основным показателям эффективности ССУ могут быть отнесены следующие вероятностные и временные характеристики: вероятность совершения НСД, ожидаемое безопасное время [1], среднее время ввода санкционирующей информации (СИ).

Для оценки указанных показателей эффективности необходимо проанализировать модель процесса ввода СИ и исследовать влияние действующих защитных механизмов. Ожидаемое безопасное время (ожидаемое время подбора СИ T_C) может быть определено как произведение среднего числа попыток подбора r на время совершения одной попытки t_n [1]

$$T_C = r t_n . \qquad (1)$$

При исчерпывающем переборе кодовых комбинаций r определяется в соответствии с выражением [2]

$$r = \sum_{i=1}^{M} i \left(1 - \frac{i}{M}\right) \frac{1}{M-i} = \frac{1}{M} \sum_{i=1}^{M} i = \frac{1}{M} \frac{M(M+1)}{2} = \frac{M+1}{2}. \qquad (2)$$

Для варианта подбора СИ с использованием случайного закона формирования кодовых комбинаций среднее число попыток r подбора СИ может быть определено по формуле [3]

$$r = \sum_{i=1}^{\infty} i q^{i-1} p, \tag{3}$$

где $p = 1/M$ – вероятность правильного подбора СИ с первой попытки; M – число возможных кодовых комбинаций; $q = 1 - p$.

Пользуясь правилами преобразования рядов, выражение (3) можно получить в виде

$$r = 1/p. \tag{4}$$

Соответственно T_C с учетом (1) будет определяться зависимостью

$$T_C = t_n / p = t_n M. \tag{5}$$

Таким образом, при подборе СИ методом случайного формирования кодовых комбинаций T_C будет в два раза больше, чем в случае исчерпывающего перебора.

Ожидаемое безопасное время должно соответствовать условию $T_C < T_{\text{отв}}$, где $T_{\text{отв}}$ – время, отводимое злоумышленнику на совершение попыток подбора СИ. В том случае, если данное условие не выполняется, необходимо предпринимать меры увеличения T_C. С этой целью применяются различные способы, в числе которых можно выделить следующие:

– динамическое увеличение времени задержки;

– динамическое увеличение разрядности СИ (эргодической мощности).

Динамическое увеличение времени задержки происходит после выполнения определенного количества κ попыток подбора СИ. При этом T_C может быть вычислено по формуле

$$T_C = 1/2M\left[t_n(\kappa+1)\kappa + \left(t_{\text{ф}} + t_{\text{в}} + wt_{\text{зд}}\right)\left((M+1)M - (\kappa+1)\kappa\right)\right], \tag{6}$$

где w – коэффициент увеличения времени задержки.

Динамическое увеличение эргодической мощности происходит в результате перехода ССУ в состояние ограничения числа попыток (ОЧП) после выполнения определенного количества неудачных операций подбора СИ [2]. С целью выхода из состояния ОЧП требуется подбор дополнительного массива СИ.

При реализации в ССУ счетчика ОЧП исчерпывающий перебор кодовых комбинаций не гарантирует 100 %-ного успеха, так как истинная комбинация СИ может быть опробована злоумышленником при нахождении ССУ в состоянии ОЧП [2]. Поэтому следует ожидать, что в этом случае осведомленный злоумышленник воспользуется альтернативным вариантом подбора СИ способом случайного формирования кодовых комбинаций.

Представляет интерес проанализировать модель ввода информации, характеризующей процесс подбора СИ для вариантов наличия и отсутствия счетчика ОЧП.

При случайном законе формирования кодовых комбинаций появление событий, соответствующих успешным попыткам подбора СИ, происходит случайным образом. Можно с некоторыми допущениями предположить, что время подбора СИ до успешной попытки характеризуется показательным законом распределения. В этом случае процесс подбора СИ может быть представлен в виде непрерывной цепи Маркова [3].

При отсутствии счетчика ОЧП процесс подбора СИ характеризуется цепью Маркова, показанной на рис. 1,а. В результате решения линейных алгебраических уравнений, составленных для цепи Маркова, получены формулы для оценки финальных вероятностей состояний:

$$P_1 = P_0 \lambda_{01}/\mu_{10};\ P_0 = \left(1 + \lambda_{01}/\mu_{10}\right)^{-1}.$$

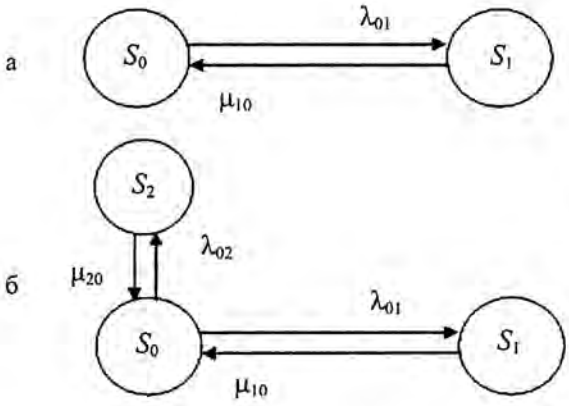

Рис. 1. Граф состояний процесса подбора СИ при отсутствии (а) и наличии (б) счетчика ОЧП: S_0 – исходное состояние процесса подбора СИ; S_1 – состояние правильного подбора СИ; S_2 – состояние ОЧП

Переход из исходного состояния S_0 в состояние правильного подбора шифра S_1 осуществляется с интенсивностью в соответствии с выражением

$$\lambda_{01} = 1/t_n M . \quad (7)$$

Переход в исходное состояние из состояния S_1 происходит с интенсивностью, определяемой временем между двумя попытками ввода СИ по формуле

$$\mu_{10} = 1/t_n . \quad (8)$$

С учетом вероятностей состояния цепи Маркова (см. рис. 1,а), а также формул (7), (8) может быть получена зависимость для определения r:

$$r = M = 1/P_1 - 1 . \quad (9)$$

При наличии счетчика ОЧП процесс подбора СИ может быть представлен в виде цепи Маркова (рис. 1,б). Решая линейные алгебраические уравнения, составленные для данной цепи, можно определить финальные вероятности состояний $P_1 = P_0\lambda_{01}/\mu_{10}$; $P_1 = P_0\lambda_{02}/\mu_{20}$; $P_0 = \left(1 + \lambda_{01}/\mu_{10} + \lambda_{02}/\mu_{20}\right)^{-1}$.

Интенсивности переходов λ_{01}, μ_{10} определяются по формулам (6), (7). Интенсивность перехода в состояние ОЧП может быть оценена в соответствии со следующим выражением $\lambda_{01} = Q_к/t_n к$, где $к$ – число попыток ограничения подбора СИ; $P_к$ – вероятность успешного подбора СИ за $к$ попыток; $Q_к = 1 - P_к$.

В том случае, если подбор СИ осуществляется по случайному закону формирования кодовых последовательностей, формула для определения вероятности $P_к$ может быть получена в соответствии с геометрическим законом распределения вероятностей в виде

$$P_к = \sum_{i=1}^{к} q^{i-1} p . \quad (10)$$

Переходы из состояния S_2 в исходное состояние S_0 осуществляются с интенсивностью $\mu_{20} = 1/M t_n$. На основании полученных соотношений выражение для определения вероятности состояния успешного подбора СИ P_1 может быть получено в виде

$$P_1 = \left(1 + Q_к M/к + 1/M\right)^{-1} 1/M . \quad (11)$$

Соответственно с учетом (1), (9) и (11) выводится формула для оценки T_C:

$$T_C = t_n\left[\left(1 + Q_к M/к + 1/M\right)M\right] - 1 . \quad (12)$$

К важнейшим показателям, характеризующим эффективность ССУ, относится вероятность совершения НСД $P_{НСД}$. В частном случае, когда злоумышленник осуществляет раскрытие СИ методом подбора, в качестве $P_{НСД}$ следует рассматривать вероятность подбора СИ за ограниченное время $P_{ПСИ}$. При исчерпывающем переборе СИ оценки $P_{ПСИ}$ могут быть получены в соответствии с выражением

$$P_{\text{ПСИ}} = l/M, \tag{13}$$

где $l = T_{\text{отв}}/t_n$ – среднее число попыток подбора СИ за $T_{\text{отв}}$.

В случае подбора СИ с использованием случайного закона формирования кодовых последовательностей $P_{\text{ПСИ}}$ определяется по следующей формуле, полученной с учетом (10)

$$P_{\text{ПСИ}} = \sum_{i=1}^{l} q^{i-1} p. \tag{14}$$

При наличии счетчика ОЧП вероятность $P_{\text{ПСИ}}$ определяется путем решения алгебраических уравнений для цепи Маркова (рис. 1,б). При этом полученное решение с достаточной степенью точности может быть аппроксимировано системой уравнений, которой удобно пользоваться для расчетов

$$\begin{aligned} P_{\text{ПСИ}} &= 1 - l^{-\frac{l}{m}} \text{ при } l \le \kappa; \\ P_{\text{ПСИ}} &= 1 - l^{-\frac{\kappa}{m}} + 1 - l^{-\frac{l}{\eta}} \text{ при } \kappa \le l \le \infty. \end{aligned} \tag{15}$$

До срабатывания счетчика ОЧП $P_{\text{ПСИ}}$ определяется верхней формулой системы уравнений (15). При реализации к попыток происходит переход в состояние ОЧП. После этого необходимо выполнить подбор дополнительного массива СИ, требуемый для возврата в исходное состояние S_0 цепи Маркова. В этом случае оценка $P_{\text{ПСИ}}$ осуществляется в соответствии с нижней формулой системы уравнений (15). Далее процесс подбора может повторяться циклически. При этом выражение для определения среднего числа попыток подбора r_l может быть получено в виде

$$r_1 = 1/P_1 - \kappa - 1_1 = \left(1 + M/\kappa\left(1 - 1/M\right)^{\kappa} + 1/M\right)M - \kappa - 1. \tag{16}$$

Показательным параметром, характеризующим оперативность управления, является среднее время ввода СИ $t_{\text{вс}}$ в аппаратуру ССУ. Для оценки $t_{\text{вс}}$ со специализированных носителей (СН) и кнопочного наборного поля может быть проанализирована модель процесса ввода СИ, представленная в виде цепи Маркова (рис. 2). В результате решения линейных алгебраических уравнений, составленных для данной цепи, получены формулы для определения финальных вероятностей состояний

$$P_1 = P_0 \lambda_{01}/\mu_{10}; P_2 = P_0 \lambda_{02}/\mu_{20}; P_3 = P_0 \lambda_{03}/\mu_{30};$$
$$P_0 = \left(1 + \lambda_{01}/\mu_{10} + \lambda_{02}/\mu_{20} + \lambda_{03}/\mu_{30}\right)^{-1}.$$

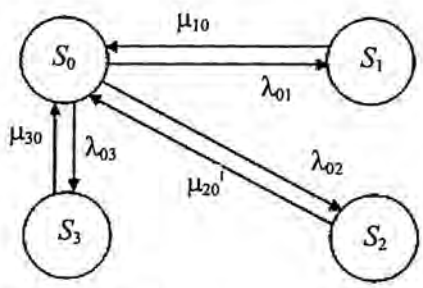

Рис. 2. Граф состояний процесса ввода информации в аппаратуру управления: S_0 – исходное состояние процесса ввода СИ; S_1 – состояние ОЧП; S_2 – состояние отказа средств ввода; S_3 – состояние безошибочного ввода СИ

Для определения $t_{\text{вс}}$ можно воспользоваться формулой

$$t_{\text{вс}} = r(t_{\text{в}} + t_{\text{зд}}). \tag{17}$$

Среднее число попыток ввода информации r определяется по аналогии с (9) с учетом вероятностей состояний цепи Маркова (рис. 2)

$$r = 1/P_3 - 1. \tag{18}$$

Таким образом, формула (17) для определения $t_{вс}$ приобретает вид

$$t_{вс} = (1/P_3 - 1)\ (t_в + t_{зд}). \tag{19}$$

Выражение для оценки интенсивности переходов в состояние безошибочного ввода СИ с СН может быть получено в следующем виде:

$$\lambda_{03} = (1 - P_{инф} - P_{от})\lambda_в, \tag{20}$$

где $\lambda_в = 1/(t_в + t_{зд})$ – интенсивность попыток ввода информации; $P_{от}$ – вероятность отказа средств ввода СИ; $P_{инф} = 1 - e^{-P_0 N}$ – вероятность ошибки ввода блока информации с СН; P_0 – вероятность ошибки передачи элемента сигнала; N – число разрядов блока СИ.

При вводе СИ с кнопочного наборного поля вероятность ошибки ввода блока информации определяется в соответствии с формулой $P_{инф} = 1 - (1 - P_{симв})^n$, где $P_{симв}$ – вероятность ошибочного ввода символа; n – число символов в кодовой комбинации.

Переход в состояние S_0 из состояния S_3 цепи Маркова (см. рис. 2) происходит с интенсивностью, определяемой временем между двумя попытками ввода СИ $\mu_{30} = 1/(t_в + t_{зд})$. В случае превышения числа ошибочных попыток ввода СИ над заданными ограничениями осуществляется переход в состояние S_1 ОЧП с частотой $\lambda_{01} = P_{ош}\lambda_в/\kappa$, где $P_{ош}$ – вероятность перехода в состояние ОЧП вследствие ошибок ввода СИ. При этом для возвращения в исходное состояние необходимо осуществить ввод соответствующей СИ. Эта операция может быть выполнена за время $t_{уб}$.

Выражение для оценки $P_{ош}$ может быть получено в следующем виде:

$$P_{ош} = P_\kappa C^1_{m-\kappa+1}/C^\kappa_m = (m - \kappa + 1)P^\kappa_{инф}(1 - P_{инф})^{m-\kappa}. \tag{21}$$

В процессе ввода СИ возможны отказы средств ввода СИ, возникающие с частотой $\lambda_{02} = P_{от}\lambda_в$. Устранение отказов осуществляется за время $t_{уо}$ с интенсивностью $\mu_{20} = 1/t_{ус}$.

С учетом полученных соотношений $t_{вс}$ может быть выражено следующей зависимостью:

$$t_{вс} = \frac{(t_в + t_{зд}) + (P_{ош}/\kappa)t_{уб} + P_{от}t_{уо}}{(1 - P_{инф} - P_{от})}. \tag{22}$$

Предложенная модель процесса ввода позволяет получать сравнительные оценки $t_{вс}$ от объемов вводимой СИ с СН и кнопочного наборного поля в виде графиков (рис. 3).

С целью обоснования выбора числа попыток подбора СИ κ может быть предложена графическая модель (рис. 4), которая характеризует зависимость вероятности перехода в состояние ОЧП P_1 вследствие ошибок ввода информации и вероятности подбора СИ $P_{ПСИ}$ от значения κ. В качестве исходных приняты следующие данные:

$$M = 16{,}7 \cdot 10^6, \quad T_{отв} = 2880\ ч, \quad t_л = 12\ с, \quad t_з = 3\ с, P_{ош} = 10^{-3}, \quad P^{доп}_{НСД} < 10^{-6}.$$

В соответствии с полученными графиками можно выделить область значений $к$, которая ограничивается, с одной стороны, допустимой вероятностью совершения НСД $P_{НСД}^{доп} < 10^{-6}$, а с другой – вероятностью P_1, которую также целесообразно ограничить уровнем $P_1 < 10^{-6}$ для того, чтобы свести к минимуму возможности перехода в состояние ОЧП вследствие ошибок ввода информации. На рис. 4 данная область заключена между значениями $к$, равными 8 и 15, которые удовлетворяют сформулированным условиям. Из этого диапазона может быть выбрано значение счетчика ОЧП.

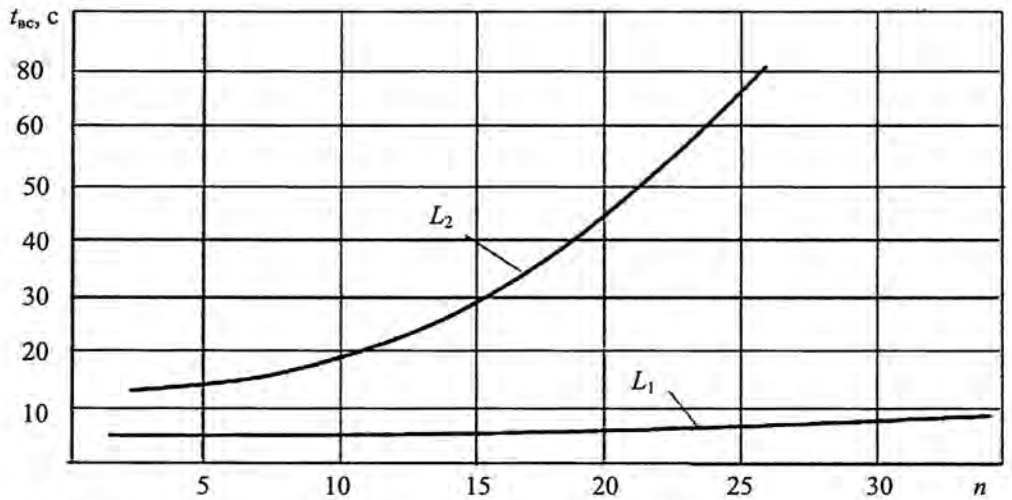

Рис. 3. График зависимости среднего времени ввода $t_{вс}$ от объемов вводимой информации с СН (L_1) и кнопочного наборного поля (L_2)

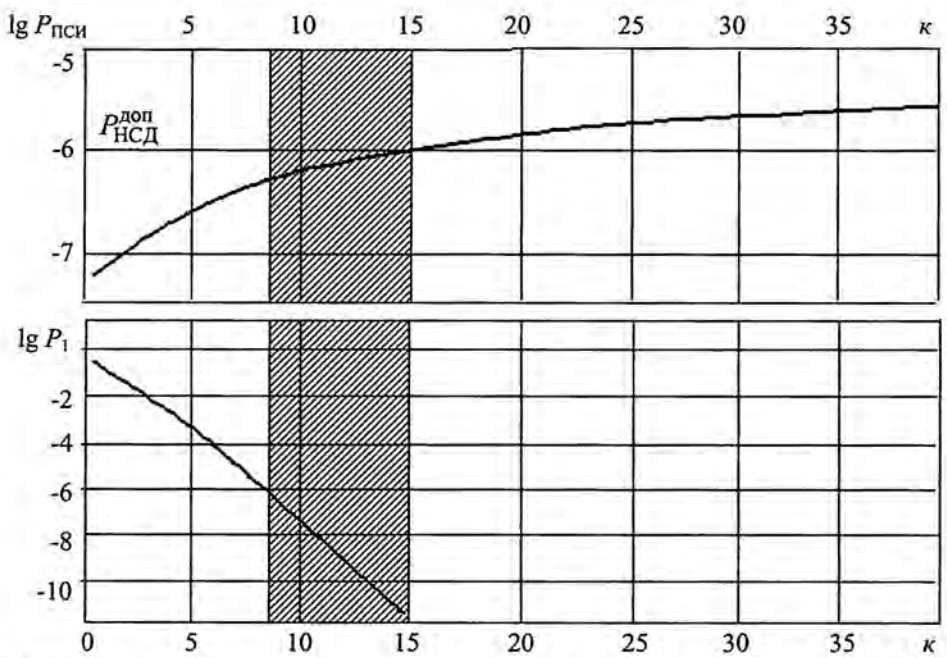

Рис. 4. Графики зависимости вероятности перехода в состояние ОЧП P_1 вследствие ошибок ввода информации и вероятности подбора СИ $P_{ПСИ}$ от значения счетчика ОЧП $к$

Предложенные модели процесса ввода СИ в ССУ, основу которых составляют марковские процессы, и разработанный методический аппарат позволяют получить оценки основных показателей эффективности ССУ, вывести формализованные зависимости основных временных и вероятностных характеристик, выполнить сравнительные оценки эффективности способов автоматизированного и ручного (кнопочного) ввода информации. Предложенная графическая модель дает возможность определить оптимальное значение ОЧП в соответствии с требуемыми показателями оперативности управления и уровнями защищенности ПОО и ТП.

Список литературы

1. Хоффман Л. Дж. Современные методы защиты информации. М.: Сов.радио,1980.

2. Александров Ю. В., Елагин С. В., Кушнарев А. П. и др. Электронные кодовые переключатели. Защита цифровой информации от утечки по побочным каналам / Научно-технический сборник под редакцией А. И. Астайкина, В. Н. Фомченко. Саров: РФЯЦ-ВНИИЭФ, 2005. С. 364–443.

3. Вентцель Е. С., Овчаров Л. А. Прикладные задачи теории вероятности. М.: Радио и связь, 1983.

Simulation of Input Information Processes and Estimation of Efficiency Parameters of Authorized Management Systems

Y. V. Alexandrov, S. V. Elagin, V. N. Fomchenko

The model of input information process in authorized management systems (AMS) on the basis of which analysis the formalized expressions for an estimation of parameters of efficiency of information – code management are received is offered. Estimations of influence of protective mechanisms on a management efficiency are made and dependences of the basic вероятностных and time characteristics by results of which analysis the choice of characteristics AMS is proved are determined.