УДК 656 05 004

Оценка рисков нарушения безопасности критически важных объектов и критических инфраструктур[1]

ISSN 1812-5220

В. Н. Цыгичко,
Федеральный исследовательский центр «Информатика и управление» РАН, г. Москва

Аннотация

В статье представлен метод расчета рисков нарушения безопасности критически важных объектов и критических инфраструктур при существующей системе защиты.

Ключевые слова: безопасность, риск, допустимый риск, уязвимость, угрозы, профиль защиты, эффективность средств защиты, композиция средств защиты.

Содержание

Введение
1. Представление КВО как объекта защиты
2. Процедура оценки рисков нарушения безопасности КВО
3. Оценка рисков нарушения безопасности критических инфраструктур
4. Расчет допустимого риска нарушения безопасности КВО
Заключение
Литература

Введение

Важной задачей в процедуре управления рисками нарушения безопасности критически важных объектов (КВО) является определение эффективности существующей системы обеспечения их безопасности (СОБ КВО). На практике эффективность СОБ определяется путем оценки уязвимости КВО, которая представляет собой регламентированную в каждой критической инфраструктуре (КИ) экспертную процедуру проверки уровня защищенности всех критических точек объекта (уязвимостей) от всех потенциальных угроз. Задачи этой проверки состоят в определении риска нарушения безопасности КВО при существующей СОБ и сравнении полученных результатов со значениями допустимого риска, нормативно закрепленными в каждой КИ. Если значения риска нарушения безопасности КВО больше нормативного, то выявляются недостатки системы обеспечения безопасности и даются рекомендации по их устранению.

Наиболее сложной задачей в процедуре оценки уязвимости КВО является объективная и корректная интегральная оценка уровня защищенности объекта, в качестве которой выступает риск нарушения безопасности хотя бы одной уязвимости КВО при существующей защите.

[1] Статья подготовлена при поддержке гранта РФФИ № 15-07 01796.

1. Представление КВО как объекта защиты

Для детального анализа процесса функционирования СОБ КВО необходима оценка рисков нарушения безопасности всех критических элементов его функциональной структуры, а в ряде случаев и структурных составляющих этих элементов. Например, такой элемент аэропорта, как центральное здание, имеет в своем составе множество различных служб и специального оборудования, нарушение работы каждого из которых ведет к возникновению чрезвычайных ситуаций. Однако для простоты дальнейшего изложения внутреннюю структуру элементов КВО мы не рассматриваем.

С учетом этого обстоятельства представим КВО как объект защиты множеством уязвимостей $Y_z = \{y_{iz}\}$:

$$Y_z = \begin{vmatrix} y_{11} \\ . \\ y_{iz} \\ . \\ . \\ y_{IZ} \end{vmatrix}, \qquad (1)$$

где $i = 1 - I$ — номер уязвимости;

I — число уязвимостей;

$z = 1 - Z$ — номер элемента КВО;

Z — число элементов.

Множество угроз $Q = \{q_{jk}\}$ уязвимостям Y_z представим матрицей-столбцом Q:

$$Q = \begin{vmatrix} q_{11} \\ . \\ q_{1K} \\ . \\ . \\ q_{jk} \\ . \\ q_{jK} \\ . \\ q_{JK} \end{vmatrix}, \qquad (2)$$

где $j = 1 - J$ — номер потенциальной угрозы;

J — число потенциальных угроз;

jk — номер способа реализации j-й угрозы;

jK — количество способов реализации j-й угрозы.

Если для каждой уязвимости y_{iz} известен перечень угроз ее безопасности и способов их реализации q_{jz}, то профиль защиты КВО можно представить матрицей бинарных отношений $M = \{y_{iz}, q_{jk}\}$:

$$M = \begin{vmatrix} & q_{11} & . & q_{1K} & . & q_{jk} & . & q_{jK} & . & q_{JK} \\ y_{11} & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ . & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ y_{iz} & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ . & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ y_{IZ} & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{vmatrix}. \qquad (3)$$

Эффективность P_{ljk} средств защиты $N = \{n_l\}$ против каждого способа реализации каждой угрозы q_{jk} представим матрицей $P = \{P_{ljk}\}$:

$$P = \begin{vmatrix} & n_1 & . & . & n_l & . & . & n_L \\ q_{11} & P_{111} & - & - & P_{l1} & - & - & P_{L1} \\ . & P_{11k} & P_{21k} & - & - & - & - & - \\ q_{1K} & P_{11K} & - & - & P_{l1K} & - & - & - \\ . & P_{12k} & - & - & - & - & - & P_{L2k} \\ q_{jk} & P_{1jk} & P_{2jk} & - & - & - & - & P_{Ljk} \\ . & P_{1jk} & P_{2jk} & - & P_{ljk} & - & - & - \\ q_{JK} & P_{1JK} & - & - & - & - & - & P_{LJK} \end{vmatrix}, \qquad (4)$$

где $l = 1 - L$ — номер средства защиты;

L — количество средств защиты;

P_{ljk} — эффективность средства защиты — вероятность нейтрализации j-го способа k-й угрозы.

Состав и распределение средств защиты СОБ $N_{iz} = \{n_{liz}\}$ между уязвимостями КВО представим матрицей $S = \{y_{iz}, n_l\}$:

$$S = \begin{vmatrix} & n_1 & . & n_l & . & n_L \\ y_{11} & 1 & 0 & 1 & 1 & 0 \\ . & 1 & 1 & 1 & 1 & 0 \\ y_{iz} & 1 & 1 & 1 & 0 & 0 \\ . & 1 & 0 & 0 & 1 & 1 \\ y_{IZ} & 1 & 0 & 1 & 1 & 0 \end{vmatrix}. \qquad (5)$$

В матрице S каждой уязвимости y_{iz} представлена композиция $N_{iz} = \{n_{liz}\} \subset N \; \forall y_i \in Y$ средств защиты от всех угроз и способов их реализации q_{jk}.

Вся информация, представленная множествами Y_z, Q, M, P и S, должна быть получена при инспек-

торской проверке КВО. Если множества Y_z, Q, M, P и S известны, то задача оценки уязвимости сводится к вычислению рисков нарушения безопасности КВО (R) и его элементов (R_z) на декартовом произведении D множеств M, P и S:

$$D = M \times P \times S =$$
$$= \{(y_{iz}, q_{ijk}, P_{ljk}, n_l) / y_{iz} \in M, y_{iz} \in S, q_{jk} \in M, P_{ljk} \in P, n_l \in S\}. \quad (6)$$

2. Процедура оценки рисков нарушения безопасности КВО

Процедура оценки рисков нарушения безопасности КВО и его элементов состоит из ряда последовательных этапов.

На первом этапе для каждой уязвимости $y_{iz} \in Y$ вычисляется эффективность $P^{jk}_{N_{iz}}$ композиции средств защиты $N_{iz} = \{n_{liz}\} \subset N$ против каждого способа реализации каждой угрозы $q_{izjk} \in M$.

Расчеты проводятся по формуле вероятности сложного события:

$$P^{izjk}_{N_{iz}} = 1 - \prod_{l=1}^{l} (1 - P_{ljk}), \forall n_l \in N_{iz}. \quad (7)$$

Формула (7) и ее инварианты являются операторами последовательного преобразования исходного массива информации D на всех этапах процедуры расчета рисков нарушения безопасности КВО и его структурных составляющих.

Риск нарушения безопасности уязвимости $y_{iz} \in Y$ от реализации каждого способа каждой угрозы $q_{izjk} \in M$ определится выражением

$$R^{izjk}_{N_{iz}} = 1 - P^{izjk}_{N_{iz}}. \quad (8)$$

Результаты расчетов представим матрицей-столбцом $A = \{R^{izjk}_{N_{iz}}\}$:

$$A = \begin{vmatrix} R^{11}_1 \\ . \\ R^{izjk}_{N_{iz}} \\ . \\ R^{IZJK}_{N_{IZ}} \end{vmatrix}. \quad (9)$$

Далее для каждой уязвимости $y_{iz} \in Y$ определяется риск нарушения безопасности R_{iz} от всех угроз и способов их реализации, представленных в профиле защиты:

$$R_{iz} = 1 - \prod_{n=1}^{N} (1 - R^{jk}_{N_{iz}}), \forall R^{izjk}_{iz} \in M. \quad (10)$$

С помощью выражения (8) матрица A преобразуется в матрицу $B = \{R_{iz}\}$:

$$B = \begin{vmatrix} R_{11} \\ . \\ R_{iz} \\ . \\ R_{IZ} \end{vmatrix}. \quad (11)$$

На третьем этапе определяются риски нарушения безопасности R_z элементов КВО от всех угроз и способов их реализации:

$$R_z = 1 - \prod_{1}^{IZ} (1 - R_{iz}). \quad (12)$$

Результаты расчетов формируют матрицу рисков нарушения безопасности элементов КВО $C = \{Rz\}$:

$$C = \begin{vmatrix} R_1 \\ . \\ R_z \\ . \\ R_Z \end{vmatrix}. \quad (13)$$

На четвертом, заключительном, этапе определяется риск R хотя бы одного нарушения безопасности КВО при существующих профиле защиты M и композиции средств защиты S:

$$R = 1 - \prod_{z=1}^{Z} (1 - R_z), \forall R_z \in C. \quad (14)$$

Матрицы A, B, C и численное значение R составляют объективную информацию о защищенности КВО и всех его структурных составляющих при существующей композиции средств защиты S и заданном профиле защиты M.

При проведении инспекции СОБ КВО эксперты часто обнаруживают неизвестные ранее уязвимости, новые угрозы или новые способы реализации известных угроз, которые не представлены в действующем профиле защиты. Эта информация служит для дополнения и корректировки профиля защиты M и матрицы эффективности средств защиты P. Метод оценки уязвимости КВО позволяет оценить влияние неполного соответствия существующей композиции средств защиты S дополненному профилю защиты M и сформулировать требования по корректировке существующей композиции средств защиты.

3. Оценка рисков нарушения безопасности критических инфраструктур

Представленный выше метод оценки уязвимости КВО может быть распространен и на оценку безопасности критических инфраструктур. Рассмотрим применение этого метода на примере расчета рисков нарушения безопасности некоторой гипотетической КИ, например отраслевого министерства. СОБ такой КИ будет иметь три уровня управления — объектовый, региональный и отраслевой. На каждом уровне этой иерархической структуры риск нарушения безопасности хотя бы одного КВО является единым интегральным показателем эффективности звеньев СОБ этого уровня. Для простоты и наглядности расчетов примем, что каждый региональный уровень имеет в своем составе 5 КВО и отрасль имеет КВО в 2 регионах.

Пусть для всех КВО нашего гипотетического КИ проведена оценка уязвимости. Результаты этих расчетов представлены матрицами рисков нарушения безопасности КВО регионов $C^1_{\text{рег}}$ и $C^2_{\text{рег}}$. Для простоты расчетов примем, что в каждом регионе выполнен принцип равной защищенности КВО, т. е. риски нарушения безопасности КВО в каждом регионе одинаковы и составляют для первого региона $R^1_g = 0.1 \forall g \in C^1_{\text{рег}}$, а для второго $R^2_g = 0.05 \forall g \in C^2_{\text{рег}}$, где $g = 1 - G$ — номер КВО; G — число КВО в регионе.

$$C^1_{\text{рег}} = \begin{vmatrix} R^1_1 = 0.1 \\ R^1_2 = 0.1 \\ R^1_3 = 0.1 \\ R^1_4 = 0.1 \\ R^1_5 = 0.1 \end{vmatrix} \quad C^2_{\text{рег}} = \begin{vmatrix} R^2_1 = 0.05 \\ R^2_2 = 0.05 \\ R^2_3 = 0.05 \\ R^2_4 = 0.05 \\ R^2_5 = 0.05 \end{vmatrix}. \qquad (15)$$

Риск нарушения региональной безопасности КИ, т. е. вероятность возникновения ЧС хотя бы на одном КВО региона R^v, рассчитывается с помощью регионального инварианта формулы (3.31):

$$R^v = 1 - \prod_1^G (1 - R^v_g) \forall R^v_g \in C^v_{\text{рег}}. \qquad (16)$$

В нашем примере $V = 2$ и $G = 5$, и с учетом равенства рисков нарушения безопасности КВО региона (3.32) выражение (3.33) запишется:

для первого региона $R^1 = 1 - (1 - 0.1)^5 = 0.4095$;

для второго региона $R^2 = 1 - (1 - 0.05)^5 = 0.2262$.

Риск нарушения безопасности КИ, т. е. вероятность возникновения ЧС хотя бы на одном КВО КИ, определяется выражением

$$R_{\text{КИ}} = 1 - \prod_1^V (1 - R^v) \forall v \in \{v\}. \qquad (17)$$

И в нашем примере

$$R_{\text{КИ}} = 1 - (1 - 0{,}4095) \times (1 - 0{,}2262) = 0{,}5406.$$

В результате проведенных расчетов уязвимости КВО КИ, рисков нарушения безопасности регионов КИ и КИ в целом формируется массив объективной информации о состоянии защищенности всех элементов иерархической структуры отрасли при существующей СОБ. Анализ этой информации позволяет выявлять недостатки СОБ и определять пути ее совершенствования.

Наши расчеты на примере гипотетической КИ показывают, что риски нарушения безопасности регионов КИ и КИ в целом слишком велики при заданных значениях рисков нарушения безопасности КВО. Здесь мы обращаемся к проблеме определения допустимого риска для всех уровней управления безопасностью КИ.

4. Расчет допустимого риска нарушения безопасности КВО

На практике чаще всего значения допустимого риска нарушения безопасности КИ в целом задаются экспертами с учетом последствий возможных ЧС на КВО КИ, возможностей средств и методов обеспечения безопасности КВО и ограничений, связанных с его производственной деятельностью [1].

Если значение допустимого риска нарушения безопасности КИ $R^{\text{доп}}_{\text{КИ}}$ задано, то в соответствии с (17) значение допустимого риска нарушения региональной безопасности $R^{\text{доп}}_{\text{рег}}$ определится выражением

$$R^{\text{доп}}_{\text{рег}} = 1 - \sqrt[v]{(1 - R^{\text{доп}}_{\text{КИ}})}. \qquad (18)$$

Величина допустимого риска КВО согласно (17) запишется

$$R^{\text{доп}}_{\text{КВО}} = 1 - \sqrt[G]{(1 - R^{\text{доп}}_{\text{рег}})}. \qquad (19)$$

Пусть для нашего гипотетического КИ задан допустимый риск нарушения ее безопасности $R_{\text{КИ}}^{\text{доп}} = 0.1$, тогда согласно формулам (18) и (19) допустимые риски нарушения региональной безопасности КИ и безопасности КВО КИ примут значения $R_{\text{рег}}^{\text{доп}} = 0.0513$ и $R_{\text{КВО}}^{\text{доп}} = 0.0105$.

Если задано $R_{\text{КИ}}^{\text{доп}} = 0.1$, то в рамках нашего примера $R_{\text{рег}}^{\text{доп}} = 0.005$ и $R_{\text{КВО}}^{\text{доп}} = 0.001$.

Значение $R_{\text{КВО}}^{\text{доп}} = 0.001$, полученное в нашем гипотетическом примере, близко к допустимым значениям риска нарушения безопасности КВО, закрепленных в ГОСТ для различных критических инфраструктур. Например, в СНиП 33-01-2003 «Гидротехнические сооружения» допустимые риски нарушения безопасности гидротехнических объектов варьируются в пределах от $3 \cdot 10^{-3}$ до $5 \cdot 10^{-5}$ в год в зависимости от класса сооружения.

Заключение

В заключение отметим, что предложенный математический аппарат позволяет организовать итеративную процедуру выбора минимального значения допустимого риска нарушения безопасности КИ в соответствии с возможностями средств и методов обеспечения безопасности КВО. Представленный инструментарий может быть использован и при решении задач синтеза состава (композиции) средств защиты СОБ КВО [2].

Литература

1. Цыгичко В.Н., Черешкин Д.С. Безопасность критически важных объектов транспортного комплекса. Lambert Academic Publishing, 2014. 217 с.
2. Цыгичко В.Н. Управление рисками нарушения безопасности КВО при неполной информации // Проблемы анализа риска. 2015. Т. 12. № 4. С. 18—28.

Сведения об авторе

Цыгичко Виталий Николаевич: доктор технических наук, профессор, главный научный сотрудник Федерального исследовательского центра «Информатика и управление» РАН, Институт системного анализа

Число публикаций: 8 монографий и более 200 статей

Область научных интересов: методологические и методические проблемы математического моделирования социально-экономических процессов, теория принятия решений, прикладной системный анализ, теория и методы социально-экономического прогнозирования, проблемы обеспечения национальной безопасности и стратегической стабильности, проблемы информационной безопасности

Контактная информация:

Адрес: 117312, г. Москва, просп. 60-летия Октября, д. 9

Тел.: +7(499) 135-50-43

E-mail: vtsygichko@inbox.ru