УДК 004.934.2

Е.С. Степанова, И.В. Машкина, В.И. Васильев

РАЗРАБОТКА МОДЕЛИ УГРОЗ НА ОСНОВЕ ПОСТРОЕНИЯ НЕЧЕТКОЙ КОГНИТИВНОЙ КАРТЫ ДЛЯ ЧИСЛЕННОЙ ОЦЕНКИ РИСКА НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Целью статьи является численная оценка риска нарушения информационной безопасности на основе модели реальных угроз.

Задача решается методом построения модели угроз на основе нечеткой когнитивной карты, отображающей пути распространения угроз от источников до объектов атак, с учетом информационной инфраструктуры; оценка потенциального ущерба.

Численные примеры показали применимость разработанного метода в прикладных задачах.

Информационная безопасность; нечеткие когнитивные карты; входной и выходной концепты; T- и S-нормы; вероятность угрозы; относительный и полный риск.

E.S. Stepanova, I.V. Mashkina, V.I. Vasilev

DEVELOPMENT OF THREATS MODEL ON THE BASIS OF FUZZY COGNITIVE MAPS CONTRACTION FOR INFORMATION RISK NUMERICAL ESTIMATION

The objective: information risk numerical estimation on the basis of real threats model.

Tasks: development of threats model on the basis of fuzzy cognitive maps displaying the threats spreading pathways from attack sources to objects taking into account the information infrastructure; an estimation of a potential damage.

Conclusions: numerical examples have proved an applicability of the developed method in applied tasks.

Information security, fuzzy cognitive maps; input and output concepts; T- and S-norms; threat probability; relative and total risk.

Для защиты информации на основе системного подхода, кроме технического, организационного, необходимо и методическое обеспечение. В соответствии с алгоритмом проектирования системы защиты информации (СЗИ) методическое обеспечение, в частности, должно обеспечивать выявление и моделирование угроз безопасности информационным ресурсам и технологиям объекта защиты. Формирование полной системы угроз – сведений об потенциально возможных угрозах и наиболее опасных угрозах – является одним из основных положений унифицированной концепции защиты информации [1].

Моделирование угроз безопасности информации является одним из важных этапов проектирования СЗИ, поскольку дает возможность специалисту по защите информации получить достаточно убедительные доводы о наличии потенциальных угроз безопасности информации на конкретном объекте защиты. Под математическим моделированием понимают процесс получения некоторого математического объекта – математической модели, соответствующей данному реальному объекту. Любая математическая модель, как и всякая другая, описывает реальную систему с некоторой степенью приближения.

Основой построения модели является описание объектов в виде совокупности элементов, связанных между собой определенными отношениями, отображающими семантику предметной области.

В [2] приведен анализ ряда моделей, позволяющих описать процесс сетевой атаки с разной степенью подробности:

- Этапная модель, рассматривающая атаку как последовательность нескольких изолированных этапов, является чрезвычайно обобщенной и не предоставляет возможностей для оценки успешности этапа.
- Деревья атаки, представляющие собой концептуальные диаграммы, которые описывают угрозы системы и атаки, направленные на их реализацию. Данная модель предоставляет большую степень детализации и возможность введения оценок по некоторым критериям, однако, не может быть использована для моделирования атак, поскольку не обеспечивает средств динамического моделирования, включения в модель условий внешней среды. Кроме этого, данная модель не учитывает решений с различной вероятностью и не обеспечивает выбора следующего этапа на основании результатов предыдущего.
- Графовая модель атак, предназначенная для оценки сложности нарушения информационной безопасности (ИБ). При моделировании атак на основе графов учитываются текущие значения некоторых параметров системы, предусматривается анализ условий, необходимых для достижения цели атаки [2].

Создание модели угроз на основе какой-либо классификации угроз по существу является единственным методом достаточно полного исследования потенциально возможных деструктивных воздействий на информационную среду.

Очевидной является необходимость построения модели угроз информационной среде, формат которой определяет сведения об источнике информации, источнике угрозы, пути ее распространения, вероятности реализации. В работе описывается топологическая (пространственная) модель угроз, которая разработана на основе изучения путей распространения потенциально возможных внешних и внутренних угроз. Такая пространственная модель должна отображать процесс реализации угрозы в пространстве на множестве элементов физической среды распространения носителя информации, определять места расположения источника информации и источника угрозы, его возможную удаленность от защищаемого ресурса, ориентацию вектора распространения носителя при реализации угрозы.

Процессы осуществления несанкционированного доступа, утечки информации и деструктивных воздействий на объект защиты следует разделить на две части: действия злоумышленника и действия нарушителя (легального пользователя, решившего нарушить установленные правила); их возможности по реализации угроз различаются.

В работе предлагается каждую угрозу безопасности объекта защиты (ОЗ) рассматривать как сложную последовательность действий, которые могут быть представлены как составляющие компоненты угрозы на пути ее распространения на множестве элементов среды информационной инфраструктуры при манипулировании злоумышленника (нарушителя) информационными потоками в целях достижения определенного воздействия на информационную среду.

Рассмотрим построение модели информационной инфраструктуры СЗИ на основе теоретико-множественного подхода.

Обозначим множество защищаемых информационных ресурсов через $\{o_1, o_2 .. o_h\} \in O$, где $h \in [1, H]$.

Обозначим через S множество субъектов доступа, под которыми понимается атакующая программа или оператор, непосредственно осуществляющий воздействие на вычислительную сеть.

$$S = S^{вн} \cup S^{внш},$$

где $S^{вн}$ – внутренние субъекты доступа,

$S^{внш}$ – внешние субъекты доступа.

Внутренние угрозы связаны с нарушением принятой политики безопасности: нелегальным поведением пользователя на компьютере или сервере, попытками доступа пользователя к информационным ресурсам, уровень конфиденциальности которых превышает его уровень доступа. Любой несанкционированный доступ является реализацией преднамеренной угрозы информационной безопасности (ИБ) и называется атакой.

Множество внутренних субъектов доступа – есть объединение множеств

$$S^{вн} = S^{н} \cup S^{с} \cup S^{в},$$

где $S^{н}$ – множество пользователей или процессов с уровнем доступа низкий, «н»,

$S^{с}$ – множество пользователей или процессов с уровнем доступа средний, «с»,

$S^{в}$ – множество пользователей или процессов с уровнем доступа высокий, «в».

Внешние угрозы – это потенциально возможные действия, заключающиеся в поиске и использовании той или иной уязвимости, предпринимаемые:

- злоумышленником с целью проникновения с удаленной машины внутрь защищаемой системы, получения, без права на то, удаленного доступа к ресурсам информационной системы (ИС) и хищения данных или вызова отклонения от нормального протекания информационных процессов;
- удаленным пользователем, имеющим определенные права, пытающимся превысить уровень своих полномочий.

Таким образом, множество внешних субъектов доступа – есть объединение множеств

$$S^{внш} = S_t^{п\,внш} \cup S_t^{внш}, t \in [1,T],$$

где $S_t^{П\,ВНШ}$ – внешние пользователи, обладающие определенными правами доступа,

$S_t^{внш}$ – несанкционированный субъект доступа,

T – число точек доступа через периметр.

Зададим множество сегментов сети C:

$$C = C^{н} \cup C^{с} \cup C^{в},$$

где $C^{н}$, $C^{с}$, $C^{в}$ – подмножества сегментов, в которых хранится и обрабатывается информация, соответственно, с низким, средним и высоким уровнем конфиденциальности (или подмножества сегментов, на хостах которых работают пользователи, имеющие уровень доступа соответственно низкий, средний и высокий).

Для описания угрозы как канала несанкционированного доступа, утечки, деструктивных воздействий, необходимо указать субъект доступа, информационный объект, к которому осуществляется несанкционированный доступ, путь распространения угрозы, информационный носитель. Тогда угроза может быть описана кортежем

$$U = \langle S, A, З_с, З_х, П, O(C) \rangle,$$

где S – источник угрозы – субъект доступа (пользователь, внешний злоумышленник или запущенные ими процессы);

A – оборудование в канале связи (коммутаторы, маршрутизаторы и другое);

$З_с, З_х$ – сервисы безопасности на пути распространения угрозы, соответственно, сетевые и хостовые (МЭ, СОА, журналы регистрации аномальных сетевых соединений, журналы регистрации операционных систем и другие);

П – протоколы;

О – объект доступа с указанием сегмента.

Представим множество угроз в виде $U = U^{ВНШ} \cup U^{ВН} \cup U^{ВН\_С}$,

где $U^{ВНШ}$ – множество внешних угроз через проводные, беспроводные и модемные каналы связи;

$U^{ВН}$ – множество внутренних межсегментных угроз (угроз между узлами, находящимися в разных локальных сегментах);

$U^{ВН\_С}$ – множество внутренних угроз, источники которых расположены в том же локальном сегменте, что и объект доступа.

Модель угроз создана для объекта защиты, при построении архитектуры безопасности которого учтен один из основных принципов, рекомендуемых в [3]: введение категорий критичности информации и создание соответственно сетевых сегментов, на хостах которых хранится и обрабатывается информация одного и того же уровня конфиденциальности. При этом каждый пользователь внутри своего сетевого сегмента имеет одинаковые права доступа к информации одного уровня конфиденциальности. В этом случае не смешиваются потоки информации разных уровней конфиденциальности. Объяснением такого разделения всех пользователей на три типа изолированных сегментов является легкость осуществления атаки внутри одного локального сегмента сети.

При реализации этого принципа $\mathrm{U}^{\mathrm{ВН\_С}} = \varnothing$.

Подмножество внутренних угроз включает в себя подмножества $U^{вн}_{d(f)}$ и $U^{вн}_{df(g)}$

$$U^{вн}_{d(f)} = \langle S^{c}, A, П, O^{B}(C^{B}) \rangle,$$

где $U^{вн}_{d(f)}$ – угроза информационным объектам в случае, когда нарушитель имеет учетную запись в системе как пользователь с правами доступа к информации с уровнем конфиденциальности «с», обрабатываемой в сегментах $\mathrm{C}^{\mathrm{c}}_{\mathrm{f}}$, и пытается превысить свои привилегии,

$$U^{вн}_{df(g)} = \langle S^{н}, A, З_{c}, З_{x}, П, O^{в}(C^{в}) \cup O^{c}(C^{c}) \rangle,$$

где $U^{вн}_{df(g)}$ – угроза информационным объектам категории «в» и «с» в случае, когда нарушитель имеет учетную запись в системе как пользователь с правами доступа к информации с уровнем конфиденциальности «н», обрабатываемой в сегментах $C^{н}_{g}$, и пытается превысить свои привилегии.

Внешняя угроза связана с внешним субъектом доступа и описывается кортежем:

$$U^{внш} = \langle S^{внш}, A, З_{c}, З_{x}, П, O(C) \rangle.$$

Таким образом, источниками внутренних угроз являются субъекты и процессы, описываемые множествами $S^{н}, S^{c}$, источниками внешних угроз – субъекты и процессы, описываемые множеством $S^{внш}$.

Обзор различных моделей, описывающих процесс осуществления атаки, приведенный выше, показал применимость графовой модели для задания оценки сложности нарушения безопасности информационной системы.

В работе предложено использовать нечеткие когнитивные карты (НКК) для построения модели угроз информационной среде объекта защиты.

НКК, описывающие воздействия потенциальных угроз на защищаемые ресурсы, могут быть использованы для анализа рисков нарушения информационной безопасности.

Нечеткие когнитивные карты задаются в виде ориентированного графа и представляют моделируемую систему в виде множества концептов $\{K_1, K_2..K_n\}$, существенных для понимания исследуемой проблемы и связанных между собой отношениями влияния, отражающими причинно-следственные связи и показывающими степень влияния одного концепта на другой $w_{ij} \in W$. Направленность этой связи w_{ij} означает, что концепт-источник влияет на концепт-приемник.

Термин «нечеткие» обозначает то, что причинные связи могут принимать значения из диапазона действительных чисел $[0,1]$.

Определим путь между входными K_i – источником угрозы, и выходными концептами K_y – объектом атаки (информационным ресурсом), нечеткой когнитивной карты следующим образом: $K_i \to K_y$, $Z = (i, z_1, z_2, z_3 ... z_m, y)$, $m \in [1, M]$ – количество промежуточных концептов.

Путь между концептами K_i и K_y представлен на рис. 1.

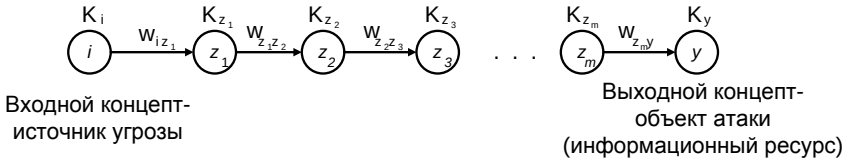

Рис. 1. Путь между концептами K_i и K_y

На рис. 2 приведен случай, когда между концептами K_i и K_y могут быть построены $l = [1, L]$ различных путей.

Нечеткие значения выходного концепта могут быть заданы с использованием операций Т-норм, характерных для нечеткой логики, над нечеткими значениями входных концептов и весов влияния.

Отдельные нечеткие влияние входных концептов, воздействующих на выходной концепт, объединяются на основе S-нормы [4]:

$$w_{iy} = \underset{l=1}{\overset{L}{S}} \; \underset{z \in Z}{T} w_{z,z+1}, \tag{1}$$

где K_i и K_y – значения входного и выходного концептов;

w_{iy} – вес влияния концепта *i* на концепт *y*.

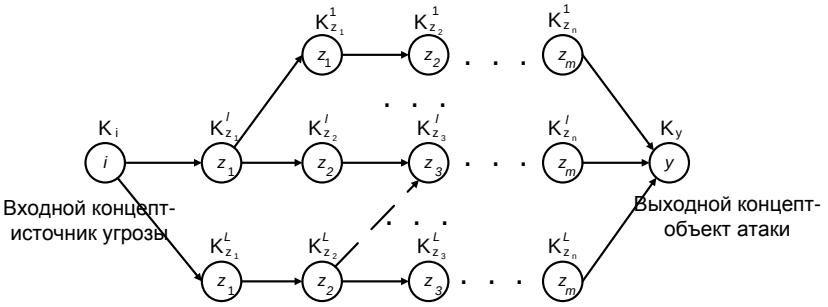

Рис. 2. Множество путей между концептами K_i *и* K_y

Наиболее распространенными разновидностями Т-норм являются операции минимума и алгебраического произведения, а наиболее распространенной разновидностью S-нормы – операция максимума.

Максимальное значение из весов $l = [1, L]$ различных путей между концептами K_i и K_y будет соответствовать вероятности реализации угрозы на информационный ресурс K_y объектом атаки K_i $P(K_i \to K_y)$.

В решаемой задаче $w_{z,z+1}$ соответствует значению уязвимости компонента инфраструктуры, представленного в НКК промежуточным концептом K_{z+1}^{l}, $P_{акт}$ – вероятность активизации входного концепта. Тогда вероятность реализации угрозы на *l*-м пути предложено вычислять по формуле (2):

$$P_l = P_{акт} \cdot \underset{z \in Z}{T} w_{z,z+1}. \quad (2)$$

Максимальное значение P_l, где $l \in [1, L]$ между концептами K_i и K_y будет соответствовать вероятности реализации угрозы на информационный ресурс K_y источником атаки K_i $P^U(K_i \to K_y)$. Таким образом, формула (1) может быть представлена в виде

$$P^U(K_i \to K_y) = \max_{l=1}^{L} P_l. \quad (3)$$

На рис. 3 приведена нечеткая когнитивная карта, показывающая различные пути распространения атаки для ресурса O_h, представленного выходным концептом $K_y^{o_h}$.

Величина относительного риска $\overline{R_{O_h}}$ может быть определена по формуле

$$\overline{R_{O_h}} = P^U\left(K_i \to K_y\right) \cdot \frac{C^{O_h}}{C_\Sigma}, \quad (4)$$

где $\frac{C^{O_h}}{C_\Sigma}$ – относительная стоимость информационного ресурса O_h.

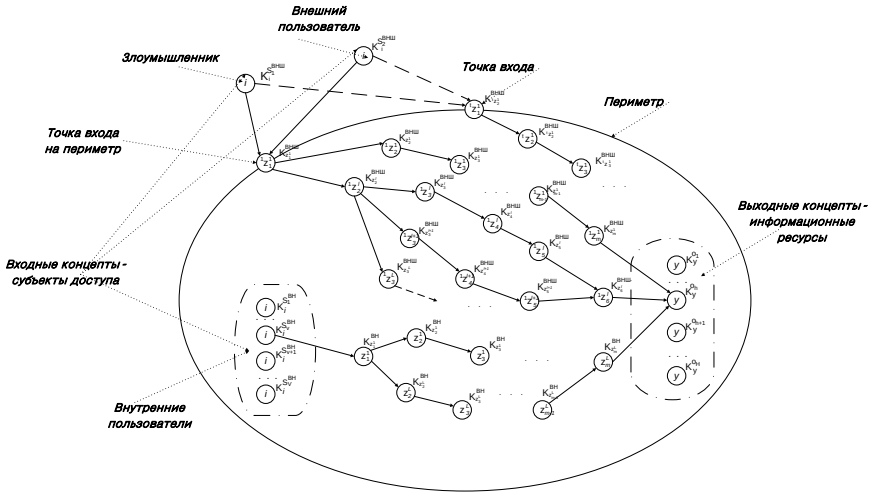

Рис. 3. Нечеткая когнитивная карта модели угроз в общем случае

Тогда величину полного относительного риска для всех информационных ресурсов можно определить по формуле

$$\overline{R} = \sum_{h=1}^{H} \overline{R_{O_h}} \cdot \qquad (5)$$

В качестве объекта защиты был выбран сегмент обработки платежей банка. На рис. 4 приведена топология сети сегмента обработки платежей.

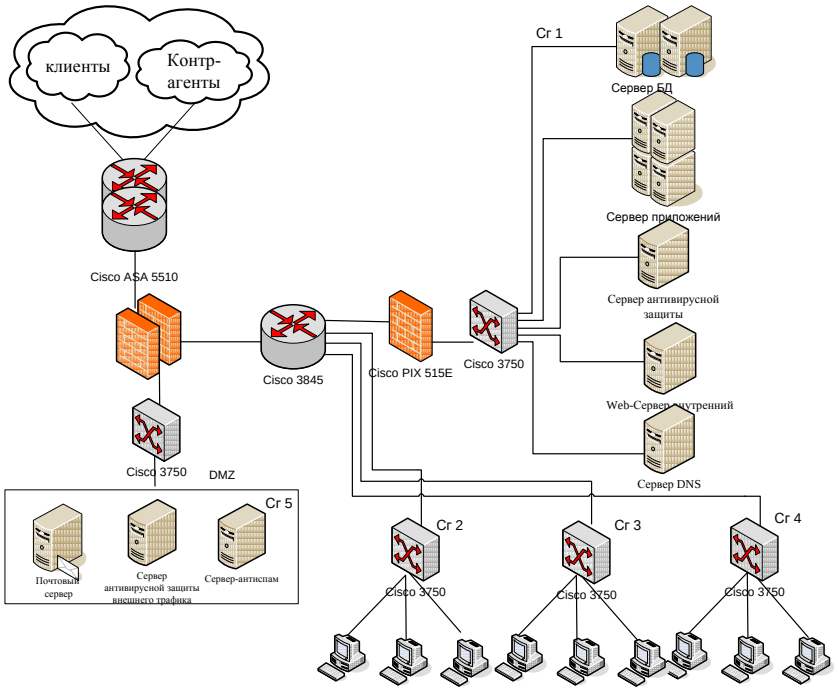

Рис. 4. Топология сегмента обработки платежей банка

Представим схему воздействия угроз на информационные ресурсы в виде НКК, приведенной на рис. 5, где концепт K_i^S соответствует рассматриваемому источнику угрозы, выходной концепт $K_y^{o_h}$ – информационному ресурсу, а концепты $K_{z,z+1}$ – промежуточные концепты, отражающие уязвимости программного обеспечения, коммуникационного оборудования, протоколов связи и сервисов безопасности.

Значения весов получены нормализацией величин, приведенных в [5].

Примем вероятности активизации входных концептов реализации угроз следующими:

- вероятность реализации угрозы злоумышленником – 0,15;
- вероятность реализации угрозы внешним пользователем – 0,15;
- вероятность реализации внутренней угрозы –0,7.

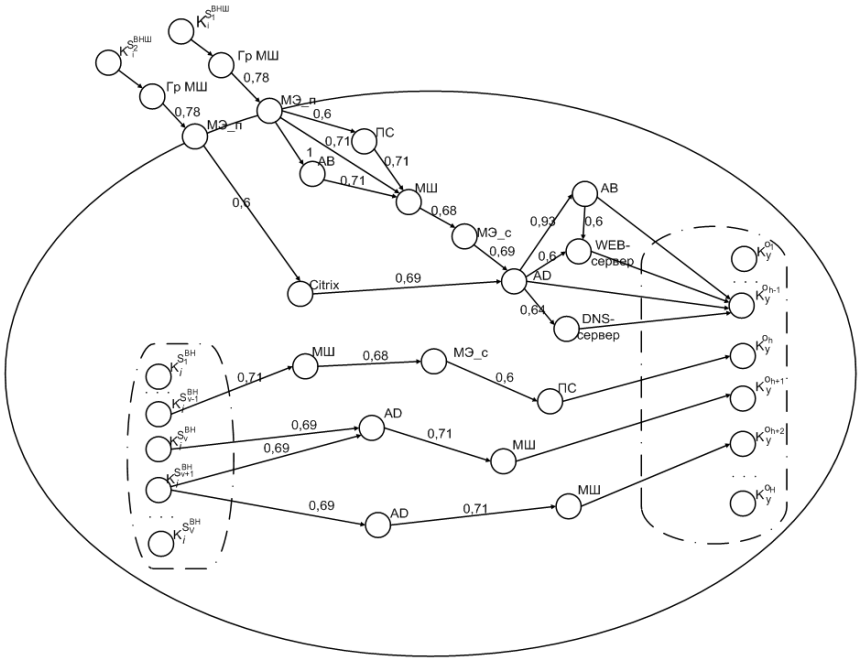

Рис. 5. Нечеткая когнитивная карта модели угроз в проекции на топологию сети: ГрМШ – граничный маршрутизатор; МЭ_п – периметровый межсетевой экран; ПС – почтовый сервер; АВ – антивирус; МШ – маршрутизатор; МЭ_с – межсегментный экран; Citrix – ПО Citrix Presentation Server 4.5; AD – Active Derectory

Рассмотрим один из возможных путей $K_i^{S_1^{ВНШ}} \to K_y^{o_{h-1}}$. Используя формулы (2) и (3), можно получить оценку влияния источника угрозы $K_i^{S_1^{ВНШ}}$ на информационный ресурс $K_y^{o_{h-1}}$:

$$P_{o_{h-1}}(K_i^{S_1^{ВНШ}} \to K_y^{o_{h-1}}) = \max_{l=1}^{L} P_l = max(0{,}023385;0{,}014967;0{,}0217485;0{,}0130485;0{,}014031;$$
$$0{,}038976;0{,}024945;0{,}0362475;0{,}0217485;0{,}0233865) = 0{,}038976.$$

Аналогично определим $P_{o_{h-1}}(K_i^{S_2^{ВНШ}} \to K_y^{o_{h-1}}) = 0{,}048438$, $P_{o_h}(K_i^{S_{v-1}^{ВН}} \to K_y^{o_h}) = 0{,}232596$, $P_{o_{h+1}}(K_i^{S_v^{ВН}} \to K_y^{o_{h+1}}) = 0{,}34293$, $P_{o_{h+1}}(K_i^{S_{v+1}^{ВН}} \to K_y^{o_{h+1}}) = 0{,}34293$, $P_{o_{h+2}}(K_i^{S_{v+1}^{ВН}} \to K_y^{o_{h+2}}) = 0{,}34293$.

Относительные стоимости информационных ресурсов, циркулирующих в сегменте обработки платежей примем следующими:

- сервер БД (O_{h-1}) – 0,8;
- почтовый сервер (O_h) – 0,1;
- хосты с высоким уровнем доступа к информационному ресурсу (O_{h+1}) – 0,06;
- хосты с среднем уровнем доступа к информационному ресурсу (O_{h+2}) – 0,04.

Воспользовавшись формулами (4) и (5), определим значение полного относительного риска: $\overline{R} = 0{,}14806 \approx 14{,}8\%$.

После модернизации системы защиты информации – определения набора добавочных средств защиты, перекрывающих пути распространения угроз, расчетное значение риска составило $\overline{R} = 2{,}8\,\%$, что в 5,2 раза меньше исходного значения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Малюк А.А.* Информационная безопасность и методологические основы защиты информации: Учеб. пос. для вузов. – М.: Горячая линия – Телеком, 2004. – 280 с.
2. *Тумоян Е.П.* Обзор методов формального моделирования компьютерных атак // Материал X Международной научно-практической конференции «Информационная безопасность». Ч. 1. – Таганрог: Изд-во ТТИ ЮФУ, 2008. – С. 194-197.
3. ГОСТ Р ИСО/МЭК 17799 – 2005[Электрон. ресурс]. – Режим доступа: http://sec7x24.net/std/17799-2005.html.
4. *Борисов В.В., Круглов В.В., Федулов А.С.* Нечеткие модели и сети. – М.: Горячая линия - Телеком, 2007. – С. 275-279.
5. CPE – Common Platform Enumeration [Электрон. ресурс]. – Режим доступа: http://nvd.nist. gov/cpe.cfm.

Степанова Екатерина Сергеевна
Уфимский государственный авиационный технический университет.
E-mail: stepanova_e_s@mail.ru.
450000, Республика Башкортостан, г. Уфа, ул. К. Маркса, д. 12.
Тел.: +79272328676.

Машкина Ирина Владимировна
E-mail: mashkina_vtzi@mail.ru.
Тел.: +79279277089.

Васильев Владимир Иванович
E-mail: vasilyev@ugatu.ac.ru.
Тел.: 83472730672.

Stepanova Ekaterina Sergeevna
The Ufa state aviation technical university chair of Computer facilities and information protection.
E-mail: stepanova_e_s@mail.ru.
12, K. Marx's street, Ufa, 450000, Russia.
Phone: +79272328676.

Mashkina Irina Vladimirovna
E-mail: mashkina_vtzi@mail.ru.
Phone: +79279277089.

Vasilev Vladimir Ivanovich
E-mail: vasilyev@ugatu.ac.ru.
Phone: +73472730672

УДК 681.1

О.М. Лепешкин

МЕТОДИКА ВЫБОРА СПОСОБОВ РЕАЛИЗАЦИИ МЕХАНИЗМОВ ОБЕСПЕЧЕНИЯ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИХ СОЦИОТЕХНИЧЕСКИХ СИСТЕМ НА ОСНОВЕ СРЕДЫ РАДИКАЛОВ

Изложены основные проблемы применительно к функциональной безопасности современных информационных систем и рассмотрена методика выбора способов реализации механизмов обеспечения функциональной безопасности критических социотехнических систем на основе среды радикалов.

Информационные системы; социотехнические системы; функциональная безопасность; радикал; оптимизация.

O.M. Lepeshkin

WAYS SELECTION METHOD OF FUNCTIONAL SAFETY MECHANISMS REALIZATION FOR CRITICAL SOCIOTEHNICAL SYSTEMS ON THE BASIS OF RADICALS

In the paper modern information systems problems of functional safety are stated and the ways selection method of functional safety mechanisms realization for critical sociotehnical systems on the basis of radicals is considered.

Information systems; sociotehnical systems; functional safety; the radcal; optimization.

Под сложной системой (человекомашинной системой – ЧМС) будем понимать систему, состоящую из технических средств (сложных информационных систем), и людей, взаимодействующих с ними. Возникают все новые и новые системы, изменяются, развиваются уже существующие системы. Развиваются многочисленные и разнообразные математические модели, методы и программно-технические средства (ПТС), предназначенные для решения задач жизненных циклов сложных систем. Растут масштабы применения таких средств. Они требуют все больших и больших ресурсов, для обеспечения которых необходимы, в свою очередь, другие системы, не менее сложные и масштабные. Аналогичные характеристики сложности и масштабности применимы и к современным ПТС – важной компоненте сложных систем. Однако из разных источников постоянно появляется информация, свидетельствующая о многочисленных и разнообразных проблемах современных сложных систем. Развиваются внутренние противоречия между составляющими систем, включая людей и ПТС, а также между системами и окружающей средой (природой и другими системами). Порой эти проблемы являются скрытыми, неучтенными и приводят к дальнейшим отрицательным последствиям, с которыми неизбежно приходится бороться, что требует огромных затрат. Мир сложных систем все больше начинает походить на гигантское скопление чрезвычайно сложных механизмов, порой остроумных в своих деталях и отдель-