References

1. Maslov O.N. *Sluchaynye antenny: teoriya i praktika* [Random antennas: theory and practice]. Samara, PGUTI-OFORT Publ., 2013. 480 p.
2. Maslov O.N., Rakov A.S., Silkin A.A. Statistical characteristics of the field of an array of random aperture antennas. *Journal of Communications Technology and Electronics*, 2013, vol. 58, no. 11, pp. 1093-1101. doi: 10.1134/S1064226913110107.
3. Maslov O.N., Rakov A.S., Silkin A.A. Statistical models of the wave field of a random aperture antenna. *Journal of Communications Technology and Electronics*, 2015, vol. 60, no. 6, pp. 642-649. doi: 10.1134/S1064226915030146.
4. Maslov O.N., Rakov A.S., Silkin A.A. Statisticheskie harakteristiki polya aperturnoy sluchaynoy antenny s uchetom korrelyacionnoy svyazi mezhdu oshibkami [Statistical characteristics of field of aperture random antenna with allowance for correlation between errors]. *Antenny*, 2012, no. 12, pp. 3-10.
5. Krasilnikova E.P., Maslov O.N., Rakov A.S. Modelirovanie statisticheskih harakteristik elektromagnitnogo polya aperturnoy sluchaynoy antenny [Modelling of electromagnetic performance of aperture random antenna]. *Infokommunikacionnye tehnologii*, 2014, vol. 12, no. 2, pp. 78-86.
6. Maslov O.N., Rakov A.S. Kompleksnoe modelirovanie statisticheskih harakteristik polya aperturnoy sluchaynoy antenny [Complex modeling of statistical characteristics of the aperture random antenna field]. *Antenny*, 2015, no. 2, pp. 41-49.
7. Maslov O.N. Primenenie metoda statisticheskogo imitacionnogo modelirovaniya dlya issledovaniya sluchaynyh antenn i proektirovaniya sistem aktivnoy zaschity informacii [Statistic imitation modeling method for random antennas investigation and active information security systems projecting application]. *Uspehi sovremennoy radioelektroniki*, 2011, no. 6, pp. 42-55.
8. Maslov O.N. Nizkoenergeticheskaya informacionnaya zaschita sluchaynyh antenn [Low-energy information protection of random antennas]. *Elektrosvyaz*, 2014, no. 1, pp. 32-38.
9. Maslov O.N. Modul-retranslyator dlya nizkoenergeticheskoy informacionnoy zaschity sluchaynyh antenn [Module-repeater for low-energy information protection of random antennas]. *Elektrosvyaz*, 2015, no. 1, pp. 40-45.
10. Maslov O.N., Rakov A.S. Apertury utechki informacii: analiz, modelirovanie, zaschita [Aperture of information leaks: analysis, modeling, protection]. *Zaschita informacii. Insayd*, 2015, no.1, pp. 30-33.
11. Maslov O.N. *Ustoychivye raspredeleniya i ih primenenie v radiotehnike* [Stable distributions and their applications in radio engineering]. Moscow, Radio i svyaz Publ., 1994. 152 p.
12. Kocherzhevskiy G.N. *Antenno-fidernye ustroystva* [Antenna-feeder devices]. Moscow, Svyaz Publ., 1972. 472 p.

Received 16.03.2015

УДК 543.42:005.056

МЕТОД УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СЕТЯХ

Аникин И.В.
Казанский национальный исследовательский технический университет им. А.Н. Туполева, Казань, РФ
E-mail: anikinigor777@mail.ru

Статья посвящена разработке метода управления рисками информационной безопасности в корпоративных информационных сетях. Метод основан на оценке эффективности реализуемых защитных мер в условиях существующих финансовых ограничений. Для решения задач оптимизации на этапе управления рисками используется генетический алгоритм.

Ключевые слова: информационная безопасность, оценка рисков, нечеткая логика, метод анализа иерархий.

Введение

В настоящее время эффективность функционирования современных предприятий напрямую зависит от степени защищенности корпоративных информационных сетей (КИС), посредством которых осуществляется автоматизация бизнес-процессов. Роль деструктивных факторов для современных КИС значительно выросла, а их растущая сложность только усугубляет ситуацию. В связи с этим защита информации должна

рассматриваться как неотъемлемая составляющая корпоративных информационных сетей современных предприятий. Известны два основных подхода [1] к обеспечению информационной безопасности КИС – обеспечение базового уровня информационной безопасности (ИБ), а также подход, основанный на оценке и управлении рисками ИБ. Основными задачами первого подхода являются: убедиться в том, что компоненты КИС удовлетворяют всем обязательным требованиям стандартов и нормативных документов, а также в том, что компоненты КИС защищены от всех видов основных угроз. Подход, основанный на оценке и управлении рисками ИБ, как правило, реализуется после обеспечения базового уровня безопасности КИС. Он приобретает особую значимость и актуальность при построении эффективных систем защиты информации с позиции ожидаемого ущерба. В настоящей статье рассматривается вопрос защиты КИС с позиции оценки и управления рисками.

Под риском ИБ понимают потенциальную опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимости [2]. Основными факторами риска ИБ являются: возможность реализации угрозы, возможность использования уязвимости, ущерб от реализации угрозы. Выделяют два подхода к оценке рисков ИБ – качественную оценку [2-3] и количественную оценку [4-5]. Преимуществами методов количественной оценки рисков ИБ являются их хорошая интерпретируемость в рамках экономических моделей и простота применения математического аппарата для формирования оптимальной совокупности защитных мероприятий. В связи с этим данные методы в последнее время приобретают особую актуальность. Однако практическое применение методов количественной оценки и управления рисками ИБ в КИС часто затрудняется следующими обстоятельствами:

- данные методы сложны в использовании и требуют глубокого анализа всех процессов, происходящих в КИС;
- количественные оценки факторов риска часто являются неточными, поскольку зависят от глубины анализа КИС и квалификации эксперта; кроме этого, эксперты часто не могут сформировать точные оценки в связи с нечеткой природой оцениваемых объектов, недостаточностью и неопределенностью исходной информации;
- факторы риска часто имеют не количественный, а качественный характер, их сложно оценить в количественном виде;
- отсутствует статистика по реализации ряда угроз, что затрудняет применение аналитических методов для оценки вероятности их реализации.

В связи с этим большую актуальность приобретает разработка методов количественной оценки и управления рисками ИБ, преодолевающих выше перечисленные сложности. Решению данной задачи посвящена настоящая статья.

Нечеткая количественная оценка рисков ИБ в КИС

Нечеткая количественная оценка рисков ИБ в КИС осуществляется на основе моделей и методов, предложенных автором в [5-9]. Разработанная модель КИС включает в себя информационные активы, автоматизированные рабочие места (АРМ), серверы, телекоммуникационное оборудование и ИТ-сервисы. Модель представляет собой следующий набор элементов:

$$M_{КИС} = \left\langle \left\langle A_{инф}, C_{инф} \right\rangle, TO, \left\langle A_{ИТС}, C_{ИТС} \right\rangle \right\rangle, \quad (1)$$
$$, G_{ЛС}, M_{ИО}, M_{ИТС}$$

где $A_{инф}$ – множество информационных активов; $C_{инф}$ – уровни конфиденциальности, целостности и доступности информационных активов; TO – компонент технического обеспечения КИС, включающий в себя АРМ, серверы, телекоммуникационное оборудование и уровни их критичности; $A_{ИТС}$ – множество ИТ-сервисов; $C_{ИТС}$ – их уровни критичности (по доступности); $G_{ЛС}$ – логическая структура КИС, представленная в виде графа, вершинами которого являются сегменты КИС и телекоммуникационное оборудование, а ребра соответствуют каналам связи в КИС; $M_{ИО}$ – модель использования информационного обеспечения КИС, определяющая факты хранения и обработки информации на АРМ и серверах КИС, факты предоставления информации конкретным ИТ-сервисом и информационные потоки в $G_{ЛС}$; $M_{ИТС}$ – модель предоставления ИТ-сервисов, определяющая деревья зависимостей ИТ-сервисов КИС с точки зрения доступности, и факты реализации ИТ-сервисов на базе конкретного технического обеспечения. Разработанная модель КИС позволяет достаточно глубоко анализировать процессы, происходящих в КИС, учитывать взаимодействие активов. Данная модель используется непосредственно для оценки факторов риска ИБ.

Для каждой угрозы T_i из множества угроз T в КИС нечеткая оценка риска ИБ $Risk(T_i)$ осуществляется в виде нечеткого числа в следующем виде:

$$Risk(T_i) = Impact(T_i) \cdot Poss(T_i) \cdot Poss(v_j), \quad (2)$$

где $Impact(T_i)$ – нечеткая количественная оценка ущерба от реализации угрозы T_i; $Poss(T_i)$ – нечеткая количественная оценка возможности реализации угрозы T_i; $Poss(v_j)$ – нечеткая количественная оценка возможности использования уязвимости v_j.

Для нечеткой количественной оценки ущерба $Impact(T_i)$ в условиях разброса экспертных мнений и качественного характера частных показателей используются разработанный метод количественной оценки частных показателей ущерба, основанный на методе анализа иерархий, а также методы теории нечетких множеств (в частности, разработанный алгоритм FZ_STAT формирования функции принадлежности на основе множества экспертных оценок) и алгоритм нечеткой экспертной оценки критичности активов [9].

Для нечеткой количественной оценки возможности реализации угрозы $Poss(T_i)$ в условиях разброса экспертных мнений и качественного характера частных показателей разработан метод [6; 8], основанный на построении опросных листов (аналогичных CRAMM), количественной оценки частных показателей с помощью метода анализа иерархий, а также множестве экспертных оценок, на базе которых формируется функция принадлежности.

Для количественной оценки возможности использования уязвимости $Poss(v_j)$ разработана нечетко-продукционная модель представления знаний и схема нечеткого логического вывода [7], позволяющая эксперту формировать нечеткие оценки частных показателей, принимать решения в условиях отсутствия части информации об уязвимости, учитывающая важность частных показателей.

Предложенный подход позволяет формировать количественные оценки рисков ИБ в условиях выше перечисленных сложностей.

Метод управления рисками ИБ в КИС

Управление рисками информационной безопасности в КИС включает в себя реализацию следующих основных шагов.

1. Оценка рисков ИБ с учетом множества защитных мер. Предлагается рассматривать модель защитных мер КИС в следующем виде:

$$M_{СЗИ} = \left\langle Z, R_{СЗИ}^{уязв}, R_{СЗИ}^{угр}, R_{СЗИ}^{ущерб\_C}, R_{СЗИ}^{ущерб\_I}, R_{СЗИ}^{ущерб\_D} \right\rangle, \quad (3)$$

где $Z = \{z_i\}_{i=1}^{n}$ – множество защитных мер; $R_{СЗИ}^{уязв} : \{Z \times A_{уязв}\} \to F([0,1])$ – задаваемое в виде матрицы отображение, определяющее уровни снижения возможности использования уязвимостей множества $A_{уязв}$ в результате реализации защитных мер $z_i \in Z$ – данные уровни определяются в виде нечетких чисел $\tilde{k} \in F([0,1])$; $R_{СЗИ}^{угр} : \{Z \times A_{угр}\} \to F([0,1])$ – задаваемое в виде матрицы отображение, определяющее уровни снижения возможности реализации угроз множества $A_{угр}$ в результате реализации защитных мер $z_i \in Z$ – данные уровни определяются в виде нечетких чисел $\tilde{p} \in F([0,1])$.

Отображения $R_{СЗИ}^{ущерб\_C}$, $R_{СЗИ}^{ущерб\_I}$, $R_{СЗИ}^{ущерб\_D}$: $\{Z \times A_{угр}\} \to F([0,1])$ задаются в виде матриц и определяют уровни снижения ущерба от реализации угроз множества $A_{угр}$ в результате реализации защитных мер $z_i \in Z$ по конфиденциальности, целостности и доступности соответственно. Данные уровни определяются в виде нечетких чисел $\tilde{c}^C, \tilde{c}^I, \tilde{c}^D \in F([0,1])$ соответственно. Значения коэффициентов $\tilde{k}, \tilde{p}, \tilde{c}^C, \tilde{c}^I, \tilde{c}^D$ формируются экспертным путем.

Под $Poss(v_j)_Z$ будем понимать возможность использования уязвимости v_j с учетом множества защитных мер Z, под $Poss(T_i)_Z$ – возможность реализации угрозы T_i с учетом множества защитных мер Z, под $Impact(T_i)_Z$ – ущерб, связанный с реализацией угрозы T_i с учетом множества защитных мер Z, а под $Risk(T_i)_Z$ – уровень риска с учетом множества защитных мер Z. Ниже вводится метод нечеткой количественной оценки риска ИБ для угрозы T_i с учетом множества защитных мер $z_i \in Z$.

Шаг 1. Оценка возможности использования уязвимости с учетом множества защитных мер

$$Poss(v_j)_Z = Poss(v_j, \hat{z}_1) = Poss'(v_j) \cdot \min_{z \in Z}(1 - R_{СЗИ}^{уязв}(v_j, z)),$$

где $Poss'(v_j)$ – возможность использования уязвимости v_i без учета реализации защитных мер; $Poss(v_j, \hat{z}_1)$ – возможность использования уязвимости v_j с учетом реализации защитной меры $\hat{z}_1 \in Z$, для которой значение $1 - R_{СЗИ}^{уязв}(v_j, z)$ является минимальным.

Шаг 2. Оценка возможности реализации угрозы T_i с учетом множества защитных мер Z

$$Poss(T_i)_Z = Poss(T_i, \hat{z}_2) =$$

$$Poss'(T_i) \cdot \min_{z \in Z}\left(1 - R_{СЗИ}^{\text{угр}}(\mathrm{T_i}, \mathrm{z})\right),$$

где $Poss'(T_i)$ - возможность реализации угрозы T_i без учета реализации защитных мер, $Poss(T_i, \hat{z}_2)$ - возможность реализации угрозы T_i с учетом реализации защитной меры $\hat{z}_2 \in Z$, для которой значение $1 - R_{СЗИ}^{\text{угр}}(\mathrm{T_i}, \mathrm{z})$ является минимальным.

Шаг 3. Оценка уровня ущерба, связанного с реализацией угрозы T_i, с учетом множества защитных мер Z

$$Impact(T_i)_Z = \widetilde{cc}(T_i)_Z + \widetilde{ci}(T_i)_Z + \widetilde{cd}(T_i)_Z,$$

где $\widetilde{cc}(T_i)_Z$ – количественная оценка суммарного ущерба, наносимого угрозой T_i по конфиденциальности, после реализации множества защитных мер Z; $ci(T_i)_Z$ – количественная оценка суммарного ущерба, наносимого угрозой T_i по целостности, после реализации множества защитных мер Z; $\widetilde{cd}(T_i)_Z$ – количественная оценка суммарного ущерба, наносимого угрозой T_i по доступности, после реализации множества защитных мер Z, а также

$$\widetilde{cc}(T_i)_Z = \widetilde{cc}(T_i, \hat{z}_3) =$$

$$= \sum_{a^j \in A^C(T_i)} \widetilde{pc}^{\,j}(T_i) \cdot \widetilde{cc}_{a^j} \cdot \left(1 - \max_{z \in Z} R_{СЗИ}^{\text{ущерб\_C}}(T_i, z)\right),$$

где $\widetilde{cc}(T_i, \hat{z}_3)$ – количественная оценка суммарного ущерба, наносимого угрозой T_i по конфиденциальности, после реализации защитной меры $\hat{z}_3 \in Z$, для которой значение $R_{СЗИ}^{\text{ущерб\_C}}(T_i, z)$ является максимальным; $\widetilde{cc}_{a^j}$ – уровень критичности актива a^j по конфиденциальности; $a^j \in A^C(T_i)$ – множество активов, для которых угроза T_i нарушает конфиденциальность; $\widetilde{pc}^{\,j}(T_i)$ – процент разрушения актива a^j по конфиденциальности в результате реализации угрозы T_i, при этом

$$\widetilde{ci}(T_i)_Z = \widetilde{ci}(T_i, \hat{z}_3) =$$

$$= \sum_{a^j \in A^I(T_i)} \widetilde{pi}^{\,j}(T_i) \cdot \widetilde{ci}_{a^j} \cdot \left(1 - \max_{z \in Z} R_{СЗИ}^{\text{ущерб\_I}}(T_i, z)\right),$$

где $\widetilde{ci}(T_i, \hat{z}_3)$ – количественная оценка суммарного ущерба, наносимого угрозой T_i по целостности, после реализации защитной меры $\hat{z}_3 \in Z$, для которой значение $R_{СЗИ}^{\text{ущерб\_I}}(T_i, z)$ является максимальным; $\widetilde{ci}_{a^j}$ – уровень критичности актива a^j по целостности; $a^j \in A^I(T_i)$ – множество активов, для которых угроза T_i нарушает целостность; $\widetilde{pi}^{\,j}(T_i)$ – процент разрушения актива a^j по целостности для угрозы T_i. Кроме того,

$$\widetilde{cd}(T_i)_Z = \widetilde{cd}(T_i, \hat{z}_3) =$$

$$\sum_{a^j \in A^D(T_i)} \widetilde{pd}^{\,j}(T_i) \cdot \widetilde{cd}_{a^j} \cdot \left(1 - \max_{z \in Z} R_{СЗИ}^{\text{ущерб\_D}}(T_i, z)\right),$$

где $\widetilde{cd}(T_i, \hat{z}_3)$ – количественная оценка суммарного ущерба, наносимого угрозой T_i по целостности после реализации защитной меры $\hat{z}_3 \in Z$, для которой значение $R_{СЗИ}^{\text{ущерб\_D}}(T_i, z)$ является максимальным; $\widetilde{cd}_{a^j}$ – уровень критичности актива a^j по доступности; $a^j \in A^D(T_i)$ – множество активов, для которых угроза T_i нарушает доступность; $\widetilde{pd}^{\,j}(T_i)$ – процент разрушения актива a^j по доступности в результате реализации угрозы T_i.

Шаг 4. Оценка уровня риска по угрозе T_i с учетом множества защитных мер $Risk(T_i)_Z = Impact(T_i)_Z \cdot Poss(T_i)_Z \cdot Poss(v_j)_Z$.

Шаг 5. Уровень риска $Risk(T)_Z$ по множеству угроз T с учетом множества защитных мер определяется в виде $Risk(T)_Z = \sum_i Risk(T_i)_Z$.

2. Оценка эффективности множества защитных мер. Будем осуществлять оценку экономической эффективности защитной меры $z_i \in Z$ через коэффициент «стоимость/эффективность»:

$$K(z_i) = \frac{Выгоды(z_i) - П\_Затраты(z_i)}{E\_затраты(z_i)},$$

где $Выгоды(z_i)$ – выгоды от реализации защитной меры z_i. Данное значение определяется следующим образом:

$$Выгоды(z_i) = \Delta R = Risk(T) - Risk(T)_{\{z_i\}},$$

где $Risk(T) = \sum_j Risk(T_j)$ – суммарный уровень риска по всем угрозам $T_j \in T$ без учета реализации защитных мер в единицу времени, выраженный в виде нечеткого числа в денежном эквиваленте; $Risk(T)_{\{z_i\}} = \sum_j Risk(T_j)_{\{z_i\}}$ – суммарный уровень риска по всем угрозам $T_j \in T$ с учетом реализации защитной меры z_i в единицу времени, выраженных в виде нечеткого числа в денежном эквиваленте; аналогичным образом $E\_затраты(z_i)$ – это единовременные затраты на реализацию защитной меры z_i, выражен-

ные в виде нечеткого числа в денежном эквиваленте, оценки которых формируются экспертным путем; а $П\_Затраты(z_i)$ – дополнительные постоянные затраты на реализацию защитной меры z_i в единицу времени, выраженные в виде нечеткого числа в денежном эквиваленте. Различные виды постоянных затрат, связанных с реализацией защитной меры z_i, характеризуются множеством частных показателей затрат $\{\chi_1,...,\chi_q\}$. Для количественной оценки частных показателей постоянных затрат в денежном эквиваленте применяется метода анализа иерархий.

Пусть Z – множество всех возможных защитных мер, которые потенциально возможно использовать для защиты КИС; $Z' \subseteq Z$ – множество защитных мер, предполагаемых к реализации в КИС в конкретной ситуации. Тогда оценка экономической эффективности множества защитных мер Z' осуществляется в виде $K(Z') = \sum_{z_i \in Z'} K(z_i)$.

Множество защитных мер $Z_1 \subseteq Z$ экономически эффективнее множества защитных мер $Z_2 \subseteq Z$, если $K(Z_1) > K(Z_2)$. В случае $K(Z') < 0$ множество защитных мер Z' является убыточным для владельца КИС, следовательно, реализовывать его нецелесообразно. В случае $K(Z') > 1$ множество защитных мер Z' окупается в срок, не превышающий рассматриваемую единицу времени (например, в течение года). Срок окупаемости множества защитных мер Z' определяется как $1/K(Z')$.

3. Выбор эффективного множества защитных мер. Поставим в соответствие каждому множеству $Z' \subseteq Z$ вектор $X = (x_1,...,x_M)$ выбираемых для реализации защитных мер в КИС. Здесь

$$x_i = \begin{cases} 1, \text{ если } z_i \in Z'; \\ 0, \text{ если } z_i \notin Z'. \end{cases}$$

Обозначим через $K(x_1,...,x_M)$ экономическую эффективность выбранных для реализации защитных мер.

$$K(x_1,...,x_M) = \sum_{i=1}^{M} K_i \text{, где}$$

$$\begin{cases} K_i = K(z_i), \text{ если } x_i = 1; \\ 0, \text{ если } x_i = 0. \end{cases}$$

Обозначим через $Risk(T, x_1,...,x_M)$ суммарный риск, вычисленный с учетом множества реализуемых защитных мер:

$$Risk(T, x_1,...,x_M) = Risk(T)_{Z'},$$

где $z_i \in Z' \Leftrightarrow x_i = 1$. Пусть

$$E\_Затраты(x_1,...,x_M) = E\_Затраты(Z') =$$

$$= \sum_{i=1}^{M} \begin{cases} E\_Затраты(z_i), \text{ если } x_i = 1; \\ 0, \text{ если } x_i = 0. \end{cases}$$

Постановки задач по управлению рисками ИБ будут выглядеть следующим образом.

Задача №1. Найти такой вектор $X = (x_1,...,x_M), x_i \in \{0,1\}$, чтобы

$$\begin{cases} K(x_1,...,x_M) \to \max; \\ Risk(T, x_1,...,x_M) \le Risk^{\text{пороговый}}. \end{cases}$$

Задача №2. Найти такой вектор $X = (x_1,...,x_M), x_i \in \{0,1\}$, чтобы

$$\begin{cases} \dfrac{1}{Risk(T, x_1,...,x_M)} \to \max; \\ \dfrac{1}{K(x_1,...,x_M)} \le \Omega; \\ E\_Затраты(x_1,...,x_M) \le E, \end{cases}$$

где Ω – максимальный срок окупаемости проекта; E – максимальные затраты на его реализацию.

Поставленные задачи по управлению рисками ИБ предлагается решать с помощью генетического алгоритма. Решение задач предлагается кодировать в виде строк-особей, заданных в бинарном виде с помощью вектора $X = (x_1,...,x_M)$, где M – количество всевозможных защитных мер, которые потенциально возможно использовать для защиты КИС, $x_i \in \{0,1\}$. Фитнес-функция генетического алгоритма определяется выражениями $K(x_1,...,x_M) \to \max$ для первой постановки задачи или $1/Risk(T, x_1,...,x_M) \to \max$ для второй постановки задачи.

Заключение

Методы оценки и управления рисками ИБ в КИС находят широкое применение для построения систем защиты информации с позиции ожидаемого ущерба. Однако их применение сдерживается нечеткостью и неопределенностью исходной информации, нечетким и качественным характером частных показателей, влияющих на возможность реализации угроз и использования уязвимостей, а также определяющих ущерб.

Метод управления рисками ИБ в КИС, предложенный в данной статье, позволяет эффективно решать оптимизационные задачи по управле-

нию рисками ИБ на основе ранее разработанного метода нечеткой количественной оценки рисков ИБ в КИС, что преодолевает данные сдерживающие факторы.

Литература

1. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. М.: АйТи, 2004. – 392 с.
2. NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments, September 2012. URL: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf (10.02.2015).
3. Губарева О.Ю., Пугин В.В. Современные методики, применяемые для оценки угроз и уязвимостей информационных систем // ИКТ. Т. 11, № 1, 2013. – С. 100-105.
4. Karabacak B., Sogukpinar I. ISRAM: information security risk analysis method // Computers & Security. №24 (2), 2005. – P. 147-159.
5. Аникин И.В. Метод количественной оценки уровня ущерба от реализации угроз на корпоративную информационную сеть // Информационные технологии. №1, 2010. – С. 2-6.
6. Аникин И.В. Метод оценки внутренних рисков информационной безопасности корпоративных информационных сетей // Информация и безопасность. Т.17, № 2, 2014. – С. 320-323.
7. Аникин И.В. Метод оценки рисков для уязвимостей информационных систем, основанный на нечеткой логике // Информация и безопасность. Т.17, № 3, 2014. – С. 468-471.
8. Аникин И.В. Метод анализа иерархий в задачах оценки и анализа рисков информационной безопасности // Вестник КГТУ им. А.Н. Туполева. №3, 2006. – С. 11-18.
9. Anikin I.V. Information Security Risks Assessment Method Based on AHP and Fuzzy Sets // Proceedings of 2nd Intl' Conference on Advanced in Engineering Sciences and Applied Mathematics (ICAESAM'2014). May 4-5, 2014 Istanbul (Turkey). – P. 11-15.

Получено 15.12.2014

Аникин Игорь Вячеславович, к.т.н., заведующий Кафедрой систем информационной безопасности Казанского национального исследовательского технического университета им. А.Н. Туполева. Тел. (8-843) 231-00-56. E-mail: anikinigor777@mail.ru

METHOD OF INFORMATION SECURITY MANAGEMENT IN CORPORATE NETWORKS

Anikin I.V.
Kazan National Research Technical University, Kazan, Russian Federation
E-mail: anikinigor777@mail.ru

This work is concerned on development of method of information security management in corporate networks. Proposed method is based on estimation of effectiveness for realized safeguards under financial constraints, and it uses quantitative risks values. Moreover, it works under ambiguous initial data and fuzzy and quality measures that contribute possibility of attacks and, using protection vulnerability, it defines damage. We use fuzzy logic and analytic hierarchy process to eliminate these difficulties and following safeguard effectiveness evaluation. Genetic algorithms are applied to solve optimization problem at the stage of risk management.

Keywords: information security, risk assessment, fuzzy logic, hierarchy analysis method.

DOI: 10.18469/ikt.2015.13.2.15.

Anikin Igor Vyacheslavovich, PhD, Head of the Information Security Systems Department, Kazan National Research Technical University, Kazan, Russian Federation. Tel.: +7 843 2310056. E-mail: anikinigor777@mail.ru

References

1. Petrenko S.A., Simonov S.V. *Upravlenie informacionnymi riskami. Jekonomicheski opravdannaja bezopasnost'*. Moscow, AjTi Publ., 2004. 392 p.
2. NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments, September 2012. URL: http://csrc.nist.gov/publications/nist-pubs/800-30-rev1/sp800_30_r1.pdf (accessed 10.02.2015).

3. Gubareva O.Ju., Pugin V.V. Sovremennye metodiki, primenjaemye dlja ocenki ugroz i ujazvimostej informacionnyh sistem [Modern techniques are used to evaluate threate and vulnerabilities information systems]. *Infokommunikacionnye tehnologii*, 2013 vol. 11, no. 1, pp. 100-105.
4. Karabacak B. and Sogukpinar I., ISRAM: information security risk analysis method. *Computers & Security*, 2005, vol. 24, no. 2, pp. 147-159.
5. Anikin I.V. Metod kolichestvennoj ocenki urovnja ushherba ot realizacii ugroz na korporativnuju informacionnuju set' [Method for Quantitative Impact Assessment for Information Security Threats in Corporative Information Network]. *Informacionnye tehnologii*, 2010, no. 1, pp. 2-6.
6. Anikin I.V. Metod ocenki vnutrennih riskov informacionnoj bezopasnosti korporativnyh informacionnyh setej [Method for internal information security risks assessment in corporative information networks]. *Informacija i bezopasnost'*, 2014, vol. 17, no. 2, pp. 320-323.
7. Anikin I.V. Metod ocenki riskov dlja ujazvimostej informacionnyh sistem, osnovannyj na nechetkoj logike [Risk assessment method for vulnerabilities of information systems based on fuzzy logic]. *Informacija i bezopasnost'*, 2014, vol. 17, no. 3, pp. 468-471.
8. Anikin I.V. Metod analiza ierarhij v zadachah ocenki i analiza riskov informacionnoj bezopasnosti [On a method of hierarchy analysis in the problems of valuation and analysis of risks in the field of information safety]. *Vestnik KGTU im. A.N. Tupoleva*, 2006, no. 3, pp. 11-18.
9. Anikin I.V. Information Security Risks Assessment Method Based on AHP and Fuzzy Sets. *Proceedings of 2nd Intl' Conference on Advanced in Engineering Sciences and Applied Mathematics (ICAESAM'2014)*, May 4-5, 2014, Istanbul (Turkey), pp. 11-15.

Received 15.12.2014

УПРАВЛЕНИЕ И ПОДГОТОВКА КАДРОВ ДЛЯ ОТРАСЛИ ИНФОКОММУНИКАЦИЙ

УДК 791.4

СРЕДСТВА МОДЕЛИРОВАНИЯ, ИСПОЛЬЗУЕМЫЕ ПРИ МОДЕЛЬНО-ПАРАМЕТРИЧЕСКОМ ОСНАЩЕНИИ КОНФЕРЕНЦ-ЗАЛОВ

Нестерова Е.И., Смогоржевский А.А.
Санкт-Петербургский государственный институт кино и телевидения, Санкт-Петербург, РФ
E-mail: nesterovaei@mail.ru

Оснащение аппаратно-технологического комплекса конференц-зала подразумевает обоснованный выбор элементов, выходные параметры которых обеспечивают выходные характеристики такого вида мультисервисных услуг, как конференц-обслуживание. На примере формирования видеопроекционной системы конференц-зала показано, что обоснованный выбор элементной и модельно-параметрической структуры конференц-зала должен являться результатом модельно-параметрического анализа, предполагающего использование методов и средств геометрического и параметрического моделирования, что позволяет решать задачи, связанные с выбором структуры комплекса с учетом требований пользователя к характеристикам видеоизображения.

Ключевые слова: модельно-параметрический анализ, конференц-зал, видеопроекционная система, геометрическое и параметрическое моделирование, качество видеоизображения.

Введение

В основе обоснованного выбора технических средств, используемых при оснащении конференц-зала, лежат результаты модельно-параметрического анализа аппаратно-технологического комплекса зала [1]. В свою очередь, модельно-параметрический анализ предполагает использование методов и средств геометрического и параметрического моделирования.

Цели, задачи и критерии модельно-параметрического анализа видеопроекционной системы конференц-зала

Цель модельно-параметрического анализа видеопроекционной системы конференц-зала – выбор элементов видеопроекционной системы, выходные параметры которых обеспечивают характеристики видеоизображения, удовлетворяющие пользовате-