Соснин Ю. В., Куликов Г. В., Непомнящих А. В.

КОМПЛЕКС МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ ОПТИМИЗАЦИИ КОНФИГУРАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Аннотация: *Предметом исследования является проблема формализованного описания конфликтной ситуации, возникающей при защите информации от несанкционированного доступа к ней, для получения дополнительной информации о возможных действиях потенциального противника и об их последствиях в интересах выбора и реализации оптимальной стратегии защиты информации в автоматизированных системах. Исходными данными являются перечень объектов автоматизированной системы и стоимость обрабатываемой на них информации; перечень средств защиты информации и их стоимость; перечень вероятных методов реализации угроз несанкционированного доступа к информации, их стоимость и эффективность. Результатом является наиболее эффективная конфигурация средств защиты информации для каждого объекта с оценками эффективности и стоимости ее реализации. Методы исследования: теория игр, теория вероятностей, теория надежности, системный анализ, теория сбора и обработки экспертной информации. Применение разработанных моделей процесса защиты информации обеспечивает оптимальную конфигурацию средств защиты информации, для которой каждый вариант системы защиты характеризуется однозначной количественной оценкой, имеющей явный физический смысл (показатель защищенности), что позволяет выбрать конкретный вариант защиты объекта автоматизированной системы по критерию максимальной защищенности (при стоимостных ограничениях) или минимальной стоимости (при фиксированных требованиях по защищенности). Кроме того, оптимизация состава и структуры системы защиты информации при проектировании и при изменении исходных данных не требует значительных временных затрат.*

Ключевые слова: *информационная безопасность, защита информации, управление защитой информации, моделирование информационных угроз, моделирование защиты информации, управление рисками безопасности, угрозы безопасности информации, оценивание защищенности информации, несанкционированные информационные воздействия, критерии защищенности информации*

Введение

Выявление возможных каналов реализации способов несанкционированного до-

DOI: 10.7256/2305-6061.2015.1.14124

ступа (НСД) к информации в автоматизированных системах (АС) требует определения топологии сетевой структуры объектов, архитектуры, используемых технических платформ и сетевых операционных систем, протоколов и т.д. [2, 6, 22]. Как правило, АС имеют иерархическую структуру с единым управляющим центром, которая отражает организационное построение системы и упрощает процесс сбора и обработки информации [3, 8, 15, 16, 24-28]. При этом неизбежно наличие определенной степени децентрализации управления, связанной с самостоятельными действиями звеньев (подсистем) в соответствии с их интересами.

Выбор объектов для осуществления НСД связан с учетом следующих соображений. В зависимости от решаемых задач и места объектов в организационной структуре их информационная ценность будет различной. Как правило, защищенность объекта должна быть пропорциональна его информационной ценности. Таким образом, осуществить успешный НСД значительно проще на нижних уровнях иерархической системы. С другой стороны, эффект от реализации НСД, определяемый ценностью полученной информации, в этом случае может быть недостаточным [5, 13, 14, 19, 29].

Также необходимо учитывать возможность доступа к информации объекта «снизу», то есть со стороны подчиненного звена, к которому уже получен доступ. В этих условиях для анализа процессов функционирования ключевых объектов необходимы модели, описывающие поведение элементов (объектов) системы и их взаимодействие. Роль этих моделей тем значительнее, чем для более высокого уровня иерархической системы они предназначены.

Построение поведенческих моделей является одной из важнейших задач теории иерархических систем [1, 4, 7, 12, 17, 18, 21]. Большое разнообразие и сложность задач, решаемых АС, не позволяет построить универсальные модели их функционирования. С другой стороны, подобные модели должны отражать только ту информацию о функционировании объектов, которая необходима для исследования их защищенности.

При анализе АС как иерархических систем в качестве основного предмета анализа традиционно рассматривают пару объектов, один из которых находится в непосредственном подчинении у другого. Исследование взаимодействия между ними служит основой изучения других структур. Для проведения такого анализа необходимо описать каждый объект в отдельности и связи между объектами [1, 16, 19, 26]. В общем случае требуется знать принципы принятия решений по управлению функционированием АС, то есть цели функционирования АС и ее подсистем, а также иметь модели информационного взаимодействия объектов. При этом анализ проводят с позиции должностного лица, отвечающего за процесс нормального функционирования объекта АС. Поэтому модели информационного обмена структурных уровней представляют собой субъективное описание ситуации и могут быть значительно более агрегированными по сравнению с теми, которые реально описывают взаимодействие объектов.

DOI: 10.7256/2305-6061.2015.1.14124

Постановка задачи

Типовая АС является иерархической структурой с конечным числом объектов, подчиненных одному центру, то есть имеет древовидную структуру. Причем обосновано, что исследование моделей иерархических структур, включающих более трех структурных уровней, не имеет практического смысла.

Цели функционирования всех объектов АС, как правило, согласованы и определяются общими задачами, а правила информационного обмена определены в соответствующих инструкциях и руководствах. Существенной особенностью АС является неравноправное положение объектов в организационной структуре АС. Место объекта в организационной структуре определяется характером решаемых задач и вкладом в достижение общей цели. Специфика хранимой, обрабатываемой и передаваемой информации и предъявление высоких требований к ее безопасности естественно приводят к необходимости выявления зависимости между значимостью объектов и их информационной ценностью [2, 3, 12-16].

Пусть S_k, $k=1,\ldots, l$ – объекты АС, функционирующие в соответствии с собственными целями, а C_k – информационная ценность объекта S_k.

При построении модели информационного взаимодействия АС важно определить значения C_k для всех объектов S_k, а также соотношения между этими значениями. Следует отметить, что объем и характер решаемых объектами задач в общем случае достаточно редко подвержен изменениям. Это означает, что информационную ценность C_k можно рассматривать как статическую характеристику объектов S_k.

Получение значений информационных ценностей объектов (на основе свертки конфиденциальности, целостности и доступности информации) позволяет определить те подсистемы, которые представляют интерес с точки зрения характера и содержания хранимой и обрабатываемой в них информации [9, 13-16, 18, 26-28]. Построение модели объекта дает возможность, во-первых, проводить в дальнейшем целенаправленный поиск каналов утечки информации в пределах выбранных подсистем, и, во-вторых, определить допустимые экономические затраты на подготовку и реализацию НСД к каждому объекту.

Следующим шагом мероприятий по исследованию процессов защиты информации является определение перечня имеющихся программных и аппаратных средств, необходимых для проведения информационных атак, а также качества этих средств. Работы этого этапа завершают построением модели НСД.

Моделирование НСД к хранимой, обрабатываемой и передаваемой информации

Знание возможных методов и средств осуществления НСД к информации, а также уязвимых мест средств защиты информации (СЗИ) АС необходимо для выбора наиболее

DOI: 10.7256/2305-6061.2015.1.14124

эффективных мер и средств информационных атак. Очевидно, что для объектов АС основным источником НСД к информации является человек, а несанкционированное использование программно-аппаратных средств и различные способы программных закладок следует рассматривать как возможные проявления его действий. При этом множество возможных способов осуществления НСД представляет собой среду с неизвестностью (с неизвестными элементами), являющуюся по своей природе целенаправленной, то есть связанной с человеческой деятельностью и подчиненной определенным целям, но о которой в той или иной степени отсутствует априорная информация [6, 15, 29].

Таким образом, принятие решений о выборе средств для противодействия осуществления НСД на АС происходит в условиях неопределенности. Источником неопределенности является невозможность формализованного описания поведения человека (злоумышленника), что проявляется в отсутствии полной информации о характеристиках НСД и особенностях их реализации. Для принятия решений в условиях неопределенности необходимо получить модель указанной среды. Как правило, составить какую-либо аналитическую или имитационную модель, то есть соотнести входные и выходные данные или входные данные с характеристиками среды с неизвестностью невозможно. В этих условиях для устранения соответствующей неопределенности можно составить аналог подобной модели и получить зависимость степени достижения сформулированных целей от входных данных [6, 10-14, 18-23].

Предположим, что для одной из АС составлен полный перечень возможных угроз НСД, заданный конечным множеством

$$X=||x_i||, \quad i=1,\ldots, n.$$

Эффективность реализации угрозы $x_i \in X$ определяют ценностью информации C_k на объекте АС S_k, оказавшемся под воздействием НСД

$$C_{ik}=\mu_{ik}C_k,$$

где C_{ik} – ценность информации при реализации НСД $x_i \in X$ на объекте АС $S_k \in S, \mu_{ik} \in$ [1;2] – показатель эффективности реализации НСД $x_i \in X$ на объекте АС $S_k \in S$ (минимальное значение показателя соответствует минимальной эффективности применения средства реализации воздействия).

Подверженность объектов НСД определяют индикаторными переменными

$$h_{ik} = \begin{cases} 0, \ если\ объект\ \ s_k \in S\ \ не\ \ подвергается\ \ угрозе\ \ x_i \in X \\ 1, \ \ если\ \ объект\ \ \ s_k \in S\ \ \ подвергается\ \ \ угрозе\ \ x_i \in X \end{cases}$$

Тогда справедливо

$$\sum_{k=1}^{l}\sum_{i=1}^{n} a_{ik}h_{ik} \le A,$$

где A – суммарные затраты на реализацию угроз НСД на всех объектах АС; a_{ik} – затраты на реализацию угрозы $x_i \in X$ на объекте АС $S_k \in S$.

DOI: 10.7256/2305-6061.2015.1.14124

Наличие модели НСД к объектам АС позволяет оценить эффективность проведения информационных атак и выявить имеющиеся на объектах уязвимости, обусловленные их архитектурой, недостатками используемых аппаратных платформ, сетевых операционных систем, программного обеспечения (ПО), применяющимися для взаимодействия между объектами сетевыми, транспортными и прикладными протоколами и т. д. Обеспечение безопасности информации от НСД на объектах АС достигают путем использования наиболее действенных мер и средств защиты информации, т. е. таких средств, которые способны максимально снизить эффективность применения угроз НСД. Проведение соответствующих исследовательских работ заканчивают построением модели СЗИ объекта АС.

Моделирование СЗИ объектов АС

Пусть множество СЗИ, используемых на объекте АС, описывается конечным множеством

$$Y=||y_j||, \quad j=1,..., m.$$

Обозначим $\gamma_{ijk} \in [1;2]$ – показатель нейтрализации угрозы НСД к информации $x_i \in X$ средством защиты информации $y_j \in Y$ на объекте $S_k \in S$ (минимальное значение показателя соответствует максимальному ослаблению средства реализации воздействия). Тогда

$$C_{ijk}=C_{ik}\,\gamma_{ijk},$$

где C_{ijk} – ценность раскрытой информации при воздействии угрозы $x_i \in X$ на объект $S_k \in S$, оснащенный средством защиты информации $y_j \in Y$. Наличие средства защиты информации $y_j \in Y$ на объекте $S_k \in S$ задают индикаторными переменными

$$h_{jk} = \begin{cases} 0, \ \textit{если объект } s_k \in S \textit{ не защищен средством } y_j \in Y \\ 1, \ \textit{если объект } s_k \in S \textit{ защищен средством } y_j \in Y \end{cases}$$

В этом случае справедливо

$$\sum_{k=1}^{l}\sum_{j=1}^{m} b_{jk} h_{jk} \le B,$$

где B – допустимые затраты на защиту информации от НСД на объектах АС; b_{jk} – стоимость средства защиты информации $y_j \in Y$ на объекте $S_k \in S$.

Построение модели СЗИ позволяет оценить действенность используемых на объекте АС средств защиты информации и подготовить необходимые исходные данные для принятия решения о выборе для оснащения объекта АС наиболее эффективными из указанных СЗИ.

Моделирование процесса защиты информации в условиях реализации способов НСД на объектах АС

Для анализа процесса защиты информации на типовом объекте АС в связи с трудностями проведения натурных испытаний необходимо использовать аналитическую модель.

DOI: 10.7256/2305-6061.2015.1.14124

Модель процесса защиты информации включает описанные ранее модели объекта, реализации способов НСД к информации на объектах и СЗИ объектов. Условие конечности множеств X и Y, допустимое при исследовании АС, позволяет классифицировать модель процесса защиты информации как конечную игру двух сторон с нулевой суммой [6, 16].

Рассмотрим процесс защиты информации для одного объекта АС $S_k \in S$. Игра Γ задают тройкой

$$\Gamma = < X, Y, \Phi >,$$

где $\Phi = \Phi(x_i, y_j)$ - функция от двух переменных $x_i \in X$ и $y_j \in Y$. Поскольку число возможных действий каждой из сторон конечно, значения функции Φ можно представить в виде матрицы

$$\Phi = \left\| \varphi_{ij} \right\|, \quad \varphi_{ij} = \Phi(i, j), \qquad i=1,..., n, \qquad j=1,..., m,$$

в i-й строке которой последовательно расположены выигрыши первой стороны в ситуациях $(i, 1), (i, 2),..., (i, m)$, а в столбце j - ее выигрыши в ситуациях $(1, j), ..., (n, j)$. Выбор первой стороной способа реализации угрозы НСД $x_i \in X$ – стратегии i – означает выбор строки i, выбор второй стороной средства защиты информации $y_j \in Y$ – стратегии j – выбор столбца j. При этом выигрыш первой стороны определяют ценностью раскрытой информации и затратами на реализацию НСД $x_i \in X$ - он равен элементу матрицы Φ, стоящему на пересечении строки i и столбца j.

Процесс защиты информации состоит в том, что стороны независимо друг от друга выбирают соответственно некоторые чистые стратегии $x_i \in X$ и $y_j \in Y$, в результате чего складывается ситуация (x_i, y_j). Первая сторона получает выигрыш φ_{ij}, вторая сторона столько же проигрывает. Пусть на объекте $S_k \in S$ реализуется угроза НСД к информации $x_i^* \in X$. Тогда защищающаяся сторона может использовать такое средство защиты информации $y_j \in Y$, которое позволит получить минимальное значение φ_{ij}, то есть

$$y_j^* = \arg\min_{y_j \in Y} \Phi\left(x_i, y_j\right).$$

Для объекта $S_k \in S$ существует такой способ реализации угрозы НСД $x_i^* \in X$, который нейтрализуется средством защиты информации $y_j^* \in Y$. Формально задача выбора лучшего по показателю «эффективность-стоимость» способа реализации угрозы НСД задают в виде

$$\min_{y_j \in Y} \Phi\left(x_i^*, y_j\right) = \max_{x_i \in X} \min_{y_j \in Y} \Phi\left(x_i, y_j\right) = \underline{V},$$

Величину $\underline{V}$ называют нижней ценой игры, а соответствующую этому значению стратегию x_i^* называют *максиминной чистой стратегией*. Таким образом, возможный выигрыш при выборе i^* - го способа реализации угрозы НСД при использовании любых комплексов СЗИ будет не меньше величины $\underline{V}$, то есть

$$\Phi\left(x_i^*, y_j\right) \geq \underline{V}.$$

Решение матричной игры позволяет определить наиболее опасный способ реализа-

DOI: 10.7256/2305-6061.2015.1.14124

ции НСД $x_i^* \in X$, самое эффективное СЗИ $y_j^* \in Y$ и размер минимального ущерба при использовании СЗИ $y_j^* \in Y$. При этом возможна ситуация равновесия в чистых стратегиях

$$\max_i \min_j \phi_{ij} = \min_j \max_i \phi_{ij},$$

то есть выигрыш в ситуации равновесия (x_i^*, y_j^*) равен минимуму всех элементов строки i^* платежной матрицы и максимуму элементов столбца j^*. В этом случае игра имеет седловую точку, а общее значение максимина и минимакса называют ценой игры V. На практике часто возникает ситуация, когда игра не имеет седловой точки:

$$\underline{V} \le V \le \overline{V}.$$

В этом случае найти решение такой задачи в частных стратегиях не удается. Для подобных игровых задач решение существует в виде комбинированных стратегий, которые чередуются по случайному закону с определенной частотой. Распределение вероятностей на множестве чистых стратегий называют *смешанной стратегией*. Очевидно, что чистая стратегия является частным случаем смешанной.

Решение игры без седловой точки имеет две отличительные особенности, значительно затрудняющие принятие решений [6, 12-16]:

- смешанная стратегия не является гарантирующей;
- практическая реализация решения в смешанных стратегиях, как правило, невозможна.

Тем не менее, решение игры без седловой точки имеет практическое значение. Рассмотрение матричной игры, являющейся моделью реального процесса защиты информации, позволяет получить информацию о защищенности объектов АС.

Для построения модели процесса защиты информации на типовом объекте АС определим платежную функцию. В общем случае при реализации угрозы НСД возможны следующие ситуации [6, 18-22]:

- угроза НСД $x_i \in X$ реализуется на незащищенном объекте $S_k \in S$;
- угроза НСД $x_i \in X$ реализуется на объекте $S_k \in S$, оснащенном средством защиты информации $y_j \in Y$;
- угрозы НСД к информации на объекте $S_k \in S$ не реализуются.

Если l – количество объектов АС, то вероятность возникновения первой ситуации P_{ik} на объекте $S_k \in S$ равна

$$P_{ik} = \left[\sum_{k=1}^{l} h_{ik} \left(l - \sum_{k=1}^{l} h_{jk} \right) \right] / l^2.$$

Вероятность возникновения второй ситуации P_{ijk} на объекте $S_k \in S$ равна

$$P_{ijk} = \sum_{k=1}^{l} h_{ik} \sum_{k=1}^{l} h_{jk} / l^2.$$

Вероятность возникновения третьей ситуации P_{jk} на объекте $S_k \in S$ равна

$$P_{jk} = \left[\sum_{k=1}^{l} h_{jk} \left(l - \sum_{k=1}^{l} h_{ik} \right) \right] / l^2.$$

DOI: 10.7256/2305-6061.2015.1.14124

Очевидно, что в первой ситуации осуществление НСД позволит получить выигрыш C_{ik}, во второй – C_{ijk}. Выигрыш в третьей ситуации пропорционален затратам на защиту информации на объекте $S_k \in S$ и равен D_{jk}. При условии конечности множеств X и Y для каждого объекта $S_k \in S$ можно задать матричную игру с платежной функцией, равной математическому ожиданию выигрыша стороны, осуществляющей НСД:

$$\Phi^K(i,j) = \sum_{i=1}^{n} C_{ik} P_{ik} + \sum_{i=1}^{n} \sum_{j=1}^{m} C_{ijk} P_{ijk} + \sum_{j=1}^{m} D_{jk} P_{jk}.$$

Поиск решения по критерию гарантированного результата сводится к отысканию такого варианта распределения, при котором величина минимального по группе объектов эффекта достигает наибольшего значения. При этом оценивают не интегральную величину суммарного эффекта, а индивидуальный эффект на каждом объекте.

При рассмотрении процесса защиты информации объекта АС разумно предполагать, что стоимость любого варианта защиты мала по сравнению с информационной ценностью объекта. Тогда естественно считать, что $D_{jk} \approx 0$. После преобразований получим

$$\Phi^k(i,j) = A \sum_{i=1}^{n} \frac{C_k \mu_{ik}}{a_{ik}} \left[1 - \left(1 - \sum_{j=1}^{m} \gamma_{ijk} \right) \frac{B}{l} \sum_{j=1}^{m} \frac{1}{b_{jk}} \right].$$

При этом элементы задающей игру платежной матрицы определяют по формуле

$$\varphi_{ij}^k = \frac{A C_k \mu_{ik}}{a_{ik}} \left[1 - \left(1 - \gamma_{ijk} \right) \frac{B}{l b_{jk}} \right].$$

Решение игры с полученной платежной матрицей позволит выбрать лучшее средство защиты информации – если игра имеет седловую точку – или получить вероятности использования различных (лучших) наборов средств защиты информации (т.е. определить состав СЗИ объекта АС) – если существует решение в смешанных стратегиях. Однако задача принятия решений состоит в выборе набора этих средств из множества Y для достижения гарантированного результата. Для решения этой задачи предлагается на основе рассмотренной платежной матрицы построить новую матрицу игры, строки которой по-прежнему задают элементами множества НСД $x_i \in X$, а столбцы представлены возможными вариантами использования комплексов СЗИ.

Для m СЗИ количество возможных вариантов их использования w вычисляют по формуле $w = 2^m - 1$. Множество вариантов СЗИ обозначим $Z = \{ z_\theta \}$, $\theta = 1, \ldots, w$, причем $Z \supset Y$. Наличие средств $y_j \in Y$ в варианте $z_\theta \in Z$ определяется индикаторными переменными

$$h_{j\theta} = \begin{cases} 0, & \text{если средство } y_j \text{ не используется в варианте } z_\theta \\ 1, & \text{если средство } y_j \text{ используется в варианте } z_\theta \end{cases}.$$

DOI: 10.7256/2305-6061.2015.1.14124

Зависимость между номером варианта СЗИ θ и составом соответствующих средств $y_j \in Y$ описывается как

$$\sum_{j=1}^{m} h_{j\theta} 2^{j-1} = \theta \ .$$

Таким образом, каждый вариант СЗИ однозначно характеризуется индивидуальным набором средств $y_j \in Y$. Стоимость реализации защиты информации на объекте $S_k \in S$ равна алгебраической сумме стоимостей соответствующих СЗИ:

$$b_{\theta k} = \sum_{j=1}^{m} b_{jk} h_{j\theta} \ .$$

Предположим, что все средства из множества Y реализуют различные функции и не дублируют друг друга. Тогда коэффициент эффективности использования варианта СЗИ для новой матрицы, определяющей состав вариантов СЗИ, вычисляют по формуле

$$\gamma_{i\theta k} = \prod_{j=1}^{m} \gamma_{jk} h_{j\theta} \quad \forall h_{j\theta} = 1.$$

При этом элементы задающей игру платежной матрицы определяют соотношением

$$\varphi_{i\theta}^{k} = \frac{AC_k \mu_{ik}}{a_{ik}} \left[1 - \left(1 - \gamma_{j\theta k}\right) \frac{B}{lb_{\theta k}} \right].$$

Заключение

Применение разработанных моделей процесса защиты информации при реализации несанкционированного доступа, в отличие от аналогичных средств, обеспечивает соответствие СЗИ от НСД следующим требованиям:

- каждый вариант системы защиты характеризуется однозначной количественной оценкой, имеющей явный физический смысл (показатель защищенности), что позволяет выбрать конкретный вариант защиты объекта АС по критерию максимальной защищенности (при стоимостных ограничениях) или минимальной стоимости (при фиксированных требованиях по защищенности);
- рациональный выбор состава и структуры системы защиты при проектировании, а также при изменении исходных данных (перечень угроз, средств защиты, информационная ценность объектов АС) не требует значительных временных затрат.

Эти требования являются, по существу, основными функциональными требованиями к программному комплексу оценивания защищенности объектов АС, созданному нами на основе соответствующей методологии - «СЗИ Корректор».

Исходными данными для расчета являются: список объектов АС и стоимость обрабатываемой на них информации; список СЗИ и их стоимость; список вероятных методов реализации угроз НСД к информации, их стоимость и эффективность. После ввода исходных данных «СЗИ Корректор» производит расчет показателей эффективности вари-

DOI: 10.7256/2305-6061.2015.1.14124

антов СЗИ для введенных исходных данных, результатами которого являются наиболее эффективный вариант СЗИ для каждого объекта; значение показателя эффективности и стоимость каждого варианта СЗИ; перечень СЗИ с указанием: удовлетворяет ли этот вариант СЗИ ограничениям на общую стоимость СЗИ для всех объектов АС.

Таким образом, описанные модели процесса защиты информации при реализации НСД к ней являются формализованным описанием конфликтной ситуации и позволяет получить дополнительную информацию о возможных действиях потенциального противника и об их последствиях.

Библиография :

1. Богомолов А.В., Майстров А.И. Технология анализа системных причинно-следственных связей на основе диаграмм Исикавы // Системный анализ в медицине (САМ 2014): Материалы VIII международной научной конференции. Благовещенск, 2014. С. 13-16.
2. Богомолов А.В., Чуйков Д.С., Запорожский Ю.А. Средства обеспечения безопасности информации в современных автоматизированных системах // Информационные технологии. 2003. № 1. С.2-8.
3. Бородакий Ю.В., Воробьев А.А., Куликов Г.В., Непомнящих А.В. Оценивание защищенности от информационных воздействий автоматизированных систем управления: теория и практика // Безопасность информационных технологий. 2005. №4. С. 61.
4. Бусленко Н.П. Моделирование сложных систем. М.: Наука, 1978. 355 с.
5. Владимирова Т.В. К социальной природе понятия «информационная безопасность» // Вопросы безопасности. 2013. №4. С. 78-95. DOI: 10.7256/2409-7543.2013.4.596. URL: http://www.e-notabene.ru/nb/article_596.html
6. Воробьев А.А., Куликов Г.В., Непомнящих А.В. Оценивание защищенности автоматизированных систем на основе методов теории игр // Информационные технологии. 2007. Приложение к № 1. 24 с.
7. Голосовский М.С. Модель жизненного цикла разработки программного обеспечения в рамках научно-исследовательских работ // Автоматизация и современные технологии. 2014. № 1. С. 43-46.
8. Грушо А.А., Грушо Н.А., Тимонина Е.Е., Шоргин С.Я. Безопасные архитектуры распределенных систем // Системы и средства информатики. 2014. № 24. С. 18-31.
9. Загузов Г.В. Административно-правовые средства обеспечения информационной безопасности и защиты информации в Российской Федерации // Административное и муниципальное право.-2010.-5.-С. 44-47.
10. Козлов В.Е., Богомолов А.В., Рудаков С.В., Оленченко В.Т. Математическое обеспечение обработки рейтинговой информации в задачах экспертного оценивания // Мир измерений. 2012. № 9. С. 42-49.
11. Коломиец Л.В., Федоров М.В., Богомолов А.В., Мережко А.Н., Солдатов А.С., Есев А.А. Метод поддержки принятия решений по управлению ресурсами при испытаниях авиационной техники // Информационно-измерительные и управляющие системы. 2010. Т. 8. № 5. С. 38-40.
12. Кукушкин Ю.А., Богомолов А.В., Ушаков И.Б. Математическое обеспечение оценивания состояния материальных систем // Информационные технологии. 2004. Приложение к № 7. 24 с.

DOI: 10.7256/2305-6061.2015.1.14124

13. Куликов Г.В., Непомнящих А.В. Метод составления наиболее полного перечня угроз безопасности информации автоматизированной системы // Безопасность информационных технологий. 2005. № 1. С. 47-50.
14. Куликов Г.В., Непомнящих А.В. Методика оценивания функциональных возможностей систем обнаружения вторжений // Информационные технологии. 2006. № 1. С. 31–36.
15. Куликов Г.В., Непомнящих А.В., Соснин Ю.В., Нащёкин П.А. Особенности технологий динамической защиты информационных ресурсов автоматизированных систем управления // Вопросы защиты информации. 2013. № 4 (102). С. 39-44.
16. Куликов Г.В., Соснин Ю.В., Непомнящих А.В., Нащекин П.А. Моделирование процесса защиты информации при реализации несанкционированного доступа к ней // Вестник компьютерных и информационных технологий. 2014. № 4 (118). С. 45-51.
17. Максимов И.Б., Столяр В.П., Богомолов А.В. Прикладная теория информационного обеспечения медико-биологических исследований. М.: Бином, 2013. 312 с.
18. Меньших В.В., Ковальчук А.А. Оценки уязвимости и опасности распространения угроз информационной безопасности в телекоммуникационных системах // Информационная безопасность регионов. 2013. № 2 (13). С. 17-22.
19. Меньших В.В., Пастушкова Е.А. Методы оценки вариантов принятия решений в системах управления с функционально избыточным набором действий // Вестник Воронежского института МВД России. 2014. № 3. С. 48-57.
20. Рудаков И.С., Рудаков С.В., Богомолов А.В. Методика идентификации вида закона распределения параметров при проведения контроля состояния сложных систем // Информационно-измерительные и управляющие системы. 2007. Т. 5. № 1. С. 66-72.
21. Сизоненко А.Б., Меньших В.В. Оптимальная реализация автоматной модели защищенной информационной системы путем представления логических функций полиномиальными формами // Информация и безопасность. 2012. Т. 15. № 2. С. 225-230.
22. Соловьев С.В., Затока И.В., Ещенко Е.В. Показатели качества защищенных информационных систем в области технической защиты информации // Телекоммуникации. 2012. № 5. С. 24-30.
23. Ушаков И.Б., Богомолов А.В. Информатизация программ персонифицированной адаптационной медицины // Вестник Российской академии медицинских наук. №5-6, 2014. С. 124-128.
24. Фёдоров М.В., Калинин К.М., Богомолов А.В., Стецюк А.Н. Математическая модель автоматизированного контроля выполнения мероприятий в органах военного управления // Информационно-измерительные и управляющие системы. 2011. Т. 9. № 5. С. 46-54.
25. Харьков В.П. Построение оптимальных алгоритмов управления нелинейными динамическими системами // Инновации на основе информационных и коммуникационных технологий. 2013. Т. 1. С. 278-281.
26. Харьков В.П., Меркулов В.И. Формирование заданной конфигурации сложной распределенной системы управления // Радиотехника. 2011. № 6. С. 96-101.
27. Чиров Д.С. Методический подход к обоснованию технических характеристик комплексов радиомониторинга для решения задач распознавания источников радиоизлучения // T-Comm: Телекоммуникации и транспорт. 2011. Т. 5. № 11. С. 85-87.

DOI: 10.7256/2305-6061.2015.1.14124

28. Чиров Д.С., Терешонок М.В., Елсуков Б.А. Метод и алгоритмы оптимизации технических характеристик комплексов радиомониторинга // T-Comm: Телекоммуникации и транспорт. 2014. Т. 8. № 10. С. 88-92.
29. Шелков А.Б., Шульц В.Л., Кульба В.В. Аудит информационной безопасности автоматизированных систем управления // Тренды и управление. 2014. №4. С. 319-334. DOI: 10.7256/2307-9118.2014.4.10281.

References:

1. Bogomolov A.V., Maistrov A.I. Tekhnologiya analiza sistemnykh prichinno-sledstvennykh svyazei na osnove diagramm Isikavy // Sistemnyi analiz v meditsine (SAM 2014): Materialy VIII mezhdunarodnoi nauchnoi konferentsii. Blagoveshchensk, 2014. S. 13-16.
2. Bogomolov A.V., Chuikov D.S., Zaporozhskii Yu.A. Sredstva obespecheniya bezopasnosti informatsii v sovremennykh avtomatizirovannykh sistemakh // Informatsionnye tekhnologii. 2003. № 1. S.2-8.
3. Borodakii Yu.V., Vorob'ev A.A., Kulikov G.V., Nepomnyashchikh A.V. Otsenivanie zashchishchennosti ot informatsionnykh vozdeistvii avtomatizirovannykh sistem upravleniya: teoriya i praktika // Bezopasnost' informatsionnykh tekhnologii. 2005. №4. S. 61.
4. Buslenko N.P. Modelirovanie slozhnykh sistem. M.: Nauka, 1978. 355 s.
5. Vladimirova T.V. K sotsial'noi prirode ponyatiya «informatsionnaya bezopasnost'» // Voprosy bezopasnosti. 2013. №4. C. 78-95. DOI: 10.7256/2409-7543.2013.4.596. URL: http://www.e-notabene.ru/nb/article_596.html
6. Vorob'ev A.A., Kulikov G.V., Nepomnyashchikh A.V. Otsenivanie zashchishchennosti avtomatizirovannykh sistem na osnove metodov teorii igr // Informatsionnye tekhnologii. 2007. Prilozhenie k № 1. 24 s.
7. Golosovskii M.S. Model' zhiznennogo tsikla razrabotki programmnogo obespecheniya v ramkakh nauchno-issledovatel'skikh rabot // Avtomatizatsiya i sovremennye tekhnologii. 2014. № 1. S. 43-46.
8. Grusho A.A., Grusho N.A., Timonina E.E., Shorgin S.Ya. Bezopasnye arkhitektury raspredelennykh sistem // Sistemy i sredstva informatiki. 2014. № 24. S. 18-31.
9. Zaguzov G.V. Administrativno-pravovye sredstva obespecheniya informatsionnoi bezopasnosti i zashchity informatsii v Rossiiskoi Federatsii // Administrativnoe i munitsipal'noe pravo.-2010.-5.-C. 44-47.
10. Kozlov V.E., Bogomolov A.V., Rudakov S.V., Olenchenko V.T. Matematicheskoe obespechenie obrabotki reitingovoi informatsii v zadachakh ekspertnogo otsenivaniya // Mir izmerenii. 2012. № 9. S. 42-49.
11. Kolomiets L.V., Fedorov M.V., Bogomolov A.V., Merezhko A.N., Soldatov A.S., Esev A.A. Metod podderzhki prinyatiya reshenii po upravleniyu resursami pri ispytaniyakh aviatsionnoi tekhniki // Informatsionno-izmeritel'nye i upravlyayushchie sistemy. 2010. T. 8. № 5. S. 38-40.
12. Kukushkin Yu.A., Bogomolov A.V., Ushakov I.B. Matematicheskoe obespechenie otsenivaniya sostoyaniya material'nykh sistem // Informatsionnye tekhnologii. 2004. Prilozhenie k № 7. 24 s.
13. Kulikov G.V., Nepomnyashchikh A.V. Metod sostavleniya naibolee polnogo perechnya ugroz bezopasnosti informatsii avtomatizirovannoi sistemy // Bezopasnost' informatsionnykh tekhnologii. 2005. № 1. S. 47-50.
14. Kulikov G.V., Nepomnyashchikh A.V. Metodika otsenivaniya funktsional'nykh vozmozhnostei sistem obnaruzheniya vtorzhenii // Informatsionnye tekhnologii. 2006. № 1. S. 31–36.

15. Kulikov G.V., Nepomnyashchikh A.V., Sosnin Yu.V., Nashchekin P.A. Osobennosti tekhnologii dinamicheskoi zashchity informatsionnykh resursov avtomatizirovannykh sistem upravleniya // Voprosy zashchity informatsii. 2013. № 4 (102). S. 39-44.
16. Kulikov G.V., Sosnin Yu.V., Nepomnyashchikh A.V., Nashchekin P.A. Modelirovanie protsessa zashchity informatsii pri realizatsii nesanktsionirovannogo dostupa k nei // Vestnik komp'yuternykh i informatsionnykh tekhnologii. 2014. № 4 (118). S. 45-51.
17. Maksimov I.B., Stolyar V.P., Bogomolov A.V. Prikladnaya teoriya informatsionnogo obespecheniya mediko-biologicheskikh issledovanii. M.: Binom, 2013. 312 s.
18. Men'shikh V.V., Koval'chuk A.A. Otsenki uyazvimosti i opasnosti rasprostraneniya ugroz informatsionnoi bezopasnosti v telekommunikatsionnykh sistemakh // Informatsionnaya bezopasnost' regionov. 2013. № 2 (13). S. 17-22.
19. Men'shikh V.V., Pastushkova E.A. Metody otsenki variantov prinyatiya reshenii v sistemakh upravleniya s funktsional'no izbytochnym naborom deistvii // Vestnik Voronezhskogo instituta MVD Rossii. 2014. № 3. S. 48-57.
20. Rudakov I.S., Rudakov S.V., Bogomolov A.V. Metodika identifikatsii vida zakona raspredeleniya parametrov pri provedeniya kontrolya sostoyaniya slozhnykh sistem // Informatsionno-izmeritel'nye i upravlyayushchie sistemy. 2007. T. 5. № 1. S. 66-72.
21. Sizonenko A.B., Men'shikh V.V. Optimal'naya realizatsiya avtomatnoi modeli zashchishchennoi informatsionnoi sistemy putem predstavleniya logicheskikh funktsii polinomial'nymi formami // Informatsiya i bezopasnost'. 2012. T. 15. № 2. S. 225-230.
22. Solov'ev S.V., Zatoka I.V., Eshchenko E.V. Pokazateli kachestva zashchishchennykh informatsionnykh sistem v oblasti tekhnicheskoi zashchity informatsii // Telekommunikatsii. 2012. № 5. S. 24-30.
23. Ushakov I.B., Bogomolov A.V. Informatizatsiya programm personifitsirovannoi adaptatsionnoi meditsiny // Vestnik Rossiiskoi akademii meditsinskikh nauk. №5-6, 2014. S. 124-128.
24. Fedorov M.V., Kalinin K.M., Bogomolov A.V., Stetsyuk A.N. Matematicheskaya model' avtomatizirovannogo kontrolya vypolneniya meropriyatii v organakh voennogo upravleniya // Informatsionno-izmeritel'nye i upravlyayushchie sistemy. 2011. T. 9. № 5. S. 46-54.
25. Khar'kov V.P. Postroenie optimal'nykh algoritmov upravleniya nelineinymi dinamicheskimi sistemami // Innovatsii na osnove informatsionnykh i kommunikatsionnykh tekhnologii. 2013. T. 1. S. 278-281.
26. Khar'kov V.P., Merkulov V.I. Formirovanie zadannoi konfiguratsii slozhnoi raspredelennoi sistemy upravleniya // Radiotekhnika. 2011. № 6. S. 96-101.
27. Chirov D.S. Metodicheskii podkhod k obosnovaniyu tekhnicheskikh kharakteristik kompleksov radiomonitoringa dlya resheniya zadach raspoznavaniya istochnikov radioizlucheniya // T-Comm: Telekommunikatsii i transport. 2011. T. 5. № 11. S. 85-87.
28. Chirov D.S., Tereshonok M.V., Elsukov B.A. Metod i algoritmy optimizatsii tekhnicheskikh kharakteristik kompleksov radiomonitoringa // T-Comm: Telekommunikatsii i transport. 2014. T. 8. № 10. S. 88-92.
29. Shelkov A.B., Shul'ts V.L., Kul'ba V.V. Audit informatsionnoi bezopasnosti avtomatizirovannykh sistem upravleniya // Trendy i upravlenie. 2014. №4. C. 319-334. DOI: 10.7256/2307-9118.2014.4.10281.

DOI: 10.7256/2305-6061.2015.1.14124