УДК 004.056

А.А. Замула[1], Ю.В. Землянко[2], Г.С. Коваль[3]

[1] *Харьковский национальный университет имени В.Н. Каразина*
[2] *Харьковский государственный университет питания и торговли*
[3] *Харьковский национальный университет радиоэлектроники*

# ОЦЕНКА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ УГРОЗ

*Рассмотрен подход к решению проблемы информационной безопасности на основе получения оценки защищенности информационных систем. Представлена модель ресурсного обеспечения информационной безопасности информационных систем.*

***Ключевые слова:*** *информационная система, угроза, ущерб, информационная безопасность.*

## Введение

Применение информационных технологий (ИТ) требует повышенного внимания к вопросам информационной безопасности [1]. Разрушение информационного ресурса, его временная недоступность или несанкционированное использование могут нанести значительный материальный ущерб компании. Без организации работ по защите информации внедрение ИТ может оказаться экономически невыгодным в результате значительных потерь конфиденциальных данных, хранящихся и обрабатываемых в компьютерных сетях. Реализация решений, обеспечивающих безопасность информационных ресурсов, существенно повышает эффективность всего процесса информатизации в организации, обеспечивая целостность, подлинность и конфиденциальность информации, циркулирующей в локальных и глобальной информационных средах.

Актуальность и важность проблемы обеспечения информационной безопасности обусловлена следующими факторами:

- увеличение рисков информационной безопасности в связи с появлением новых угроз информационной безопасности;
- современные темпы и уровни развития средств информационной безопасности значительно отстают от темпов и уровней развития информационных технологий;
- активным применением ЭВМ в разнообразных сферах человеческой деятельности;
- резкое расширение сферы пользователей, имеющих непосредственный доступ к вычислительным ресурсам;
- доступность корпоративной информации через мобильные устройства (ноутбук, планшет, смартфон);
- значительное увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации;
- стремительное развитие информационных технологий открыло новые возможности эффективной работы организации, однако привело и к появлению новых угроз.

Современные программные продукты находятся в продаже с ошибками и недоработками. Разработчики, включая в свои продукты всевозможные функции, не успевают выполнить качественную проверку и отладку создаваемых программных систем. Ошибки и недоработки, оставшиеся в этих системах, приводят к случайным и преднамеренным нарушениям информационной безопасности.

Оценка защищенности информационных систем позволяет определить, какие мероприятия эффективны для минимизации и предотвращения рисков. На основе анализа защищенности можно определить возможный ущерб от реализации риска, его оценки и рекомендовать необходимые действия.

## Арбитражная модель ресурсного обеспечения информационной безопасности организационных систем

Ключевым элементом управления информационными рисками, является эффективная методология их снижения за счет реализации определенных контрмер, направленных на ликвидацию существующих уязвимостей и угроз. Основой указанной методологии должен стать механизм эффективного использования имеющихся в наличии ресурсов (финансовых, организационных, технологических и т.д.).

Рассмотрим организационную систему (ОС), состоящую из управляющего центра и агентов $\{a_1,...,a_n\}$. Жизненный цикл основных мер по управлению ИБ может иметь следующий вид.

1. Центр устанавливает для *i*-го агента уровень допустимого риска $w_i^* \ge 0, i \in n$, который представляет собой приемлемый сточки зрения центра ущерб от реализации возможных угроз.

2. Центр (или агенты) проводят аудит ИБ и анализ рисков, по результатам которого определяется уровень текущего риска $w_i^0$, $i \in N$, который представляет собой ущерб от реализации возможных угроз до применения каких-либо контрмер, а также уровень остаточного риска $w_i^\infty, i \in N$, который никакими контрмерами не может быть устранен.

3. Агенты $a_i$ сообщают значения $w_i^0, w_i^\infty, i \in n$, центру. Если для некоторого агента $k \in N : w_k^0 \le w_k^*$, то такой агент на данном цикле управления ИБ исключается из рассмотрения.

Для остальных агентов центр на основании установленных значений $w_i^* \ge 0$ и полученных значений $w_k^0, i \in n$, определяет количество ресурсов $b_i \ge 0$, необходимое агенту для снижения текущего уровня риска $w_i^0$ до уровня допустимого риска $w_i^*$. Значение $b_i \ge 0, i \in n$, рассматривается как заявка *i*-го агента. Считаем, что $b_i$ – предполагаемые затраты на создание эффективной системы ИБ (принятие эффективных контрмер).

4. На основании вектора заявок $b = (b_1,...,b_n)$ центр выделяет количество ресурсов $X = X(b)$. Будем предполагать, что $b_1 + ... + b_n \ge X(b)$, т.е. имеет место дефицит ресурса.

5. Центр, в соответствии с некоторым правилом распределяет ресурс X между агентами $a_i : \pi^*(X) = (\pi_1^*(X),...,\pi_n^*(X))$, где $\pi_i^*(X) \ge 0$ – объем ресурса, выделенный i-му агенту. При этом $X(b) \ge \pi_1^*(X) + ... + \pi_n^*(X)$.

6. Агенты реализуют контрмеры в объеме полученного ресурса, после чего цикл управления ИБ повторяется.

Целью центра, управляющего ИБ, является снижение текущих уровней рисков агентов до уровней их допустимых значений.

Пусть задан некоторый объем ресурса X ≥ 0 и распределение данного ресурса $x = (x_1,...,x_n)$, такое, что $x_i \ge 0$. Здесь $x_i$ – ресурс, который затрачивается на реализацию контрмер для снижения риска агентом $a_i$. Сопоставим каждому агенту функцию риска $w_i = w_i(x)$ и предположим, что $w_i(x)$ обладает следующими свойствами:

1. Для $\forall x = (x_1,...,x_n) : w_i(x) \ge 0, i \in N$.

2. $w_i(0,...,0) = w_i^0 \ge 0, i \in N.$

3. Для $\forall x^1 = (x_1^1,...,x_n^1)$ и $x^2 = (x_1^2,...,x_n^2)$, таких, что

$$x^1 \ge x_i^2, i \in N : w_j(x^1) \le w_j(x^2), j \in N, \text{причем},$$

если для некоторого $k : x_k^1 > x_k^2$, то $w_k(x^1) < w_k(x^2)$.

Из свойств 1-3 следует следующее свойство:

4. Для $\forall j \in N \exists w_j^\infty \ge 0$, такое, что $w_j(x) \ge w_j^\infty$, для $\forall x = (x_1,...,x_n) : x_i \ge 0, i \in N$

Более подробную информацию о функции риска можно получить, например, в [2]. Необходимо отметить что, как правило, конкретный вид функции риска лицу, принимающему решение (ЛПР), неизвестен. Детальный анализ свойств 1 – 4 функции риска приводится в [3 ,4]. Далее предполагаем, что для агентов, участвующих в распределении ресурса, выполняется соотношение:

$$0 \le w_k^\infty \le w_k^* < w_k^0.$$

Обозначим $\pi(x) = \left\{ \begin{matrix} \pi(x) = (\pi_1(x),...,\pi_n(x)) : \\ \pi_k(x) \ge 0, k \in N, x \ge \sum_{k=1}^n \pi_k(x) \end{matrix} \right\}$ – множество возможных распределений ресурса X между агентами.

Предположим, что ЛПР известен конкретный вид функций риска для всех агентов. Тогда оптимальное распределение ресурса может быть найдено как решение следующей задачи:

$$\max_{i \in N} w_i(\pi(x)) \to \min_{\pi(x) \in \Pi(x)},$$

это будет подмножество дележей $\pi^*(X)$, таких, что

$$\pi^*(X) = \arg \min_{\pi(x) \in \Pi(x)} \max_{i \in N} w_i(\pi(x))$$

Обозначим

$$\pi^*(X) = \left\{ \pi^*(X) = (\pi_1^*(X),...,\pi_n^*(X)) \right\} \subseteq \pi(X)$$ – множество распределений, являющихся решением задачи.

Решение задачи может быть получено традиционными методами [6], при известных ЛПР функциях риска $w_i(.), i \in N$. Однако, если конкретный вид функций риска агентов неизвестен $b_i \ge 0, i \in N$, то задача усложняется.

Утверждение 1. Пусть $w_i(.), i \in N$, удовлетворяют свойствам 1-4, и существует распределение $\pi(X) = (\pi_1(X),...,\pi_n(X)) \in \pi(X)$, такой, что $X = \sum_{k=1}^n \pi_k(X)$ и

$$w_i(\pi_1(X),...,\pi_n(X)) = c = \text{const}, \text{ для } \forall i \in N.$$

Тогда $\pi(X)$ – единственное решение задачи.

Утверждение 1 показывает, что цель управления ИБ с точки зрения центра может быть сведена к задаче поиска распределенТия ресурса, приводящего к выравниванию уровней текущих информационных рисков всех агентов на текущем цикле организационного управления. Решение указанной задачи должно представлять собой единое для всех циклов управления ИБ правило распределения ресурса между агентами (организационный механизм управления ИБ), зависящее от заявок агентов.

## Нечеткая оценка защищенности информационных систем

Защищенность информационных систем определяется исходя из ущерба организации, связанного с реализацией угроз, носящих случайный характер [5]. Коэффициенты опасности представляются нечеткими величинами, а показатель защищенности ИС определяется посредством матрицы нечетких отношений между коэффициентом опасности множества угроз и степенью защищенности ИС.

Подход к оценке эффективности технической защиты информации (ТЗИ) в информационных системах основан на сравнении показателей защищенности без применения ТЗИ и с применением ТЗИ в условиях нечеткого представления о степени опасности комплекса антропогенных и техногенных угроз.

Под эффективностью понимают меру достижения цели ТЗИ. Оценка эффективности ТЗИ – процесс установления соответствия между результатом защиты и поставленной целью. С ростом сложности объектов анализа, состава и характеристик угроз (особенно угроз несанкционированного удаленного доступа) задача количественной оценки защищенности актуальна. Оценка эффективности ТЗИ возможна: 1) на основе сравнения значения показателя защищенности с нормативным (пороговым) значением; 2) на основе сравнения показателей защищенности информации без ТЗИ и в условиях ТЗИ. Оба подхода применяются на уровне частных моделей и методик. Для комплексной оценки эффективности первый подход является мало приемлемым, т. к. сложно определить допустимые уровни снижения защищенности информации от комплекса угроз. Второй подход применим при сравнительном анализе эффективности мер и средств защиты информации и не позволяет определить достаточность ТЗИ.

Если защищенность информации оценивается показателем $Э_{ОТИ}(t)$ без принятия мер защиты и $\mu_{ТЗИ}(t)$ в условиях ТЗИ, то эффективность ТЗИ может быть оценена относительным показателем

$$Э_{ОТИ}(t)=\frac{\mu_{ТЗИ}(t)-\mu_0(t)}{\mu_0(t)},\mu_0(t)>0.$$

Пусть известны возможные угрозы безопасности информации в ИС и любая из этих угроз проявляется и реализуется за рассматриваемый период t с некоторой вероятностью $P_{реал.u}(t)$. Ущерб $D_u$ от реализации u-й угрозы является величиной случайной, распределенной в интервале $[0,D_{пр}]$, где $D_{пр}$ — уровень ущерба, превышение которого неприемлемо. Если ущерб от реализации угрозы превышает $D_{пр}$, то он принимается равным $D_{пр}$. Отношение $D_u/D_{пр}$ будет характеризовать уровень опасности u-й угрозы и вероятность, что ущерб будет не более $D_u$. Вероятность, что уровень ущерба при реализации совокупности n из U возможных угроз не превысит величину $D_{\sum n}$:

$$\frac{D_{\sum n}}{D_{пр}}=-\frac{1}{n!}\frac{\partial^n}{\partial\lambda^n}\prod_{u=1}^{U}\left[(1-P_{реал}(t))+\lambda\frac{D_u}{D_{пр}}P_{реал}(t)\right]_{\lambda=0}$$

или

$$K_{\sum n}=-\frac{1}{n!}\frac{\partial^n}{\partial\lambda^n}\prod_{u=1}^{U}\left[(1-P_{реал}(t))+\lambda K_u P_{реал}(t)\right]_{\lambda=0},$$

где λ – вспомогательный параметр, $K_{\sum n}$ и $K_n$ – отношения соответственно $D_{\sum n}$ и $D_u$ к $D_{пр}$ назовем коэффициентами опасности угроз, так как они соответствуют уровню наносимого ущерба, вплоть до неприемлемого.

Если рассматривать все U угроз и учесть, что коэффициенты опасности являются функциями времени, то последняя формула преобразуется к виду

$$K_{\sum}(t)=1-\prod\left[(1-K_u(t)P_{реал}(t)\right],u=\overline{1,U}.$$

Мера опасности угрозы - четко заданная величина либо нечеткая величина, характеризующая суждение эксперта об опасности угрозы. В первом случае защищенность ИС оценена показателем — «степень защищенности»

$$\eta(t)=1-\prod_u\left[(1-K_u(t)P_{реал}(t)\right],u=\overline{1,U}.$$

Данный показатель позволяет оценить эффективность ТЗИ как по всему множеству угроз, так и подмножеству угроз, составляющих определенную направленность: нарушение целостности, доступности или конфиденциальности информации. Достоинство показателя — полиморфизм, исключающий корректировку методов расчета в зависимости от состава угроз.

Определение коэффициентов опасности угроз в виде четких значений основано на аналитических соотношениях, связывающих эти коэффициенты с показателями ценности информации. Такие показатели в виде коэффициентов важности могут быть определены на основе эвристического анализа и категорирования информации в ИС по важности. Пусть информация на объекте информатизации представлена в виде файлов и для каждого файла пользователь устанавливает категорию важности информации. Например, введены 4 категории важности информации: 1 — особо важная, 2 — очень важная, 3 — важная, 4 — маловажная. При этом все угрозы разделяются на 3 группы: нарушение целостности, доступности и конфиденциальности информации. Пользователем эвристически определяются коэффициенты важности f-го файла $Vz(t,f)<1$, относящегося к z-й категории.

Применительно к нарушению

конфиденциальности информации соотношение для расчета коэффициентов опасности u-й угрозы имеет вид

$$K_u(t) = 1 - \prod_{z=1}^{Z_u} \prod_{f=1}^{F_z} \left[1 - V_u(t,f)\right], z = \overline{1, Z_u},$$

а для угроз, направленных на нарушение целостности и доступности информации, или для комплексных угроз коэффициент опасности

$$K_u(t) = 1 -$$

$$- \prod_{z=1}^{Z_u} \prod_{f=1}^{F_z} \left\{1 - V_z(t,f) \times \left[1 - P_{восст,f}(t)\right]\right\}, z = \overline{1, Z_u},$$

где $Z_u$ — количество категорий важности информации, для которой u-я угроза представляет опасность; $F_z$ — количество подлежащих защите файлов в системе, имеющих z-ю категорию важности; $P_{восст.f}(t)$ — вероятность восстановления за рассматриваемый период времени t целостности (доступности) информации, содержащейся в f-м файле (если файл не подвержен воздействию или коэффициент важности содержащейся в нем информации равен нулю, то эта вероятность тождественно равна 1).

При определении коэффициентов опасности угроз в виде нечетких величин необходимо проводить экспертный анализ опасности угроз. Такой подход может оказаться наиболее адекватным реальной опасности угроз, если анализ осуществляется высококвалифицированными специалистами. Как правило, различные эксперты по-разному оценивают значение параметра и часто затрудняются задать конкретное число, поскольку существует много факторов, влияющих на оцениваемые величины и имеющих вероятностную природу. Для подобных ситуаций используется аппарат нечетких множеств, коэффициенты опасности задаются в виде нечетких чисел, способных принимать свои значения из определенного заданного интервала (множества) с различными значениями функций принадлежности [6].

Коэффициент опасности каждой угрозы описывается функцией принадлежности треугольной формы [7] (рис. 1).

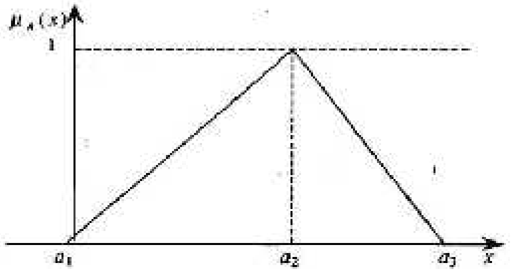

Рис. 1. Треугольное представление нечеткого числа

Представляется тройкой чисел, определяющих левую и правую границу области определения, а также значение, соответствующее максимальной истинности коэффициента опасности угрозы. Значения функции принадлежности $\mu_A(x)$ для этих точек задаются так, что для средней точки это значение наибольшее, а остальные два являются нулевыми.

В соответствии с теорией нечетких множеств операции над значениями коэффициентов опасности $K_и$ заменяются операциями над их функциями принадлежности $\mu_{Ku}(K_{ui})$. При обработке результатов опроса экспертов функция принадлежности может потерять треугольный вид.

Для случая задания коэффициентов опасности угроз нечеткими числами формула для показателя «степень защищенности» запишется в виде

$$\eta(t) = \prod_{u=1}^{U} \left[(1 - K_u(t) P_{ðåàë}(t)\right].$$

где операция умножения нечетких чисел производится по следующему правилу:

$$\mu_D(t) = \mathrm{sap}\min \mu_A(a)\mu_B(b), a \times b = x.$$

Назовем нечеткое множество $K_\Sigma$, характеризующее опасности в ИС, пространством опасности (угроз) системы. Если между коэффициентом опасности множества угроз и показателем «степень защищенности» ИС имеется четкая зависимость, то она может быть представлена в простом виде

$$\eta(t) = 1 - K_\Sigma(t).$$

Часто соотношение между коэффициентом опасности совокупности угроз и степенью защищенности ИС оказывается приблизительным. В этом случае необходимо определить причинные отношения между значениями этого коэффициента (предпосылками) и конечным результатом — степенью защищенности $\eta$ (заключениями). Для этих целей как ключевой момент методики экспертного оценивания эффективности средств технической защиты информации вводится матрица нечетких отношений R размерностью n * m. В матрица нечетких отношений заключены правила, определяющие причинные отношения между каждым членом предпосылок $K_\Sigma$ и каждым членом заключений $\eta(t)$ [7]

$$R = K_\Sigma \to \eta.$$

Элементы матрицы $r_{ij} = \mu_R(K_\Sigma, \eta)$ должны отражать нечеткие отношения между $K_\Sigma$ и $\eta_i$. Величину R можно рассматривать как нечеткое пространство на прямом произведении $K_\Sigma * \eta$ полного пространства предпосылок $K_\Sigma$ и полного пространства заключений $\eta$, а процесс получения нечеткого результата $\eta$ с использованием данных $K_\Sigma$ и знания $K_\Sigma^{эт} \to \eta^{эт}$ (эталонного преобразования) можно представить в виде:

$$\eta(t) = K_{\Sigma}(t)\left(K_{\Sigma}^{эт}(t) \to \eta^{эт}(t)\right),$$

где знак • определяет операцию «max-min» композиции в качестве композиционного правила нечеткого вывода и операции взятия минимума в качестве нечеткой импликации

$$\mu_D(\eta) = \max_{K_{\Sigma}}\left\{\min\left(\mu_{K_{\Sigma}}(K_{\Sigma}), \mu_R(K_{\Sigma}, \eta)\right)\right\}.$$

Размерность матрицы нечетких отношений определяется количеством заданных числовых градаций коэффициента опасности и порогов функции принадлежности. Корректная формализация правил, с помощью которых формируется эта матрица, определит точность и достоверность конечного результата, являющегося выводом системы экспертного оценивания.

Возможны несколько вариантов построения правил вывода в зависимости от важности объекта информатизации и отношения к нему экспертов. Однако наиболее широко в экспертных оценках [7] используется набор правил, основанный на определении связи коэффициента $K_{\Sigma}$ и показателя защищенности системы $\eta$ в виде пропорциональной зависимости с равномерным уменьшением достоверности оценки. В простейшем случае значения элементов матрицы нечеткого вывода рассчитываются по формуле

$$r_{ij} = \begin{cases} k_{\Sigma i} + \eta_j, \text{если\_эта сумма\_меньше;} \\ 0, \text{в\_противном\_случае.} \end{cases}$$

Оценить эффективность ТЗИ можно, определяя степень защищенности $\eta(t)$ в условиях отсутствия и применения мер ТЗИ. Для этого осуществляют дефаззификацию [8] одним из следующих способов;

1) задавшись требуемым уровнем функции принадлежности $\mu_{\eta}(\eta)$, проводят отсечение и выбирают первое приемлемое значение $\eta$

$$\eta_a = \{\eta_i \mid \mu_{\eta}(\eta_i) \geq a\}.$$

2) проводят отсечение по способу 1 и берут два крайних значения $\eta_н$ и $\eta_к$. Тогда значение коэффициента защиты будет определяться как:

$$\eta = \frac{\eta_н \mu_{\eta}(\eta_н) + \eta_к \mu_{\eta}(\eta_к)}{\mu_{\eta}(\eta_н) + \mu_{\eta}(\eta_к)}$$

со степенью достоверности:

$$\mu_{\eta}(\eta) = \mu_{\eta}(\eta_í) \times \mu_{\eta}(\eta_ê).$$

Зная нечеткие значения и функции принадлежности коэффициентов опасности угроз, можно с учетом вероятностей реализации угроз по правилам теории нечетких множеств рассчитать нечеткие значения степени защищенности объекта информатизации от комплекса угроз. Недостатками подобного оценивания являются статичность оценки защищенности и отсутствие взаимосвязи показателей защищенности с местоположением МЗ в структуре системы информационной безопасности (СИБ).

## Комплексная оценка защищенности информационных систем

Динамичный характер оценки защищенности ИС обеспечивает модель адаптивной СИБ [9]. Одним из компонентов СИБ является блок расчета показателей защищенности, который совместно с методикой оценки защищенности ИС, позволяет:

- обеспечить близкое к оптимальному отношение «стоимость/эффективность» СИБ за счет использования только необходимых МЗ;
- отслеживать динамику использования МЗ при изменении множества угроз;
- формировать спецификацию требований на отсутствующие МЗ;
- оценивать защищенность ИС через величины ожидаемого ущерба и интегральные показатели активности МЗ, распределенных по СИБ.

Решение о расширении классификаций угроз и МЗ производится в соответствии с системой оценок достоверности нейтрализации угроз в разрезе отдельных МЗ или уровней СИБ и аналогичных оценок предполагаемого ущерба, соотносимых с отдельными МЗ или уровням СИБ. Ущерб рассматривается в относительных величинах, к примеру, по отношению к значению допустимого ущерба в ИС хозяйствующего субъекта.

Результаты экспертных оценок представляют в виде матрицы достоверности «угрозы – уровни СИБ»:

$$ME_{n \times m} = \begin{pmatrix} me_{11} & me_{12} & \vdots & me_{1n} \\ me_{21} & me_{22} & \vdots & me_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ me_{m1} & me_{m2} & \vdots & me_{mn} \end{pmatrix},$$

где m – число механизмов защиты, n - число уровней СИБ.

Активность уровня СИБ по нейтрализации угроз, входящих в систему предикатных правил в качестве посылок, определяют строкой интегральных показателей строкой показателей значимости уровня в структуре СИБ:

$$x_j = \sqrt{\sum_{j=1}^{m} me_{ij}}, \ j = \overline{1,n},$$

нормированных по значению максимального из $x_{i,j} = \overline{1,n}$ или по значению суммы элементов строки показателей значимости $\sum_{j=1}^{m} x_{i,j} = \overline{1,n}$. Сопоставление интегральных показателей в пределах строки позволяет выявить наиболее активные уровни модели СИБ по нейтрализации угроз.

Аналогично можно получить столбец интегральных показателей активности использования механизма защиты на всех уровнях

СИБ:

$$x_j = \sqrt{\sum_{j=1}^{n} me_{ij,}} \; i = \overline{1, n} \;,$$

Сопоставление интегральных показателей в пределах столбца дает возможность выявить наиболее активно используемые МЗ в структуре СИБ. Анализ интегральных показателей позволяет обосновать целесообразность использования МЗ в составе соответствующего уровня СИБ.

Использование экспертных оценок и отражение в структуре сети опыта экспертов ИБ сопровождают проверкой на непротиворечивость результатов опроса экспертов. Непротиворечивость экспертных оценок может быть обеспечена применением, например, метода экспертных оценок матрицы нечетких отношений [5] или метода на основе расчета максимального собственного значения матрицы парных сравнений [9].

Приведенные показатели будут более информативными, если учитывать не только достоверность использования МЗ в структуре СИБ, но и показатели предполагаемого ущерба, возникающего при реализации угроз в ИС и который может быть предотвращен системой информационной безопасности.

С этой целью оценку защищенности можно косвенно связать с предотвращением ущерба и использовать экспертные оценки для сопоставления множества угроз с потенциальным ущербом от их реализации и размера ущерба с местом реализации угрозы в структуре ИС.

Проведенный анализ показал необходимость разработки обобщенного количественного показателя для оценки свойства «защищенность» ИС, который должен объединить положительные стороны известных подходов с целью его дальнейшего использования в качестве целевой функции для оптимизации структуры информационной системы по критерию «стоимость/защищенность».

Кроме того, необходима разработка процесса двухступенчатой оптимизации средств мониторинга безопасности ИС, включающего:

- оптимизацию набора функций безопасности объекта оценки в условиях бюджетных ограничений;
- оптимизацию размещения механизмов защиты в структуре системы информационной безопасности по критерию максимизации рейтингового показателя защищенности ИС.

## Выводы

С ростом сложности объектов информатизации, изменением множества и характера угроз информационной безопасности, особенно угроз несанкционированного удаленного доступа к ресурсам и процессами критических информационных систем, задача количественной оценки защищенности является актуальной.

Корректная оценка защищенности критических информационных систем необходима для выполнения сравнения аналогичных по назначению и уровню сложности систем либо для мониторинга динамики уровня защищенности конкретной информационной системы во времени.

## Список литературы


1. *Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. - М.: ИД "ФОРУМ": ИНФРА-М, 2008. - 416с.*
2. *Буянов В.П. Рискология (управление рисками. / В.П. Буянов, К.А. Кирсанов, Л.М. Михайлов. – М.: Экзамен, 2003. – 384 с*
3. *Калашников А.О. Управление информационными рисками с использованием арбитражных схем // Системы управления и информационные технологии. – 2004, – № 4 (16). – С. 57 – 61.*
4. *Калашников А.О. Управление информационными рисками с использованием математического аппарата арбитражных схем/ Мат. Межд. конф. и российской научн. шк. «Системные проблемы надежности, качества информационных и электронных технологий. Информационные бизнес системы». – М.: Радио и связь, 2004. Ч. 3. С. 166 – 174.*
5. *К оценке эффективности защиты информации в телекоммуникационных системах посредством нечетких множеств / Жижелев А.В., Панфилов А.П и др. // Изв. вузов. Приборостроение. 2003. т. 46, № 7. С. 22 - 29.*
6. *Кофман А. Введение в теорию нечетких множеств. – М.: Радио и связь, 1982.*
7. *Асаи К., Ватада Д., Иваи С.И др. Прикладные нечеткие системы / Под ред. Т. Тэрано, К. Асаи, М. Сугэно. – М.: Мир, 1993.*
8. *Нестерук Г.Ф., Молдовян А.А., Осовецкий Л.Г. и др. К разработке модели адаптивной защиты информации // Вопросы защиты информации. 2005, № 3. С. 11 – 16.*
9. *Базы данных. Интеллектуальная обработка информации / Корнеев В.В., Гареев А.Ф., Васютин С.В., Райх В.В.. – М.: Нолидж, 2001.*


*Надійшла до редколегії 4.09.2013*

**Рецензент:** д-р техн. наук, проф. В.А. Краснобаев, Полтавский национальный технический университет, Полтава.

## ОЦІНКА ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ ВІД ЗАГРОЗ

О.А. Замула, Ю.В. Землянко, Г.С. Коваль

*Розглянуто підхід до вирішення проблеми інформаційної безпеки методом отримання оцінки захищеності інформаційних систем. Представлена модель ресурсного забезпечення інформаційної безпеки організаційних систем.*

***Ключові слова:*** *інформаційна система, загроза, збиток, інформаційна безпека.*

## ASSESS THE SECURITY OF INFORMATION SYSTEMS THE THREAT OF DAMAGE

A.A. Zamula, Yu.V. Zemlyanko, G.S. Koval

*An approach to solving the problem of information security evaluation method of obtaining information systems security. The model of resource information security organizational systems.*

***Keywords:*** *information system, the threat of damage, information security.*