Климов С.М., Котяшев Н.Н.

МЕТОД РЕГУЛИРОВАНИЯ РИСКОВ КОМПЛЕКСОВ СРЕДСТВ АВТОМАТИЗАЦИИ В УСЛОВИЯХ КОМПЬЮТЕРНЫХ АТАК

Статья посвящена методу регулирования рисков комплексов средств автоматизации в условиях компьютерных атак на основе динамического управления и минимизации рисков нарушения информационных ресурсов. В методе предложены аналитические выражения для целевых функционалов и допусков на факторы риска, позволяющие формировать рациональные решения по управлению рисками комплексов средств автоматизации.

***Ключевые слова*:** *комплекс средств автоматизации, компьютерная атака, регулирование рисков.*

Актуальной проблемой информационной безопасности является обоснование требований к регулированию рисков (управлению рисками) применения комплексов средств автоматизации реального масштаба времени (КСА) в условиях компьютерных атак.

Под КСА будем понимать критически важные сегменты автоматизированных систем, функционирующие в режимах, близких к реальному масштабу времени, выход параметров (времени сбора, обработки, передачи информации и выдачи управляющих воздействий) которых за установленные пределы приводит к нарушению устойчивости функционирования.

Регулирование рисков рассмотрим для проектируемых КСА, состояние которых динамически изменяется во времени в условиях компьютерных атак.

Сущность метода регулирования рисков КСА состоит в минимизации рисков вида $R=PY \rightarrow \min$, где P – вероятность события реализации компьютерной атаки нарушителем за период времени обнаружения; Y – математическое ожидание ущерба от воздействия компьютерной атаки. Пусть имеется достигнутый уровень этого риска $R_0=P_0*Y_0$. Тогда регулирование рисков заключается в целенаправленном изменении факторов риска до уровня возможности выполнения целевой функции КСА по двум возможным критериям: снижение уровня риска до требуемых значений или минимизация риска при имеющихся ограничениях на информационные ресурсы.

Задача регулирования рисков КСА решается в линейной и нелинейной постановке. В работах [1, 2] рассмотрены примеры регулирования рисков в линейной постановке при малых ограничениях на факторы риска, которые сведены к задаче линейного программирования в нормированном пространстве функционала затрат и ограничений.

$$\overline{S}(\overline{P},\overline{Y}) = (1-a)\cdot\overline{P} + (1-b)\cdot\overline{Y} \quad (1)$$

где $\overline{X} = (X - X_0)/X_0$; $\overline{X}_1 \le \overline{X} \le \overline{X}_2$, a, b – коэффициенты затрат на уменьшение факторов риска.

Аддитивное представление функционала получено путем записи и раскрытия мультипликативной формы вида (P0+dP)(Y0+dY) с отбрасыванием членов второго порядка малости и добавлением (с обратным знаком) управляющих затратами составляющих a(P-P0)Y0 и b(Y-Y0)P0.

Ввиду того, что оператор нормирования не меняет положения экстремума, эта задача разрешима и для ненормированных факторов риска, что упрощает задачу

$$S(P,Y) = (1-a)\cdot P + (1-b)\cdot Y \text{ , где } X_1 \le X \le X_2.$$

Проверка подобной замены осуществляется путем проверки равенства частных производных от функционалов по факторам риска нарушения устойчивости функционирования КСА в условиях компьютерных атак не только для линейных, но и для произвольных функционалов, а также взаимообратимости ограничений. Данное утверждение вытекает из положений теории чувствительности, определяющих соотношения для функционала и факторов риска.

Регулирование рисков КСА в условиях вероятностной неопределенности в задании факторов риска и их малых вариациях на основе использования функций чувствительности первого порядка [3] выполняется следующим образом.

Пусть риск обеспечения устойчивости функционирования КСА в условиях компьютерных атак описывается выражением

$$R = Y \cdot P,$$

где Y и P – средние значения для вероятности реализации компьютерных атак и ущерба.

Запишем разложение функции риска в ряд Тейлора с удержанием в нем только линейных членов

$$R(P,Y) = R_0(P_0,Y_0) + \left(1 - \frac{dR}{dP}\right)\cdot dP + \left(1 - \frac{dR}{dY}\right)\cdot dY.$$

Пусть также заданы их исходные значения R0 и Y0 и, значит, исходный уровень риска R0=P0*Y0.

Соответствующими функциями чувствительности по параметрам риска будут

$$FZp = \left.\frac{\partial R}{P}\right|_{R_0} = \left.\frac{\partial(P\cdot Y)}{P}\right|_{R_0} = Y_0,$$

и

$$FZp = \left.\frac{\partial R}{Y}\right|_{R_0} = \left.\frac{\partial(P\cdot Y)}{Y}\right|_{R_0} = P_0.$$

Уровень вероятностной неопределенности отдельных факторов риска при нормальном законе распределения погрешностей их задания составит соответственно

$$\delta P = \chi_q \cdot \sigma_p,$$

$$\delta Y = \chi_q \cdot \sigma_y ,$$

где χ_q и χ_y, а также σ_q и σ_y – соответствующие квантили и средние квадратические отклонения (СКО) распределения погрешностей задания этих факторов.

Тогда функциями влияния на функцию риска указанных неопределенностей будут

$$FWp = FZp \cdot \delta P$$

и

$$FWy = FZy \cdot \delta Y .$$

В зависимости от функциональных особенностей КСА они могут складываться либо арифметически (наихудший случай), либо геометрически

$$FW_1 = FZp \cdot dP + FZy \cdot dY,$$

$$FW2 = \sqrt{(FZp \cdot dP)^2 + (FZy \cdot dY)^2}.$$

В общем случае гарантированный риск составит

$$R_Г = R_0 + FW.$$

Так, например, для P_0=0.5 и Y_0=20, следовательно R_0=10, FZp=20, FZy=0.5, СКО σ_p=0.1 и σ_y=1, а также неопределенности с уровнем доверия 0.993 гарантированный уровень риска будет равен для наихудшего случая только Rг=16.75.

При этом методическая ошибка линеаризации определяется выражением

$$dR_г = R_г - P_г \cdot Y_г = P_0 \cdot Y_0 - (P_0 - \delta P) \cdot (Y_0 - \delta Y)$$

и составит хотя и вполне допустимую величину – 0.729, но способную изменить направление управления по выражению (1).

Для компенсации этой суммарной неопределенности в задании только одного фактора риска, например, управления, потребуется введение следующих управлений

$$dPu = \frac{-1}{FZp} \cdot FW,$$

и

$$dYu = \frac{-1}{FZy} \cdot FW.$$

В обоих случаях будем иметь новый гарантированный риск, равный исходному среднему значению

$$R_г^н = P_г \cdot Y_г = (P_0 - \delta P) \cdot Y_0 + FW = P_0 \cdot (Y_0 - \delta) + FW = R_0.$$

Формирование КСА с минимальным риском нарушения устойчивости функционирования на основе использования функций чувствительности, когда требуется уменьшить уровень риска до некоторого требуемого значения Rtr, осуществляется следующим образом.

Составим систему алгебраических уравнений с учетом равенства вкладов факторов риска в функцию риска сложных КСА

$$FZ_p \cdot (P - P_0) = FZ_y \cdot (Y - Y_0)$$

и заданного ограничения на величину функции риска $P \cdot Y = Rtr$

$$\begin{cases} FZ_p \cdot (P - P_0) = FZ_y \cdot (Y - Y_0), \\ P \cdot Y = Rtr. \end{cases}$$

С учетом $Ytr(Rtr) = Rtr / Ptr$ приведем первое уравнение к виду

$$FZ_p \cdot (Ptr - P_0) - (FZ_y \cdot (\frac{Rtr}{Ptr} - Y_0) = 0.$$

Корень этого уравнения и будет искомой величиной Ptr (находится с использованием средств компьютерной математики MathCad «root») из ограничения на величину функции риска

$$Ytr(Rtr) = \frac{Rtr}{Ptr(Rtr)}.$$

Пусть Rtr=1. Элементарные вычисления дают

Ptr(Rtr)=0.158 и Ytr(Rtr)=6.35.

при условии, что $Ptr(Rtr) \cdot Ytr(Rtr) = 1$.

Значения факторов риска чувствительны к своим начальным уровням и к уровню требований для функции риска (рис. 1).

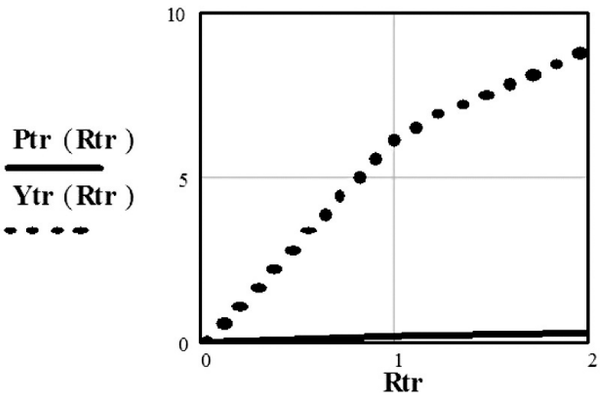

Рис. 1. Зависимости факторов риска от требований к уровням риска

Весьма важно аналитическое решение для определения значений рассматриваемых рисков с использованием функций чувствительности и затрат при ограничениях на уровень неопределенности

риска. Пусть требуется уменьшить гарантированный уровень риска обеспечения устойчивости функционирования КСА

$$R_г = P_0 \cdot Y_0 + FZ_p \cdot dP + FZ_y \cdot dY.$$

Имеющийся уровень неопределенности снизим наиболее экономичным образом до некоторого заданного уровня Rtr. Минимизируем функционал стоимости вида

$$C_s = C_p \cdot \left(P_0 / dP \right)^{\nu} + C_y \cdot \left(Y_0 / dY \right)^{\nu},$$

где C_p и C_y – коэффициенты затрат, ν – коэффициент, обеспечивающий выбор наилучших аппроксимаций. Зададим также уровень неопределенности вида

$$FZ_p \cdot dP + FZ_y \cdot dY = eps.$$

Задача сводится к поиску безусловного экстремума с использованием принципа Лагранжа. Запишем лагранжиан вида

$$FL(dP, dY, \lambda) = Cp \cdot \left(P0 / dP \right)^{\nu} + Cy \cdot \left(Y0 / dY \right)^{\nu} + \lambda \cdot \left[\left(FZp \cdot dP + FZy \cdot dY \right) - eps \right]$$

Имеется аналитическое решение

$$dP = \frac{eps \cdot \left[Cp \cdot \left(P0^{\nu} / dP \right) \right]^{\frac{1}{1+\nu}}}{FZp \cdot \left[Cp \cdot \left(P0^{\nu} / dP \right) \right]^{\frac{1}{1+\nu}} + FZy \cdot \left[Cy \cdot \left(Y0^{\nu} / dY \right) \right]^{\frac{1}{1+\nu}}},$$

$$dY = \frac{eps \cdot \left[Cy \cdot \left(Y0^{\nu} / dY \right) \right]^{\frac{1}{1+\nu}}}{FZp \cdot \left[Cp \cdot \left(P0^{\nu} / dP \right) \right]^{\frac{1}{1+\nu}} + FZy \cdot \left[Cy \cdot \left(Y0^{\nu} / dY \right) \right]^{\frac{1}{1+\nu}}}.$$

Из зависимостей видно, что увеличение исходных вероятностей и уменьшение уровней неопределенности увеличивает затраты Z(dP, dY) (рис. 2).

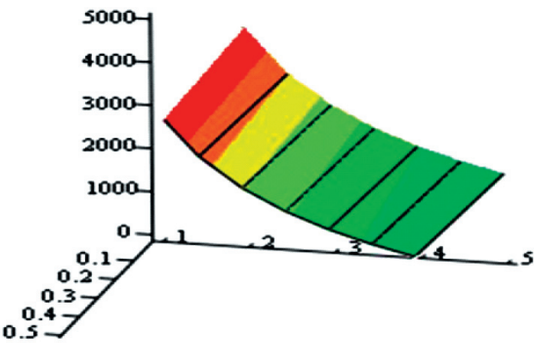

Рис. 2. Зависимость возрастания затрат от снижения уровней неопределенности в оценках риска

Не изменяя принятых исходных предположений и принимая eps=1, Ср=20, Су=1, будем иметь

$$dP = 0.036,\ dY = 0.561 \text{ и } CS = 5.502 \cdot 10^4.$$

Уровень нового гарантированного риска составит

$$(P_0 + dP) \cdot (Y_0 + dY) = 11.02.$$

Как видим, погрешность линеаризации относительно номинального риска и принятого ограничения и в этом случае незначительна (0.02).

Для проверки правильности аналитического решения был проведен численный эксперимент. Вычисления оптимальных вариаций факторов риска осуществлялись с использованием директивы «Given» и процедуры «Minimise» в средствах компьютерной математики MathCad. Результаты решения практически (с точностью до машинного представления чисел) совпадают. Та же задача, но при ограничении в виде геометрической суммы функций влияния

$$\sqrt{(FZp \cdot dP)^2 + (FZy \cdot dY)^2} = eps,$$

обеспечивает такой же уровень гарантированного риска при более высоких значениях факторов риска в сравнении с наихудшим случаем

$$dP = 0.047,\ dY = 0.691 \text{ и } CS = 242.068.$$

Уровень гарантированного риска составит

$$R_г = 11.317$$

Риск невыполнения расчетной функциональной задачи КСА может быть определён через произведение вероятности возникновения опасного события на величину ущерба [4]. Наиболее существенным является получение функции риска с учетом состояния информационного ресурса КСА. Зависимости для состояния информационных ресурсов (при показательном законе распределения компьютерных атак) и функции распределения времени реализации процесса в КСА, а также средний ущерб представлены на рисунке 3.

Функцию риска с учетом состояния информационных ресурсов КСА можно представить в следующем виде:

$$R(t) = \begin{cases} 0 \quad при \ \ t \le t[N(t) = РФЗ], \\ FR(t \le T_{фз}) \cdot [РФЗ - N(t)] \quad при \quad t > t[N(t) = РФЗ], \end{cases}$$

где $FR(t)$ – функция распределения времени формирования набора операций по управлению информационными ресурсами КСА;

$N(t)$ – текущий информационный ресурс КСА;

РФЗ – уровень расчетной функциональной задачи;

$T_{фз}$ – момент времени, когда текущий уровень информационных ресурсов КСА достигает уровня, минимально необходимого для решения функциональной задачи.

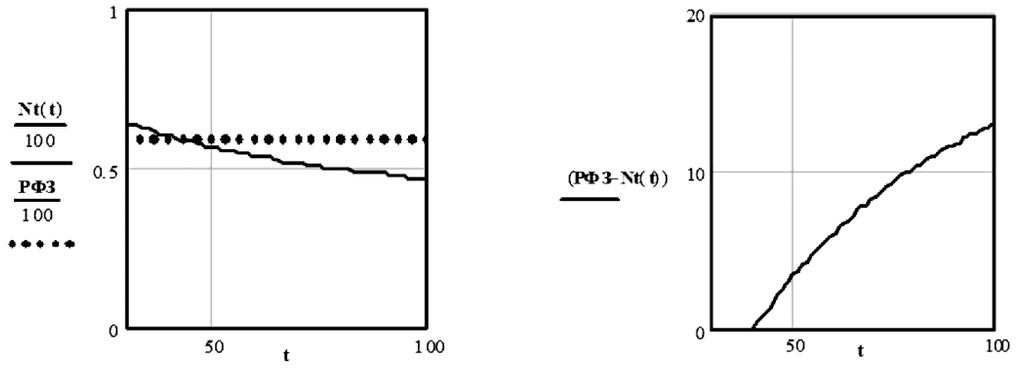

Рис. 3. Зависимости функции риска с учетом состояния информационного ресурса КСА

На рисунке 4 представлены функции среднего риска, включая риск относительно расчетной функциональной задачи для непрерывных КСА в условиях компьютерных атак, а также их нижние и верхние границы.

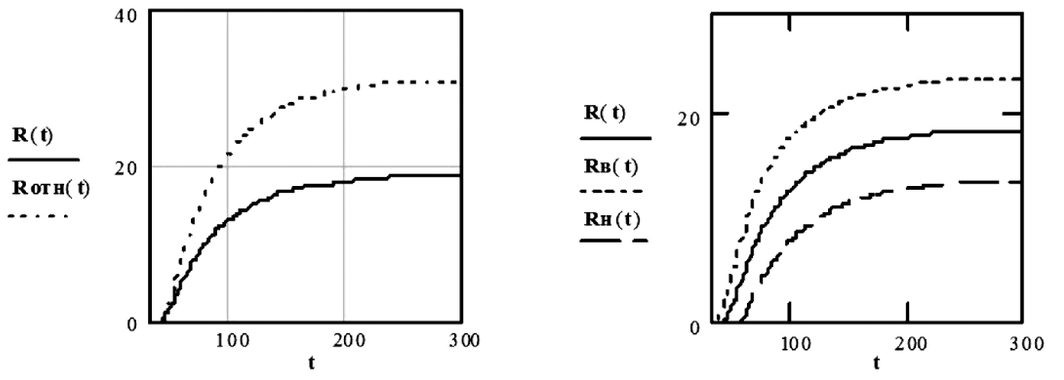

Рис. 4. Функции для среднего риска применения непрерывных КСА

Значения функций на рисунке 4 определяются выражениями

$$R_н(t) = \begin{cases} 0 \quad при \quad t \le t\left[N_в(t) = РФЗ\right], \\ FR(t \le T_{фз}) \cdot \left[РФЗ - N_в(t)\right] \quad при \quad t > t\left[N_в(t) = РФЗ\right], \end{cases}$$

$$R_в(t) = \begin{cases} 0 \quad при \quad t \le t\left[N_н(t) = РФЗ\right], \\ FR(t \le T_{фз}) \cdot \left[РФЗ - N_н(t)\right] \quad при \quad t > t\left[N_н(t) = РФЗ\right], \end{cases}$$

где Nн(t) и Nв(t) – нижняя и верхняя границы разброса информационных ресурсов КСА.

На практике регулирование рисков нарушения устойчивости функционирования КСА в условиях компьютерных атак обеспечивается:

– поддержанием в КСА необходимого уровня информационных ресурсов при априорно заданном законе распределения компьютерных атак;

– активным противодействием источникам компьютерных атак;

– повышением оперативности вычислительных процессов управления и расчетных функциональных задач КСА.

Таким образом, предложен метод регулирования рисков КСА в условиях компьютерных атак, основанный на аналитических выражениях для целевых функционалов и допусков на факторы риска и позволяющий формировать рациональные решения по управлению рисками КСА.

Литература

1. **Волков Л.И.** Безопасность и надежность систем. М.: СИП РИА. 2003.-268 с.

2. **Василенко В.В., Глухов А.П., Котяшев Н.Н.** Управление рисками применения проектируемых систем в условиях воздействий //Стратегическая стабильность, №1, 2008г. – с. 39-46.

3. **Розенвассер Е.Н., Юсупов Р.М.** Чувствительность систем управления. М.: Наука. 1981. – 464 с.

4. **Шубинский И.Б.** Функциональная надежность информационных систем. Методы анализа. – Ульяновск: Областная типография «Печатный двор», 2012. – 296 с., ил.