***В.А. Хвостов*[1], *В.П. Гулов*[2]**

К ВОПРОСУ ОБ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

[1]*ФГБОУ ВО Воронежский государственный университет инженерных технологий,*
[2]*ФГБОУ ВО ВГМУ им. Н.Н. Бурденко Минздрава России*

Резюме. Предложен нормативный метод обоснования требований к информационной безопасности персональных данных (ПДн), обрабатываемых в медицинских учреждениях с применением автоматизированных систем (АС). Метод основан на количественной оценке показателей защищенности информации, анализе их влияния на процессы, протекающие в защищаемой системе при выполнении основных технологических операций управления, полное множество угроз безопасности информации и обеспечивает с системных позиций оптимальность количественных требований к системам защиты информации (СЗИ).

Ключевые слова: средства защиты информации, методы нормирования, модель защиты, несанкционированный доступ.

Вопросы обоснования требований к СЗИ АС являются из одними из важнейших задач защиты персональных данных (ПДн). Эта особенность проблемы защиты ПДн обусловлена значительным влиянием степени (уровня) защищенности (“защиты ”) конфиденциальных данных на общий уровень качества функционирования автоматизированных систем (АС), и соответственно, на эффективность работы медицинской организации в целом. Актуальность задачи обоснования требований к системам защиты информации (СЗИ) АС определена тем, что в результате ее решения появляется возможность оптимизации ресурсов АС, выделяемых на обеспечение эксплуатации (функционирования) СЗИ при обеспечении неизменности требуемой эффективности АС при решении основных функциональных задач в технологическом цикле работы организации.

Важнейшей особенностью СЗИ является обязательность использование на каждом технологическом этапе работы и при любом режиме системы. Глубинное интегрирование СЗИ в состав АС по функциям и ресурсам определяет такое же глубокое влияние показателей характеризующих систему защиты информации на показатели эффективности защищаемой системы. При этом важнейшим показателем СЗИ, как любой системы, является ее эффективность (достигнутый уровень БИ). Поэтому при проектировании (модернизации) АС в защищенном исполнении требуется детальный учет уровня БИ, обеспечиваемого СЗИ.

В настоящее время методологической основой обоснования требований к СЗИ при разработке на всех этапах выступают руководящие документы (РД) Федеральной службы технического и экспортного контроля России (ФСТЭК) [1-3]. Задание требований, в соответствие с [1-3], заключается в выборе необходимого класса защищенности исходя из условий эксплуатации и уровня конфиденциальности и обеспечения выполнения требований этого класса в виде совокупности организационных и технических мероприятий по защите ПДн. Вновь вводимый в России международный стандарт «Общие критерии оценки безопасности информационных технологий» ISO / IEC 15408: 1999. “Информационная технология — Методы и средства защиты информации — Критерии оценки безопасности

информационных технологий” «Общие критерии» (ОК) использует аналогичный подход. Отличием является и [4].

Из анализа этих документов видно, что категория эффективности СЗИ в них не присутствует.

В связи с этим возникает проблема, состоящая в том, что учет характеристик БИ при проектировании АС не находит прямого отражения в практике при обосновании требований к БИ в методах используемых в настоящее время.

Причина лежит в принципиальных теоретических трудностях применения существующих методов обоснования требований к СЗИ, особенно из-за отсутствия методик оценки и обоснования требований к качеству обеспечения БИ и норм безопасности информации, показателей и критериев. Природа этих трудностей может быть определена как противоречие между необходимостью опираться при построении АС в защищенном исполнении на строго научные методы анализа и синтеза СЗИ, во первых, как методологической основы современной системотехники, а во вторых, исходя из требований самого процесса проектирования и построения АС, требующей количественного рассмотрения вопросов обеспечения БИ. С другой стороны, существующий подход к формированию требований базируется на качественном формировании перечня требуемых к реализации функций безопасности, обеспечивающий только полноту, достаточность и непротиворечивость защиты информации и не как не связанный с категориями эффективность.

Разрешение рассмотренной проблемы в рамках традиционной «классификационной» общенаучной парадигмы теории защиты информации невозможно. В качестве решения авторам видится необходимость разработки теоретических основ и технологии обоснования количественных норм безопасности информации на основе оценки эффективности защиты информации обеспечивающих максимальный уровень защищенности при минимальном влиянии системы защиты на эффективность автоматизированной системы в условиях реализации полного множества угроз безопасности информации.

Таким образом, целью статьи является разработка и исследование нормативного метода обоснования требований к БИ АС обеспечивающего возможность синтеза и анализа СЗИ с использованием количественных показателей и учитывающих архитектурные особенности реализации защищаемой системы в условиях реализации полного множества угроз.

В обобщенном виде технологию обоснования требований к СЗИ с использованием нормативного метода можно представить в виде показанном на рис. 1.

Технология нормирования базируется на двух совокупностях исходных данных: структурной схеме АС и модели полного множества угроз БИ, характерной для АС.

Необходимо отметить существующее в настоящее время многообразие АС разных видов, характеризующихся, в том числе, и разнообразием технической структуры и модели полного множества угроз БИ, характерной для АС.

Поэтому при построении технологии нормирования необходимо предварительное проведение типизации структуры и реализация нормы безопасности к ней.

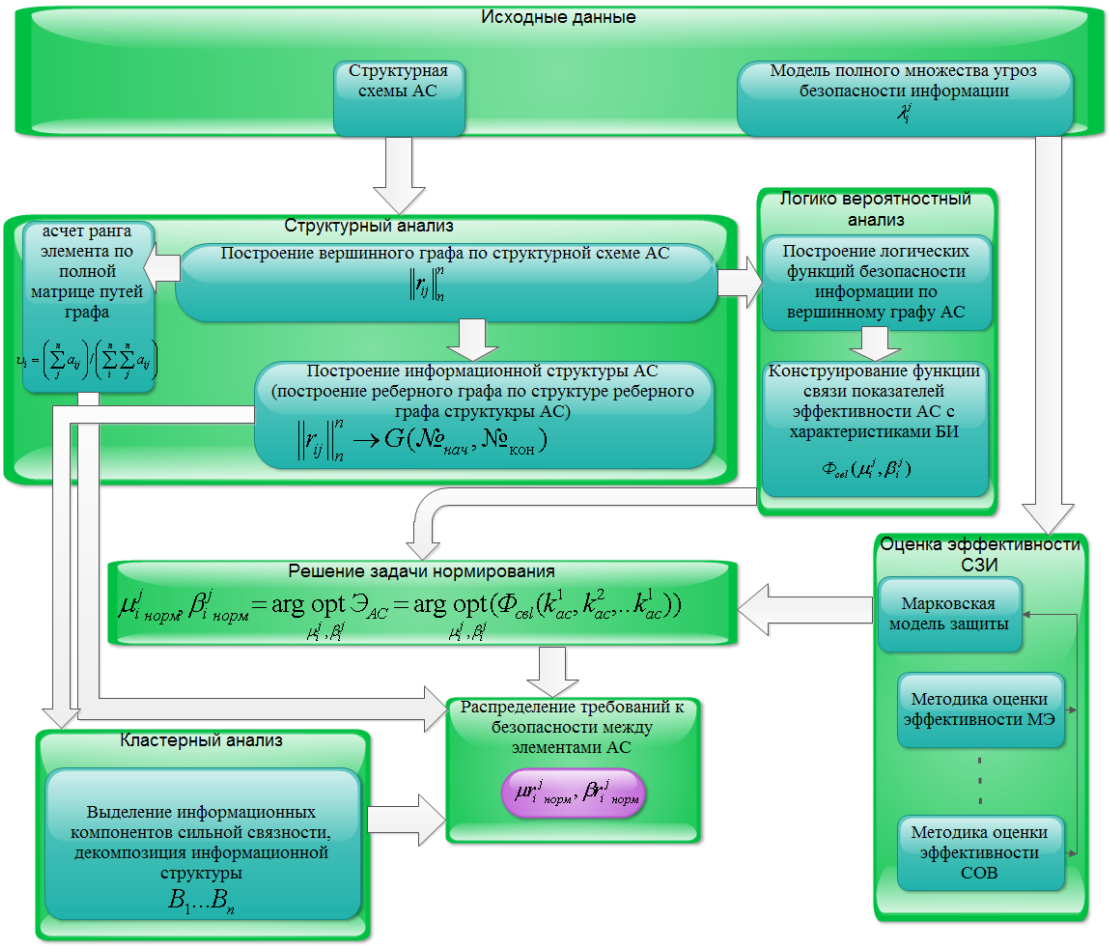

Рис. 1 Обобщенная схема нормирования требований к СЗИ

Структура АС определяется ее основными функциональными частями, их информационными связями и назначением. Выделенные в структуре функциональные части можно определить как функциональные блоки. Под понятием блок традиционно понимается устройство, законченное функционально и выделенное в виде отдельного целостного устройства.

Главным принципом выделения блока при синтезе информационно-логических схемы АС является возможность описания АС функционального блока и одностороняя направленность передачи результатов расчетов.

Методика синтеза структуры АС разработана в [5] состоит следующих этапов.

1. В структуре системы выделяются блоки, изображаемые как условные символы с фиксацией ролей блока в АС.

2. Связи по информации, необходимые для проведения анализа АС, отображаются как линии между блоками.

3. С помощью стрелок на линиях связи отображаются отношения между блоками определяемые направленностью процессов обработки информации в АС.

Для построения модели полного множества угроз БИ используется математический аппарат логических деревьев атак [6] с присвоением дугам дерева числовых коэффициентов, имеющих временной смысл.

Основой конструкцией при этом выбрано иерархическое дерево вида *G = (L, E),* где $L = \{l_i\}$ — вершины дерева, $E = \{e_s\}$, $E \in \{L^2\}$ –дуги дерева.

Каждая из вершин иерархического дерева *G* обозначает определенное действие злоумышленника. Корень дерева ассоциируется с конечной целью угрозы БИ, с реализацией которой может быть нанесен существенный ущерб. Поэтому, с использованием иерархического графа G позволяет формализовать все возможные пути $Gp = \{gp_r\}$. Каждый путь gp_r является последовательностью дуг $(e_1, e_2, ...e_n)$ имеющий вид $e_i = (l_i, l_j)$, $l_i, l_j \in L$. Конечная вершина дуги l_i. связана с начальными вершинами дуг l_{i+1}. Начальные вершины пути рассматриваются как листья дерева *G*, а конечная вершина — корень дерева *G*.

Деревья атак удобно формализовать в графическом и текстовом виде. Корни дерева — вершины $l_0 \in L$ — обозначают этапы реализации угрозы БИ. Для реализации этой угрозы БИ атакующий должен реализовать операции, обозначенные элементами $\{l_i \in L\}_{i[1,n]}$. Последовательность действий нарушителя, обозначается индексом вершины $\{l_i \in L\}_{i[1,n]}$. Первым реализуется шаг, обозначенный вершиной $l_1 \in L$, последним — $l_n \in L$.

Разработанная модель угроз БИ, построенная с применением математического аппарата теории деревьев, позволяет формализовать сложные многовариантные и многоэтапные сценарии атаки. В интересах количественной оценки опасности угрозы каждой дуге дерева сопоставлен параметр времени реализации этапа угрозы БИ, определяемого дугой.

Модель анализируемого множества угроз БИ формализуется множеством параметров вида $\lambda_i^j = 1/t_i^j$ для каждой из рассмотренных угрозы БИ.

Построенная структурная схема АС, в свою очередь, нуждается в формализации [7]. При этом элементам структурной схемы АС ставятся в соответствие вершины графа вида $X = \{x_1, x_2, ...x_n\}$. Связи между элементами обозначаются дугами графа $U = \{u_1, u_2, ...u_m\}$. Полученный вершинный граф полностью соответствует структуре системы, характеризуемый матрицей смежности $\|r_{ij}\|_n^n$. Модели систем, представленные в виде вершинных графов, используются для построения и анализа информационной структуры АС, для расчета ранга элемента в структуре и для конструирования функций связи показателей информационной безопасности элементов структуры с показателями эффективности АС по прямому назначению $\Phi_{свl}(\mu_i^j, \beta_i^j, \nu_i^j)$.

При построении информационной структуры АС используется реберный граф той же системы. Реберные графы сопоставляют свойства элементов, определяемые обрабатываемой в них информации дугам графа, а логические аспекты их работы – вершинам. Использование реберных графов реализует формальные методы анализа

структуры. При этом описания структур могут использовать разнообразные логические функции.

Преобразование вершинного графа архитектуры АС в ее реберный граф реализуется с применением теоремы эквивалентности матрицы смежности вершинного и реберного графа [8].

Методика, преобразования вершинного графа в реберный граф состоит из трех этапов: вначале строится квазиканоническая матрица смежности реберного графа; далее проводится нумерация вершин реберного графа; с использованием квазиканонической матрицы смежности реберного графа строится реберный граф.

Полученный в результате преобразования реберный граф, эквивалентный вершинному графу ($\|r_{ij}\|_n^n \to G(№_{нач}, №_{кон})$), соответствует информационной структуре АС и математически представляет собой орграф $G(№_{нач}, №_{кон})$.

При расчете ранга элемента в структуре вершинный граф является основой для определения полной матрицы путей [9]. Чем большим числом путей элемент связан с другими элементами, тем большее число элементов структуры прекращает адекватно работать при реализации угрозы БИ к этому элементу. Поэтому важность рассматриваемого элемента в структуре определяется количеством его связей. Таким образом, нормировании требований к безопасности информации элементов АС, часть заданного общего уровня безопасности должна быть определена с учетом количества связей. Одним из простейших в реализации методов построения матрицы путей является метод с использованием алгебры квазиминоров. Метод применяется при построении матрицы путей ориентированных графов без петель и кратных дуг.

Способ на основе матрицы смежности вершин графа $\|r_{ij}\|_n^n$ осуществляет построение матрицы непосредственных путей. С использованием $\|r_{ij}\|_n^n$ с помощью алгебры квазиминоров осуществляется построение полной матрицы путей графа. Ранг элемента рассчитывается с использованием полной матрицы путей с использованием следующей формулы:

$$\upsilon_i = \left(\sum_j^n a_{ij}\right) / \left(\sum_i^n \sum_j^n a_{ij}\right);$$

где a_{ij} — элементы полной матрицы путей графа соответствующего технической структуре АС.

Конструирование функций связи показателей информационной безопасности элементов структуры с показателями эффективности АС по прямому назначению $\Phi_{свI}(\mu_i^j, \beta_i^j, \nu_i^j)$ возможно с использованием логико-вероятностного метода [9]. В основе метода используется математический аппарат булевой алгебры на первом этапе построения функций связей структурно сложных систем. Как и при проведении расчетов надежности сложных систем при применении логико-вероятностного метода, функция связи строится в три этапа.

Этап 1. Элементам системы сопоставляются логические переменные x_i, принимающие два значения: 1, элемент находится в безопасном состоянии и 0, если безлопастное состояние элемента нарушено. Далее на основе анализа условий работоспособности при реализации угрозы БИ к элементу синтезируется ЛФИБ следующего вида $F(X)$ где $X=(x_1,x_2,...x_n)$ является вектор-строкой логических переменных. Значение функция $F(X)=1$, при наличии хотя бы одного безопасного пути от входного элемента к выходному. Примем постулат о том что путь безопасен, при безопасных всех входящих в него элементов. Для каждого пути в ЛФИБ поставлена в соответствие элементарная конъюнкция переменных x_n, в соответствии с входящими в путь элементами. Логические функции информационной безопасности являются дизъюнкциями, элементарных конъюнкций возможных путей между входными и выходными элементами. Полученная форма ЛФИБ является исходной для проведения дальнейшего анализа.

Этап 2. Полученная форма ЛФИБ преобразуется к стандартной форме перехода для полного замещения логических переменных вероятностями и логических операций арифметическими операциями.

Этап 3. Логическая переменная x_i замещаетс вероятностью $p_i=P(x_i)$, отрицание логической переменной $\bar{x}_i$ замещается вероятностью $q_i=1-p_i=P(x_i=0)$, дизъюнкции $\vee$ замещаются сложением +, конъюнкции $\wedge$ замещаются умножением $\times$, логическое отрицание $\neg y$ замещается вычитанием из единицы вида $1-P(y=1)$.

Информационная структура АС является основой для проведения анализа в интересах выделения сильно связанных элементов — декомпозиции информационной структуры системы [9]. При этом в информационной структуре необходимо выделять составные подсистемы, элементы которых взаимно достижимы. Выделение сильно связанных и слабосвязанных информационных элементов позволяет осуществить кластеризацию информационных объектов в интересах оптимального использования СЗИ. Процесс декомпозиции информационной структуры можно формализовать сокращением ориентированного графа. Результатом декомпозиции информационной структуры АС является множество кластера информационных объектов, характеризуемых сильной связностью $\{B_1...B_n\}$, используемых при обосновании комплекта средств защиты.

Задача нормирования характеристик защищенности объектов от НСД формулируется как:

Найти вектор качества системы защиты информации $\vec{K}=\langle k_1,k_2,...k_p\rangle$, удовлетворяющий множеству $\{У,\mathrm{O_s},S,O_k,\Phi_c\}$ и обладающему характеристиками наилучшего при использовании выбранного критерия предпочтений.

k_i — числовые характеристики защиты, определяемы эффективностью СЗИ как монотонная зависимость. При уменьшении k_i система лучше при прочих равных

условиях. Таким образом, при неизменных значениях $\{У, О_s, S, O_k, Ф_c, О_э\}$ и неизменных остальных $m-1$ показателях качества СЗИ.

$У$ — условия применения СЗИ в виде вектора $У = \{У_1, У_2, ...У_l\}$;

$О_s$ — множество ограничений на архитектуру и характеристики СЗИ, вектор вида $О_s = \{O_{s1}, O_{s2}, ...O_{sq}\}$;

S — множество СЗИ (реализуемых или проектируемых вариантов построения системы). Вектор вида $S = \{S_1, S_2, ...S_d\}$. Где d — величина, описывающая допустимое множество СЗИ (существующих и перспективных);

O_k — вектор ограничений на показатели качества вида $O_k = \{O_{k1}, O_{k2}, ...O_{kh}\}$. В случае использования вероятностных показателей качества ограничения принимаются в виде диапазона $0 < O_i < 1$.

$Ф_c$ —функция связи вектора показателей количественных характеристик защиты и эффективности АС.

в качестве целевой функции при решении задачи нормирования, целесообразно использовать марковскую модель защиты [10, 11]. Модель защиты формализует полное множества угроз БИ к информации при реализации ряда мер по обеспечению БИ.

Модель защиты, используется для проведения количественной оценки целевой функции БИ различных вариантов угроз и механизмов защиты в виде:

$$P_{нсд} = \prod_{i=1}^{3}(1-1/(1+\sum_{j=1}^{n,k,m}\frac{\lambda_i^j}{\mu_i^j}(1+\beta_i^j\frac{\mu_i^j}{\nu_i^j})))$$

i — этапы выполнения угрозы БИ;

j — способы i –го этапа реализации формализуются экспоненциальным распределением с параметрами λ_{ij};

β_i^j — вероятность необнаружения СЗИ угроз БИ при j – гом способе i –го этапа реализации;

ν_i^j — среднее время задержки обнаружения действий злоумышленника j – тым способом i –го этапа угрозы;

μ_i^j — среднее время нейтрализации обнаруженных действий j – го способа i –го этапа реализации угрозы;

n, k, m —способы реализации угроз НСД для первого, второго и третьего этапа.

Числовые значения λ_i^j рассчитываются на основе анализа исходных данных модели полного множества угроз БИ [10].

Методика нормирования основана на решении задачи нормирования требований к количественным характеристикам БИ, при использовании марковской модели защиты, может быть осуществлена с использованием методов принятия решений.

Поскольку уровень БИ АС системы определяется уровнями БИ ее элементов, то завершением процесса нормирования является рациональным распределением интегрального уровня требований по БИ к АС в целом между ее составляющими элементами.

Решение задачи нормирования требований к безопасности основных элементов АС при заданном общем уровне безопасности основано в обоснованном выборе значений весовых коэффициентов υ_i, выполненном при расчете ранга элемента по полной матрице путей [12]. При наличии оценок рангов υ_i элементов можно записать математическое выражение для максимального значения эффективности АС:

$$Э_{\max} = \overline{\Phi}_{св}(\mu_i^j{}_{норм}, \beta_i^j{}_{норм}, \nu_i^j{}_{норм}) = \overline{\Phi}_{св}(\sum_k \upsilon_k(\mu_{ik}^j{}_{норм}, \beta_{ik}^j{}_{норм}, \nu_{ik}^j{}_{норм}))$$

Исходя из независимости показателей СЗИ $\mu_i^j, \beta_i^j, \nu_i^j$, положенной в основу при разработке целевой функции в главе 2:

$$\mu_i^j{}_{норм} = \sum_k \upsilon_k \mu_{ik}^j{}_{норм}, \quad \beta_i^j{}_{норм} = \sum_k \upsilon_k \beta_{ik}^j{}_{норм}, \quad \nu_i^j{}_{норм} = \sum_k \upsilon_k \nu_{ik}^j{}_{норм}$$

Исходя из этого:

$$\mu_{ik}^j{}_{норм} = \upsilon_k \mu_i^j{}_{норм}, \beta_{ik}^j{}_{норм} = \upsilon_k \beta_i^j{}_{норм}, \nu_{ik}^j{}_{норм} = \upsilon_k \nu_i^j{}_{норм}.$$

Выводы. Таким образом, предложена технология нормирования разработанная применительно к типовым структурам АС и характерным для этих типовых структур модели полного множества угроз БИ. При нормировании последовательно проводится структурный анализ архитектуры АС, выделение кластеров информационных объектов, определение рангов элементов, и конструирование функций связи показателей информационной безопасности элементов структуры с показателями эффективности АС по прямому назначению логико-вероятностным методом.

Нормирование требований осуществляется применительно к марковской модели защиты с последовательным использованием метода модифицированных рабочих характеристик и условного минимаксного критерия.

Полученные значения интегральной нормы безопасности оптимально распределяются между элементами АС с использованием полученных на этапе структурного анализа значений рангов элементов.

Литература.1. Гостехкомиссия РФ. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. М.: Воениздат, 1992.

2. Гостехкомиссия РФ. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. - М.: Воениздат, 1992.

3. Гостехкомиссия РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. - М.: Воениздат, 1992.

4. ГОСТ Р ИСО / МЭК 15408-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. - М.: ИПК Издательство стандартов, 2002 40 с.

5. Липаев В.В. Качество программного обеспечения. – М.: Финансы и статистика. – 1983 г. – 250 с.

6. Модель полного множества реализаций угроз информационной безопасности в ИТКС / Хвостов В.А. [и др.] // Вестник Воронежского государственного технического университета. – 2011. – Т.7 №6 – С. 126 — 130.

7. Методы и средства повышения защищенности автоматизированных систем: монография / Е.А. Рогозин, В.А. Хвостов [и др.]. – Воронеж: Воронежский институт МВД России, 2013. – 108 с.

8. Метод построения информационной структуры автоматизированной системы при нормировании требований к информационной безопасности / Макаров О.,Ю., Рогозин Е.А., Хвостов В.А. // Вестник Воронежского государственного технического университета. – 2011. – Т.7 №9 – С. 61 – 64.

9. Алгоритм кластеризации организационно-технических систем биологической деятельности, для которых предусмотрена защита информации / В.П. Гулов, В.А. Хвостов // Прикладные информационные аспекты медицины: межвуз. сб. науч. тр. – Воронеж: ВГМА им. Н.Н. Бурденко, 2011. – Т. 14 № 2 – С. 12 – 17.

10. Методика оценки вероятности несанкционированного доступа в автоматизированные системы, использующие протокол TCP / IP / О.Ю. Макаров, Е.А. Рогозин, В.А. Хвостов // Информация и безопасность – 2009. – Т. 12 №2 С. 285 –288.

11. Об одном способе формализации понятия стойкости функции безопасности ГОСТ ИСО / МЭК 15408 / О.Ю. Макаров, Е.А. Рогозин В.А. Хвостов // Вестник Воронежского государственного технического университета. – 2009. – Т.5 №2 – С. 94 – 98.

12. Нормирование требований к основным элементам автоматизированной системы информационной безопасности / С.В. Белокуров, А.А. Змеев, В.А. Хвостов // Проблемы обеспечения надежности и качества приборов устройств и систем: межвуз. сб. науч. тр. – Воронеж: ВГТУ, 2012. – С. 29 – 31.

Abstract.

V.A. Hvostov, V.P. Gulov

MODELS AND ALGORITHMS OF STANDARD METHOD OF JUSTIFICATION OF REQUIREMENTS TO SAFETY OF PERSONAL DATA IN MEDICAL INFORMATION SYSTEMS

Voronezh State University of engineering technologies , Voronezh State Medical University

This paper proposes a method of justifying regulatory requirements for information security automated systems. The method is based on quantifiable indicators of information security, analysis of their influence on the processes occurring in the protected system in basic manufacturing operations management, a complete set of security threats and provides information to the system positions optimal quantitative requirements for the protection of information systems.

Keywords: protection of information, methods of valuation, security model, unauthorized access.

References.

1. Gostehkomissiya RF. Rukovodyatshii dokument. Sredstva vy4islitelnoi tehniki. Zatshita ot nesankcionirovannogo dostupa k informacii. Pokazateli zatshitshennosti ot nesankcionirovannogo dostupa k informacii. M.: Voenizdat, 1992.

2. Gostehkomissiya RF. Rukovodyatshii dokument. Vremennoe polojenie po organizacii razrabotki, izgotovleniya i ekspluatacii programmnyh i tehni4eskih sredstv zatshity informacii ot nesankcionirovannogo dostupa v avtomatizirovannyh sistemah i sredstvah vy4islitel^noi tehniki. - M.: Voenizdat, 1992.

3. Gostehkomissiya RF. Rukovodyatshii dokument. Avtomatizirovannye sistemy. Zatshita ot nesankcionirovannogo dostupa k informacii. Klassifikaciya avtomatizirovannyh sistem i trebovaniya po zatshite informacii. - M.: Voenizdat, 1992.

4. GOST R ISO / MEK 15408-2002. Informacionnaya tehnologiya. Metody i sredstva obespe4eniya bezopasnosti. Kriterii ocenki bezopasnosti informacionnyh tehnologii. - M.: IPK Izdatelstvo standartov, 2002 40 s.

5. Lipaev V.V. Kachestvo programmnogo obespe4eniya. – M.: Finansy i statistika. – 1983 g. – 250 s.

6. Model polnogo mnojestva realizacii ugroz informacionnoi bezopasnosti v ITKS / Hvostov V.A. [i dr.] // Vestnik Voronejskogo gosudarstvennogo tehnicheskogo universiteta. – 2011. – T.7 №6 – S. 126 — 130.

7. Metody i sredstva povyweniya zatshitshennosti avtomatizirovannyh sistem: monografiya / E.A. Rogozin, V.A. Hvostov [i dr.]. – Voronej: Voronejskii institut MVD Rossii, 2013. – 108 s.

8. Metod postroeniya informacionnoi struktury avtomatizirovannoi sistemy pri normirovanii trebovanii k informacionnoi bezopasnosti / Makarov O.,YU., Rogozin E.A., Hvostov V.A. // Vestnik Voronejskogo gosudarstvennogo tehni4eskogo universiteta. – 2011. – T.7 №9 – S. 61 – 64.

9. Algoritm klasterizacii organizacionno-tehni4eskih sistem biologi4eskoi deyatel^nosti, dlya kotoryh predusmotrena zatshita informacii / V.P. Gulov, V.A. Hvostov // Prikladnye informacionnye aspekty mediciny: mejvuz. sb. nau4. tr. – Voronej: VGMA im. N.N. Burdenko, 2011. – T. 14 № 2 – S. 12 – 17.

10. Metodika ocenki veroyatnosti nesankcionirovannogo dostupa v avtomatizirovannye sistemy, ispolzuyutshie protokol TCP / IP / O.YU. Makarov, E.A. Rogozin, V.A. Hvostov // Informaciya i bezopasnost – 2009. – T. 12 №2 S. 285 –288.

11. Ob odnom sposobe formalizacii ponyatiya stoikosti funkcii bezopasnosti GOST ISO / MEK 15408 / O.YU. Makarov, E.A. Rogozin V.A. Hvostov // Vestnik Voronejskogo gosudarstvennogo tehni4eskogo universiteta. – 2009. – T.5 №2 – S. 94 – 98.

12. Normirovanie trebovanii k osnovnym elementam avtomatizirovannoi sistemy informacionnoi bezopasnosti / S.V. Belokurov, A.A. Zmeev, V.A. Hvostov // Problemy obespe4eniya nadejnosti i ka4estva priborov ustroistv i sistem: mejvuz. sb. nau4. tr. – Voronej: VGTU, 2012. – S. 29 – 31.

Сведения об авторах: Хвостов Виктор Анатольевич – к.т.н., доцент кафедры информационной безопасности Воронежского государственного университета инженерных технологий, E-mail: hvahva1@mail.ru; Гулов Владимир Павлович – д.м.н., профессор каф. общественного здоровья, здравоохранения, гигиены и эпидемиологии ИДПО ВГМУ им. Н.Н. Бурденко, v.gulov@vsmaburdenko.ru.