Оригинальная статья/Original article

УДК 004.056

DOI: http://doi.org/10.20914/2310-1202-2018-4-96-110

Нормирование требований к характеристикам программных систем защиты информации

Алексей В. Скрыпников [1] skrypnikovvsafe@mail.ru
Виктор А. Хвостов [1] hvahva1@mail.ru
Елена В. Чернышова [1]
Вадим В. Самцов [1] samcovVV@mail.ru
Максим А. Абасов [1] maxAb@mail.ru

[1] Воронежский государственный университет инженерных технологий, пр-т Революции, 19, г. Воронеж, 394036, Россия

Аннотация. Статья посвящена решению научной проблемы разработки теоретических основ и технологии обоснования количественных требований (норм) к программным системам защиты информации (ПСЗИ). Основой современной теории защиты информации является классификационный подход. При использовании классификационного подхода требования к ПСЗИ задаются как совокупность функциональных требований необходимых к реализации для определенного класса защищенности. При этом, понятие «эффективность защиты информации» не рассматривается. Противоречие между качественным классификационным подходом при формировании требований к ПСЗИ и необходимостью использовать их количественные характеристики при разработке автоматизированных систем (АС) в защищенном исполнении потребовали разработки нового нормативного подхода обоснования требований к защите информации. Нормативный подход основывается на системном рассмотрении проблемы, при котором проводится анализ взаимодействия элементов АС друг с другом и оценивается влияние ПСЗИ на АС в целом, а также проводится анализ поставленной цели безопасности информации (БИ). На основе анализа топологии АС, внутренних и внешних связей и потоков информации конструируется информационная структура системы. При этом, нормативный метод рассматривает полное множество угроз БИ. Угрозы БИ носят стохастический характер, являются многоэтапными и многовариантными. В свою очередь, ПСЗИ при реализации функций защиты нейтрализует угрозы БИ с некоторой вероятностью (существуют остаточные риски) и протяженностью во времени. Наличие множества угроз БИ, характеризуемых различным временем реализации, вероятностными характеристиками преодоления ПСЗИ и деструктивными возможностями, требуют нахождения норм БИ оптимизационными методами и с учетом требований минимизации влияния на эффективность автоматизированной системы.

Ключевые слова: защита информации, автоматизированная система, система защиты информации, несанкционированный доступ, информационная безопасность, ФСТЭК России.

Rationing requirements to the characteristics of software tools to protect information

Alexey V. Skrypnikov [1] skrypnikovvsafe@mail.ru
Victor A. Khvostov [1] hvahva1@mail.ru
Elena V. Chernyshova [1]
Vadim V. Samtsov [1] samcovVV@mail.ru
Maxim A. Abasov [1] maxAb@mail.ru

[1] Voronezh state university of engineering technologies, Revolution Av., 19 Voronezh, 394036, Russia

Abstract. The article is devoted to the solution of the scientific problem of the development of theoretical foundations and technology of substantiation of quantitative requirements (rules) for software information security (PSI). The basis of the modern theory of information security is a classification approach. When using the classification approach, the requirements for PSSS are defined as a set of functional requirements necessary for implementation for a certain class of security. At the same time, the concept of "effectiveness of information protection" is not considered. The contradiction between the qualitative classification approach in the formation of requirements for PSI and the need to use their quantitative characteristics in the development of automated systems (as) in protected execution required the development of a new normative approach to substantiate the requirements for information protection. Normative approach based on the systematic consideration of problems in which the analysis of interaction of elements as each other and the influence of PSSI on the AU in General and the analysis of the goals of security of information (BI). The information structure of the system is constructed on the basis of the analysis of the AU topology, internal and external relations and information flows. At the same time, the normative method considers the full set of BI threats. BI threats are stochastic, multi-stage and multi-variant. In turn, the NSCI in implementing protection functions neutralizes BI threats with some probability (there are residual risks) and length in time. The presence of a variety of BI threats, characterized by different time of implementation, probabilistic characteristics of overcoming PSI and destructive capabilities, require the finding of BI norms by optimization methods, based on the requirements of minimizing the impact on the efficiency of the automated system.

Keywords: information security; automated system; information security system; system effectiveness; unauthorized access; information security; FSTEC.

Для цитирования

Скрыпников А.В., Хвостов В.А., Чернышова Е.В., Самцов В.В., Абасов М.А. Нормирование требований к характеристикам программных систем защиты информации // Вестник ВГУИТ. 2018. Т. 80. № 4. С. 96–110. doi:10.20914/2310-1202-2018-4-96-110

For citation

Skrypnikov A.V., Khvostov V.A., Chernyshova E.V., Samtsov V.V., Abasov M.A. Rationing requirements to the characteristics of software tools to protect information. *Vestnik VGUIT* [Proceedings of VSUET]. 2018. vol. 80. no. 4. pp. 96–110. (in Russian). doi:10.20914/2310-1202-2018-4-96-110

Введение

Современное состояние теории защиты информации можно характеризовать как противоречивое. Развитие методов и реализуемых способов защиты информации в последнее десятилетие можно характеризовать как бурное. При этом множественность аппаратных и программных платформ АС, подлежащих защите, потребовали стандартизации и унификации разнообразных методов и способов защиты информации. Стандарты и другие нормативно-распорядительные документы в рассматриваемой области в настоящее время играют роль методических документов, концентрирующих обширные знания экспертов и обобщающих существующие методы и средства обеспечения информационной безопасности. В России основой для решения задач защиты информации являются руководящие документы Федеральной службы технического и экспортного контроля (ФСТЭК) [1–3]. Задание требований в соответствии с [1–3] заключается в сопоставлении его с одним из заданных классов защищенности. Подобный подход применен в международном стандарте «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). Место класса в ОК занял профиль защиты (ПЗ) [4].

Анализ документов [1–4] показывает, что современные методы формирования требований к безопасности информации базируются на классификационном подходе. Рассматриваемый подход ориентирован на обеспечение полноты и непротиворечивости защиты информации и не рассматривает категорию **эффективность**.

Таким образом, налицо оказывается проблема, состоящая в том, что учет уровня БИ при проектировании АС не находит прямого отражения в практике при обосновании требований к ПСЗИ в методах обоснования требований, используемых в настоящее время.

Теоретический анализ

В статье проанализированы существующие методы обоснования требований к ПСЗИ и разработан нормативный метод, основанный на анализе понятия «эффективность защиты информации» и взаимосвязи системы защиты и защищаемой АС.

Причина отсутствия учета характеристик эффективности защиты информации при проектировании АС в практике в методах, используемых в настоящее время, лежит в принципиальных теоретических трудностях применения существующих методов обоснования требований к ПСЗИ, особенно из-за отсутствия механизмов полного и достоверного подтверждения качества обеспечения защиты и нормативно-методического обеспечения в области 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 ПСЗИ, во-первых, как методологической основы современной системотехники, а во-вторых, исходя из требований самого процесса проектирования и построения АС, и обоснованием требований, базирующихся на качественном формировании перечня требуемых к реализации функций безопасности, обеспечивающих только полноту, достаточность и непротиворечивость защиты информации и никак не связанных с категорией **эффективность**.

Разрешение рассмотренной проблемы в рамках традиционного классификационного метода невозможно. В качестве решения авторам видится необходимость разработки теоретических основ и технологии обоснования количественных требований (норм) к ПСЗИ на основе оценки эффективности защиты информации, обеспечивающих максимальный уровень защищенности при минимальном влиянии системы защиты на эффективность АС. При этом необходимо рассмотреть вопросы эффективности в условиях реализации полного множества угроз безопасности информации.

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

Модели и методы нормативного метода обоснования требований к ПСЗИ

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

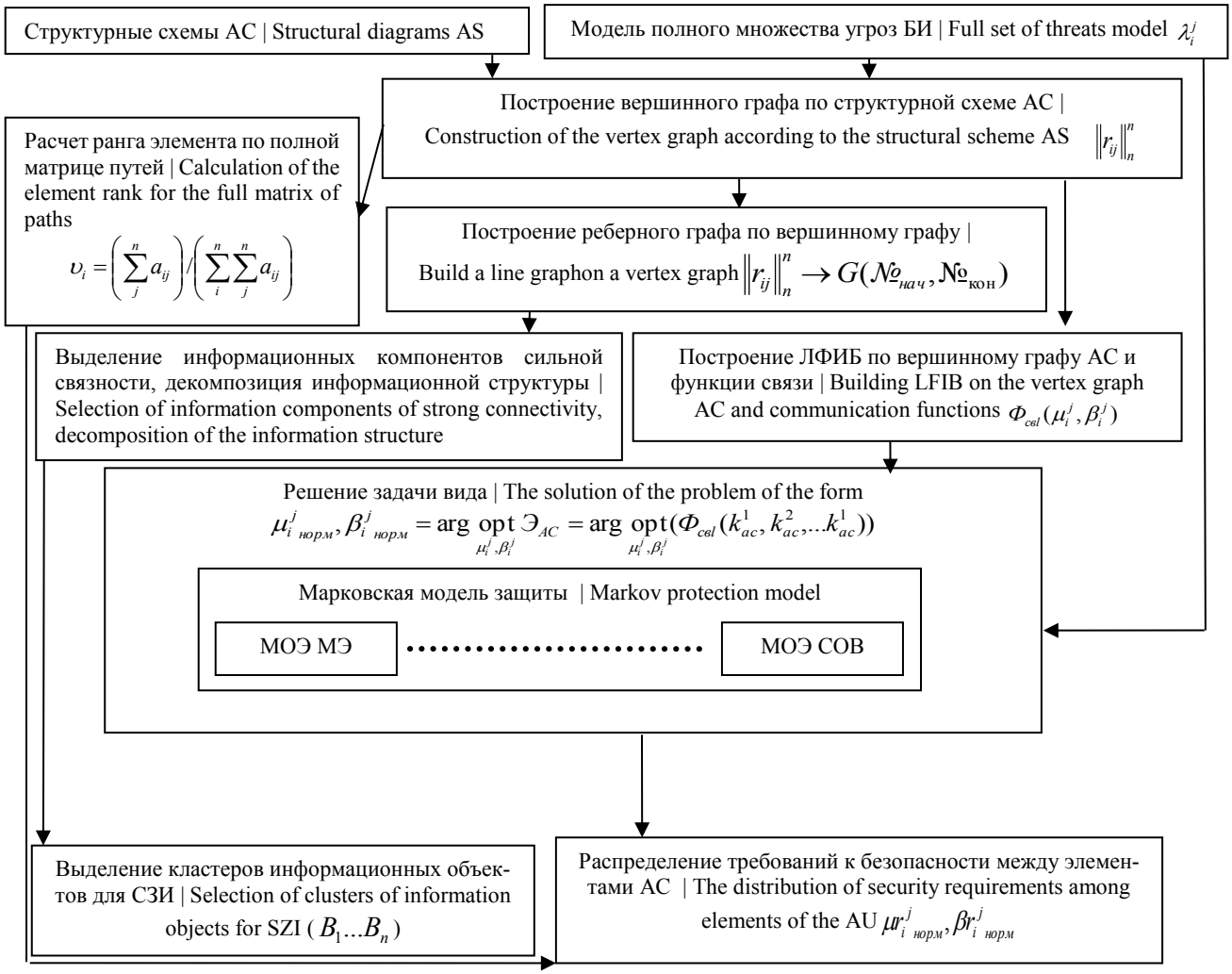


Рисунок 1. Технология обоснования требований к безопасности информации АС

Figure 1. Technology of justification of information security requirements

Решение задачи нормирования требований к БИ АС предлагается искать классическими методами теории принятия решений [5].

Примем постулат, что эффективность АС характеризуется вектором частных показателей $Q = \{Q_1, Q_2 \ldots Q_k\}$. Совокупность A альтернативных вариантов СЗИ $A = \{A_1, A_2 . A_n\}$ характеризуется множеством остаточных рисков по каждой возможной угрозе БИ, которые можно выбрать при построении АС. На выбор того или иного решения оказывают влияние объективные условия, представляемые в задачах принятия решения в виде множества возможных состояний природы $W = \{w_1, w_2 \ldots w_m, \}$, одно из которых w_i будет иметь место в действительности при реализации выбранного альтернативного варианта СЗИ, имеющего смысл варианта совокупности угроз БИ.

Для АС, эффективность которой характеризуется вектором частных показателей $\boldsymbol{Q}$, имеется совокупность $\boldsymbol{A}$ альтернативных вариантов ПСЗИ. На выбор того или иного решения оказывают влияние объективные условия, представляемые в задачах принятия решения в виде множества состояний природы $\boldsymbol{W}$, одно из которых будет иметь место в действительности при реализации выбранного альтернативного варианта. Вариант $\boldsymbol{W}$ в задаче выбора имеет смысл возможного варианта совокупности угроз БИ.

Другой фактор, влияющий на выбор альтернативы варианта ПСЗИ $\boldsymbol{A}$, – последствие принимаемого решения, являющегося числовой характеристикой эффективности автоматизированной системы, получаемой в условиях реализации угроз безопасности информации.

Другими словами, последствие есть функция, определенная на множестве альтернатив вариантов ПСЗИ (множестве вариантов остаточных рисков) и на множестве совокупности угроз БИ. Таким образом, для каждой альтернативы a_i и для каждого состояния природы w_i определим последствия в виде полезности (достижимого уровня эффективности АС, связанного, в свою очередь, с понятием эффективности ПСЗИ, т. е. $Q_{нсд}:(A*W)\overset{A\in}{\rightarrow},W\in W_{доп}R$). Значения показателей эффективности АС играют роль платежей теории игр.

Для каждого частного показателя эффективности АС можно составить матрицы платежей задачи принятия решения с m возможными вариантами построения СЗИ и n состояниями природы (совокупностями реализаций угроз БИ) с соответствующими оптимальными в смысле критерия ζ решениями $\hat{a}_k^{\zeta}$ следующего вида [5]:

$$\begin{matrix} Q_{1\text{нсд}}(a_1,w_1) & \dots & Q_{1\text{нсд}}(a_1,w_n) \\ \vdots & \ddots & \vdots \\ Q_{1\text{нсд}}(a_m,w_1) & \dots & Q_{1\text{нсд}}(a_m,w_n) \end{matrix} \overset{}{\underset{R}{\rightarrow}} \hat{a}_1^{\zeta}$$

$$\begin{matrix} Q_{2\text{нсд}}(a_1,w_1) & \dots & Q_{2\text{нсд}}(a_1,w_n) \\ \vdots & \ddots & \vdots \\ Q_{2\text{нсд}}(a_m,w_1) & \dots & Q_{2\text{нсд}}(a_m,w_n) \end{matrix} \overset{}{\underset{R}{\rightarrow}} \hat{a}_2^{\zeta}$$

$$\vdots$$

$$\begin{matrix} Q_{k\text{нсд}}(a_1,w_1) & \dots & Q_{k\text{нсд}}(a_1,w_n) \\ \vdots & \ddots & \vdots \\ Q_{k\text{нсд}}(a_m,w_1) & \dots & Q_{k\text{нсд}}(a_m,w_n) \end{matrix} \overset{}{\underset{R}{\rightarrow}} \hat{a}_k^{\zeta}$$

Выбор критериев ζ для решения задачи оптимизации для каждого показателя эффективности АС осуществляется в условиях неопределенности принятия решения (игра с природой) из-за необходимости получения норм безопасности применительно ко всем возможным условиям эксплуатации АС. То есть исходя из принципа максимизации энтропии, заключающегося в том, что в ситуациях, когда распределение вероятностей или значения вероятностей неизвестны, их задают, исходя из следующего утверждения: система находится в равновесии, когда энтропия максимальна, что соответствует полному беспорядку. То есть все возможные состояния природы равновероятны. Принцип максимизации энтропии также соответствует равновесному и наиболее вероятному состоянию системы.

При принятии решения в условиях неопределенности вероятностное распределение, соответствующее состояниям w_i, либо неизвестно, либо не может быть определено. Этот недостаток информации обусловил одновременное использование следующих критериев:

- критерия Лапласа;
- минимаксного критерия (критерий Вальда);
- критерия Сэвиджа.

Выбранные критерии отличаются по степени консерватизма в отношении неопределенности исходных данных [6–8].

Критерий Лапласа опирается на принцип недостаточного основания, сформулированный Я. Бернулли, который гласит, что, поскольку распределение вероятностей состояний неизвестно, нет причин считать их различными. Следовательно, используется оптимистическое предположение, что вероятности всех состояний природы равны между собой. Максиминный (минимаксный) критерий основан на консервативном (осторожном) отношении к неопределенности и сводится к выбору наилучшей альтернативы из наихудших альтернатив. Критерий Сэвиджа стремится смягчить консерватизм минимаксного (максиминного) критерия путем замены матрицы платежей матрицей потерь. Значение нормированных значений характеристик СЗИ из полученной совокупности оптимальных в смысле критериев ζ значений характеристик СЗИ $\hat{a}_1^{\zeta},\hat{a}_2^{\zeta}\dots\hat{a}_k^{\zeta}$, полученных для частных показателей эффективности АС $Q_{1нсд}Q_{2нсд}\dots Q_{кнсд}$, может быть получено исходя из анализа комплексного показателя эффективности АС.

При проведении синтеза множества W требуется проведение анализа множества угроз безопасности информации. При этом необходим подробный анализ наиболее полной совокупности угроз. При синтезе множества W [9] в качестве основополагающей конструкции формальной модели выступает иерархическое дерево $G=(L,E)$, где $L=\{l_i\}$ – множество вершин логического дерева реализации угрозы, $E=\{E_s\},E\in L$ – множество дуг дерева. Каждая вершина дерева G ассоциируется с каждым действием по реализации угрозы. Корень дерева обозначает конечную цель информационной атаки. Каждый вариант реализации угрозы БИ можно представить множеством возможных путей $G_p=\{g_p\}$, где каждый путь g_p представляет

собой последовательность дуг $(e_1, e_2, \ldots e_n)$, вида $e_i = (l_i, l_j), l_i \in L, l_j \in L$. При этом конечная вершина дуги l_i одновременно является начальной вершиной дуги l_{i+1}. В качестве начальной вершины пути могут выступать листья дерева G. В качестве конечной вершины – корень дерева G. Если каждой дуге дерева сопоставить параметр, имеющий смысл времени реализации действий по реализации этапа угрозы, тогда формальная модель угрозы БИ будет иметь следующий вид:

$$G = \left(L, E, \overline{T_G}\right),$$

$$L = \{l_1, l_2, \ldots l_n\},$$

$$E = ((l_0, l_1 t_{01}, l_0, l_2 t_{02}, \ldots l_i, l_j t_{ij},$$

где t_{ij} – время реализации, соответствующее дуге дерева атаки ij; T_G – среднее время реализации всего логического дерева реализации атаки.

Среднее время реализации связано со временем реализации действий по реализации этапа угрозы БИ, соотнесенного с дугой ij в соответствии со следующим математическим соотношением:

$$\overline{T_G} = \frac{1}{P} \sum_{ij \in G_P} t_{ij}$$

где P – количество путей логического дерева реализации угрозы БИ.

Построенные с использованием предложенного подхода логические деревья основных видов реализаций угроз БИ, содержащихся в [10, 11], а также расчеты с оценкой их среднего времени реализации, разработаны в [12, 13].

При проведении оценок параметров времени реализации угроз БИ в качестве исходных данных возможно использовать данные, содержащиеся в базах знаний, накапливающих информацию о реализациях угроз. Такие базы знаний ведутся ФСТЭК России и зарубежными организациями, регулирующими вопросы защиты информации (NIST, MITRE, DARPA).

Второй совокупностью исходных данных задачи нормирования требований к ПСЗИ является реакция АС на реализованные угрозы БИ (модель защиты). При разработке модели защиты использовалась заданная в явном виде в Общих критериях [4] и неявном виде в руководящих документах ФСТЭК [1, 3] модель с полным перекрытием (периметровая модель).

В основу модели защиты информации положено агрегированное представление АС. Основные элементы периметровой модели и двудольный граф реализации множества угроз БИ представлены на рисунках 2, 3.

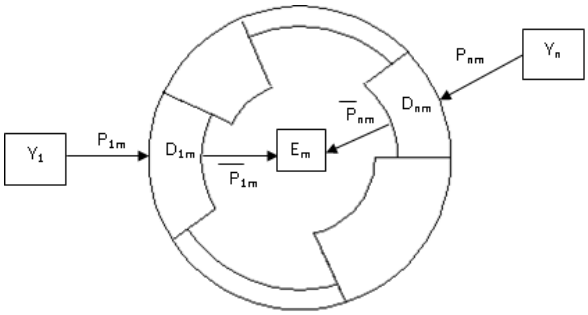


Рисунок 2. Основные компоненты периметровой модели безопасности информации

Figure 2. The main components of the perimeter security information partition

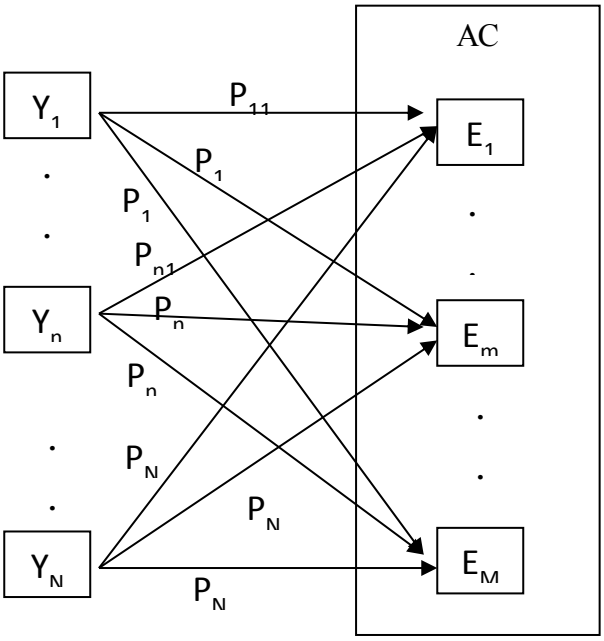
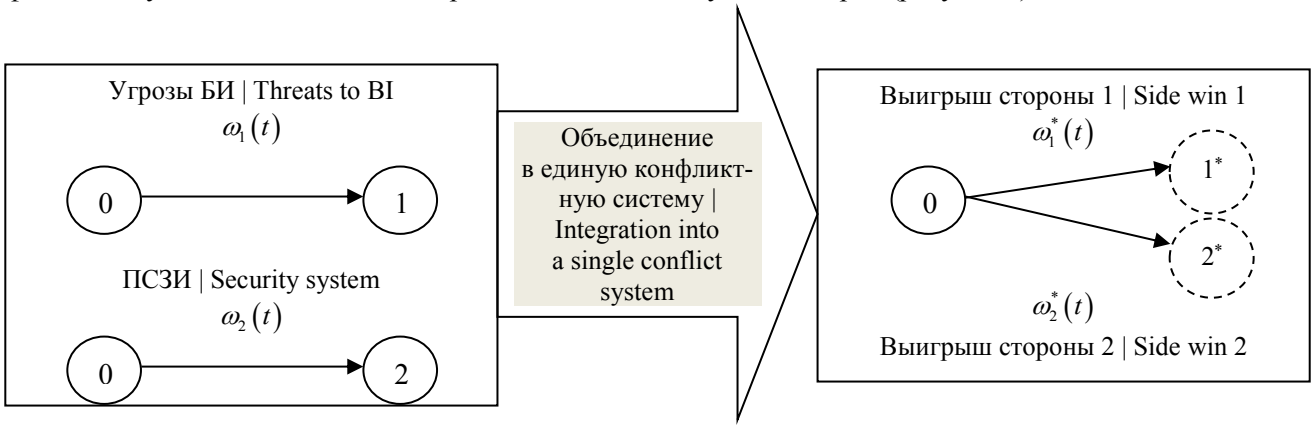


Рисунок 3. Двудольный граф реализации множества угроз БИ

Figure 3. Bipartite graph of the implementation of a variety of safety of information threats

Подробный содержательный анализ компонентов безопасности, представленных на рисунках 2, 3, проведен в [14]. Формальное описание двудольного графа, представленного на рисунке 3, можно реализовать на основе теории динамического конфликта [15]. Теория динамического конфликта в сочетании с теорией случайных процессов позволяет разрабатывать математические модели динамики функционирования сложных иерархических систем, отвечающих требованиям по адекватности и точности получаемых результатов. Основная идея построения вероятностной модели

динамического конфликта заключается в переходе от независимого описания функционирования противоборствующих сторон безусловными вероятностно-временными характеристиками (ВВХ) к описанию их взаимодействия конфликтно-обусловленными ВВХ, отражающими выигрыш одной из сторон в случае опережающего выполнения ею своей задачи. В качестве ВВХ динамического конфликта используются конфликтно-обусловленные плотности распределения вероятности (ПРВ) выигрыша конфликтующих сторон (рисунок 4).



S_1^0 – АС функционирует в режиме информационной безопасности;

S_2^0 – этап анализа сетевого трафика завершен, начало этапа – активное сканирование СВТ и их IP портов;

0 – начальное состояние процессов независимого функционирования ПСЗИ и реализации угрозы БИ;

1,2 – конечное состояние процессов независимого функционирования ПСЗИ и реализации угрозы БИ (сторона 1 (2) выполнили свою задачу);

1^*, 2^* – конечное состояние динамического конфликта, соответствующее выигрышу стороны 1, 2 (угроза БИ реализована раньше, чем ПСЗИ выполнила защитные функции, ПСЗИ выполнила защитные функции раньше, чем реализована угроза БИ);

$\omega_1(t)$, $\omega_2(t)$ – безусловные плотности распределения вероятности (ПРВ) времени реализации угрозы БИ выполнения защитных функций ПСЗИ;

$\omega_1^*(t)$ – конфликтно-обусловленная ПРВ времени реализации угрозы БИ;

$\omega_2^*(t)$ – конфликтно-обусловленная ПРВ времени выполнения защитных функций ПСЗИ

Рисунок 4. Вероятностная модель динамического конфликта ПСЗИ – угроза БИ:

Figure 4. Probabilistic model of dynamic conflict protection system – security threat:

Аналитическое решение исходной системы интегро-дифференциальных уравнений, представленных на рисунке 4, для произвольного распределения вероятностей является достаточно сложной задачей, поэтому целесообразно упрощенное рассмотрение динамической модели конфликта в марковском приближении [16, 17].

Марковская модель защиты информации в АС, разработанная на основе [9, 12, 13, 16, 17], представлена на рисунке 5.

На рисунке 5 отражены последовательные этапы реализации НСД.

Этап 1 – анализ сетевого трафика при ведении пассивной предварительной фазы НСД.

Этап 2 – активное сканирование СВТ и их IP портов.

Этап 3 – внедрение средств программно-технического воздействия на СВТ (внедрение «эксплойтов» и «руткитов»).

S_3^0 – этап активного сканирования завершен, начало этапа внедрения средств программно-технического воздействия на СВТ (внедрение эксплойтов и руткитов).

S_4^0 – достигнута цель НСД, в СВТ внедрены средства программно-технического воздействия.

S_1^1 – реализован первый способ анализа сетевого трафика, средства ЗИ от НСД не обнаружили первый способ анализа сетевого трафика.

S_1^{n+1} – средства ЗИ от НСД обнаружили первый способ анализа сетевого трафика, осуществляется его нейтрализация.

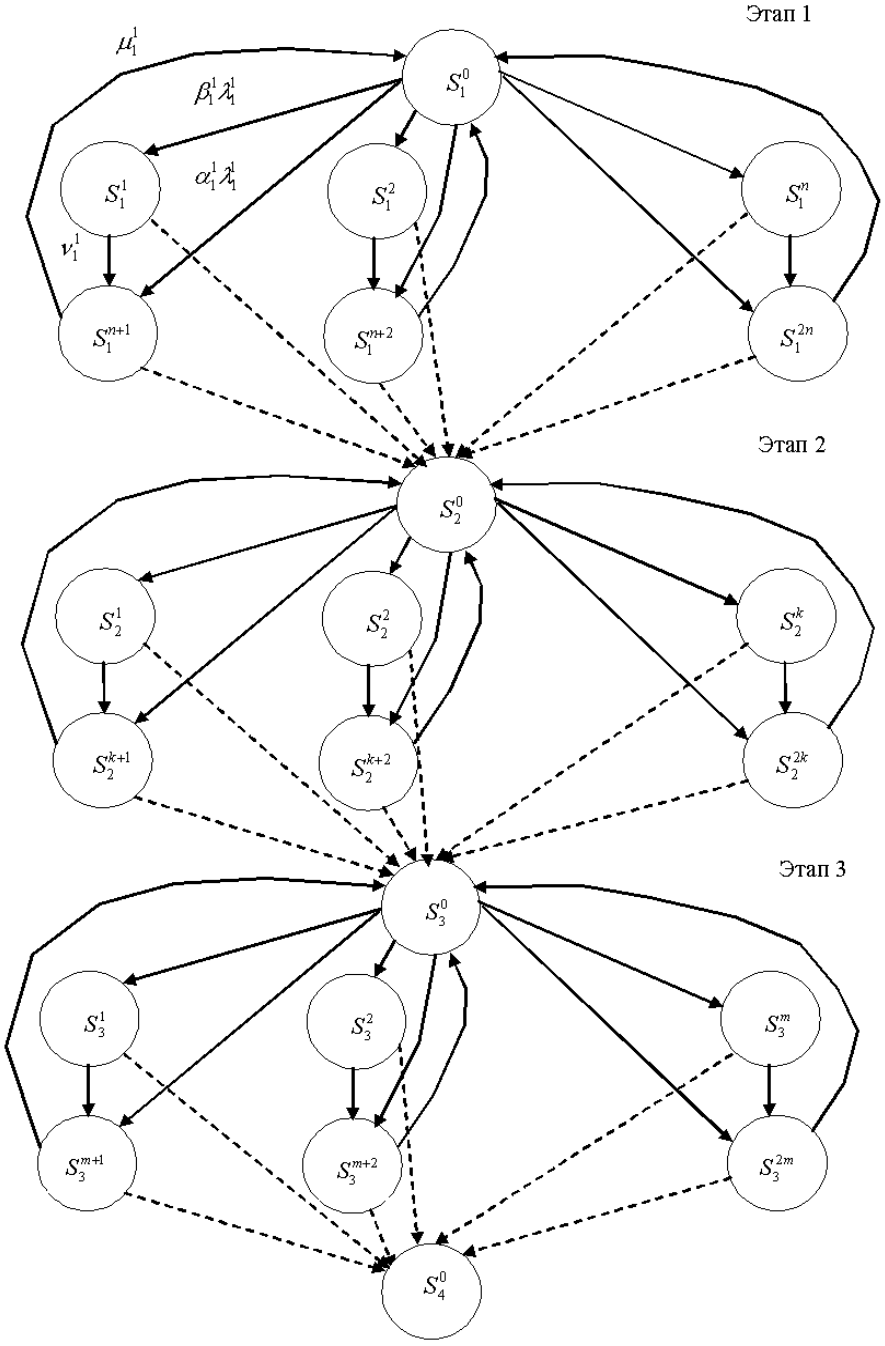


Рисунок 5. Марковская модель защиты информации в АС
Figure 5. Markov model of information safety

Состояния S_1^2, S_1^{n+2}, S_1^n, S_1^{2n} аналогичны состояниям S_1^1, S_1^{n+1} применительно ко второму способу (*n* способу анализа сетевого трафика).

Состояния S_2^1, S_2^{k+1}, S_2^2, S_2^{k+2}, S_2^k, S_2^{2k}, S_3^1, S_3^{m+1} S_3^2, S_3^{m+2}, S_3^m, S_3^{2m} аналогичны состояниям S_1^1, S_1^{n+1} применительно к 2-му и 3-му этапам НСД и k способам активного сканирования, m способам внедрения средств программно-технического воздействия на СВТ.

Переходы $S_i^{j\neq 0}$ в состояния S_i^0 являются безвременными и отражают процесс перехода к следующему этапу НСД по достижению предыдущего.

При допущении экспоненциального распределения времени перехода процесса из состояния в состояние решена система алгебраических уравнений относительно стационарных вероятностей состояний.

Результирующее математическое выражение, являющееся основой для методики комплексной оценки эффективности СЗИ,

для стационарной вероятности выполнения всех трех последовательных этапов НСД при использовании всех ν_i^j, λ_i^j возможных типовых сценариев для первого, второго и третьего этапов при всех возможных способах противодействия, характеризуемых величинами μ_i^j, β_i^j, можно записать в следующем виде:

$$P_{нсд} = P_4^0 = \prod_{i=1}^{3}(1-1/(1+\sum_{j=1}^{n,k,m}\frac{\lambda_i^j}{\mu_i^j}(1+\beta_i^j\frac{\mu_i^j}{\nu_i^j}))).$$

Параметры β_i^j, μ_i^j являются характеристиками ПСЗИ. Для определения требований к особенностям технической реализации, а также к настройке и функционированию разработаны частные методики оценки эффективности МЭ и СОВ [17–19], других средств защиты информации.

Одним из наиболее важных вопросов при применении предлагаемого нормативного метода обоснования требований к ПСЗИ является оценка влияния процессов защиты на основные процессы, протекающие в АС. Для проведения этой оценки разработана методика формализации структуры АС [20].

Структурная схема АС определяет основные функциональные части системы, их назначение и взаимосвязи. Выделяемые в системе функциональные части называются блоками. Под блоком обычно понимают устройство, функционально законченное и оформленное в виде отдельного целого.

Основными принципами выделения блоков при составлении информационно-логических схем являются возможность функционального описания АС блока и однонаправленность его действия.

Методика описания АС структурной схемы состоит в следующем [20].

1. Система разбивается на блоки, которые изображаются в виде условных символов с обозначением роли элемента в системе.

2. Информационные связи, учет которых необходим при исследовании системы, изображаются в виде линий между элементами, для которых эти связи существуют.

3. Отношения между блоками определяются обозначением направленности процессов в системе с помощью стрелок на линиях связи.

Построенная структурная схема АС формализуется следующим образом. Элементам структурной схемы АС ставят в соответствие вершины графа $X = \{x_1, x_2, ...x_n\}$. Связям между элементами ставятся в соответствие дуги графа $U = \{u_1, u_2, ...u_m\}$. В результате получается вершинный граф, отражающий структуру 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 $\Phi_{свI}(\mu_i^j, \beta_i^j)$.

Для построения информационной структуры АС используется ее реберный граф [20]. Реберные графы дают возможность сопоставить информационные свойства элементов дугам графа, а логические условия их осуществления – вершинам. Это позволяет разработать полностью формализованные методы исследования структур, описания которых могут включать любые логические функции. Основанием преобразования вершинного графа системы в реберный граф служит теорема об условиях эквивалентности матриц смежности вершинного и реберного графов.

Методика, обеспечивающая выполнение условий эквивалентности при преобразовании вершинного ориентированного графа без кратных дуг в реберный граф, включает в себя три этапа:

1) построение квазиканонической матрицы смежности реберного графа;

2) нумерация вершин реберного графа;

3) построение диаграммы реберного графа.

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. При этом чем большим числом путей он связан с другими элементами, тем большее число элементов прекратит правильно функционировать при нарушении БИ рассматриваемого элемента, тем больше важность данного элемента в структуре АС. Исходя из этого при нормировании требований к элементам системы большая часть заданного общего уровня безопасности АС должна быть направлена на этот элемент. Существует несколько способов построения полной матрицы путей. Наиболее простым в реализации из них является способ, основанный на использовании алгебры квазиминоров и применимый к ориентированным графам без петель и кратных дуг.

Сущность рассматриваемого способа состоит в том, что на основе матрицы смежности вершин графа $\left\| r_{ij} \right\|_n^n$ строится матрица непосредственных путей, а по ней с помощью алгебры квазиминоров находится полная матрица путей. Ранг элемента рассчитывается с использованием полной матрицы путей:

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

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 $\Phi_{свл}(\mu_i^j, \beta_i^j)$ осуществляется логико-вероятностным методом [21]. Основная идея логико-вероятностного метода состоит в использовании математического аппарата булевой алгебры на начальной стадии анализа конструирования функции связи структурно-сложной системы. По аналогии с расчетом надежности сложной системы логико-вероятностным методом конструирование функции связи можно провести в три этапа.

Этап 1. Каждому элементу системы сопоставляется логическая переменная γ_i, принимающая два значения: 1, если элемент в состоянии безопасности, и 0, если элемент в состоянии нарушения безопасности. Затем из условий работоспособности в условиях реализации угроз к элементам АС составляется логическая функция информационной безопасности (ЛФИБ) вида $\Phi(\mathrm{Y})$, где $\mathrm{Y} = (\gamma_1, \gamma_2 \ldots \gamma_m)$ – вектор-строка логических переменных, многомерный аргумент функции. Функция $\Phi(\mathrm{Y}) = 1$, если есть хотя бы один безопасный путь от входного полюса к выходному. Путь безопасен, если безопасны все входящие в него элементы. Каждому пути в ЛФИБ соответствует элементарная конъюнкция булевых переменных, соответствующих входящим в путь элементам. ЛФИБ есть дизъюнкции всех элементарных конъюнкций, соответствующих возможным путям между входным и выходным полюсами. Полученная таким образом форма ЛФИБ является исходной.

Этап 2. Исходная форма преобразуется к одной из стандартных форм перехода к полному замещению логических переменных вероятностями, а логических операций – арифметическими.

Этап 3. В стандартной форме логической функции проводится замещение логической переменной γ_i вероятностью $p_i = P(\gamma_i = 1)$, отрицания логической переменной $\overline{\gamma_i}$ вероятностью $q_i = 1 - p_i = P(\gamma_i = 0)$, дизъюнкции $\vee$ сложением +, конъюнкции $\wedge$ умножением $\times$, логического отрицания $\neg y$ вычитанием из единицы $1 - P(\gamma = 1)$.

Подробное описание метода построения функции связи показателей информационной безопасности элементов структуры с показателями эффективности АС по прямому назначению и пример конструирования функции связи типовой АС представлены в [21].

Информационная структура АС является основой для проведения анализа в интересах выделения сильно связанных элементов – декомпозиции информационной структуры системы. При этом в информационной структуре можно выделить все составные части (подсистемы), элементы которых благодаря обратным связям взаимно достижимы. Выделение сильносвязанных 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 кластеров информационных объектов, характеризуемых сильной связностью $\{B_1 \ldots B_n\}$, используемых при обосновании комплекта средств защиты.

Исходные данные для проведения нормировании требований к ПСЗИ

При формировании множества вариантов состояний природы при построении в качестве исходных данных целесообразно использовать, как указывалось ранее, данные о статистических характеристиках, содержащихся в база данных компьютерных атак, ведущихся в России и различных международных организациях [22–26]. Композиция всех возможных вариантов сочетаний реализаций угроз этапов 1, 2, 3 показана на рисунке 6.

Статистические характеристики отдельных шагов по реализации угроз безопасности информации, составленные по результатам анализа баз знаний угроз безопасности информации [22], представлены в таблице 1.

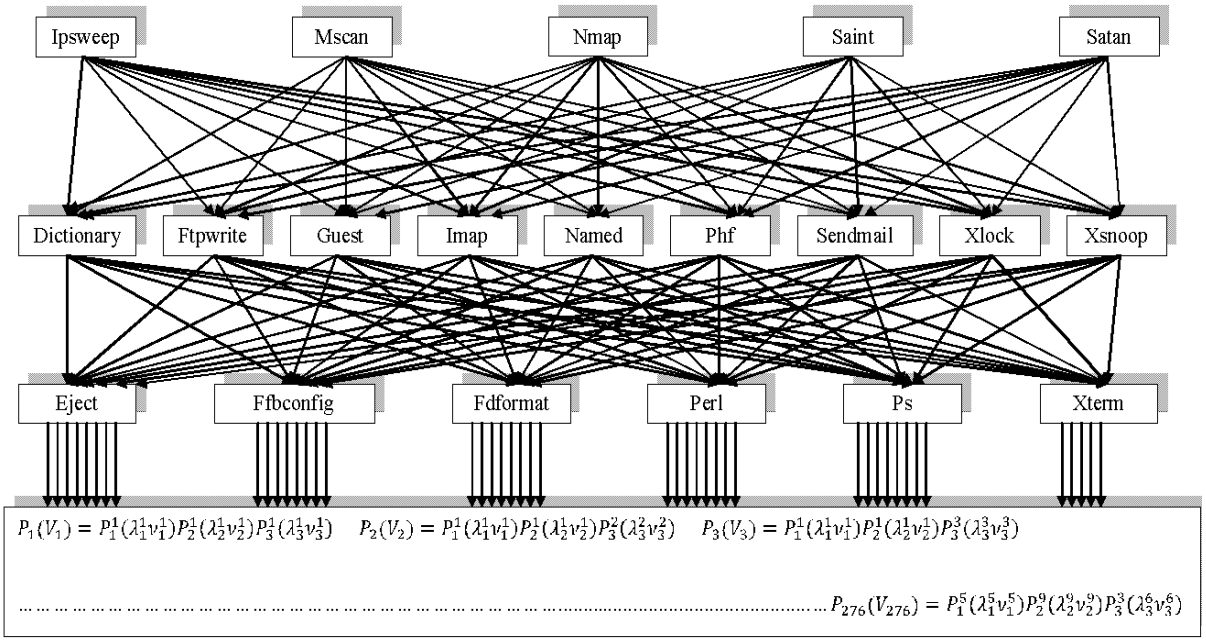


Рисунок 6. Исходные данные задачи нормирования требований к ПСЗИ

Figure 6. The initial data of the problem of standardization of information security requirements

Таблица 1.

Статистические характеристики угроз БИ по данным [22]

Table 1.

Statistical characteristics of threats to the safety of information on data [22]

Наименование атаки Name of attack	Вид параметров модели защиты Type of parameters protection models	Параметр времени реализации Parameter of time implementation v_i^j	Интенсивность реализации Intensity implementation λ_i^j
1	2	3	4
Сбор информации о топологии и принципах функционирования информационной системы (Probes)			
Ipsweep	$v_1^1 \lambda_1^1$	0.01	4,59 e-6
Mscan	$v_1^2 \lambda_1^2$	0.01	1,83 e-7
Nmap	$v_1^3 \lambda_1^3$	0.01	3,30 e-6
Saint	$v_1^4 \lambda_1^4$	0.01	3,67 e-7
Satan	$v_1^5 \lambda_1^5$	0.01	3,30 e-6
Непосредственное проникновение в информационную систему (RemotetoLocalUserAttacks)			
Dictionary	$v_2^1 \lambda_2^1$	0.001	9,18 e-7
Ftpwrite	$v_2^2 \lambda_2^2$	0.01	5,51 e-7
Guest	$v_2^3 \lambda_2^3$	0.01	7,34 e-7
Imap	$v_2^4 \lambda_2^4$	0.01	5,51 e-7
Named	$v_2^5 \lambda_2^5$	0.01	1,28 e-6
Phf	$v_2^6 \lambda_2^6$	0.01	5,51 e-7
Sendmail	$v_2^7 \lambda_2^7$	0.0001	3,67 e-7
Xlock	$v_2^8 \lambda_2^8$	0.001	3,67 e-7
Xsnoop	$v_2^9 \lambda_2^9$	0.01	3,67 e-7

Продолжение табл. 1 | Continuation of table 1

1	2	3	4
Установление контроля над информационной системой (UsertoRootAttacks)			
Eject	$\nu_3^1 \lambda_3^1$	0.001	8,45 e-6
Ffbconfig	$\nu_3^2 \lambda_3^2$	0.001	4,77 e-6
Fdformat	$\nu_3^3 \lambda_3^3$	0.001	3,49 e-6
Perl	$\nu_3^4 \lambda_3^4$	0.01	2,93 e-6
Ps	$\nu_3^5 \lambda_3^5$	0.01	7,34 e-7
Xterm	$\nu_3^6 \lambda_3^6$	0.01	5,51 e-7

Совокупность альтернативных вариантов ПСЗИ можно сформировать в виде:

$$A_1\left(\mu_1^1,\beta_1^1,\mu_1^2,\beta_1^2\ldots\mu_3^9,\beta_3^9\right);$$
$$A_2\left(\mu_1^1,\beta_1^1,\mu_1^2,\beta_1^2\ldots\mu_3^9,\beta_3^9\right);$$
$$A_{20}\left(\mu_1^1,\beta_1^1,\mu_1^2,\beta_1^2\ldots\mu_3^9,\beta_3^9\right).$$

Значения величин $\mu_1^1,\beta_1^1\ldots\mu_3^9,\beta_3^9$ перекрывают диапазон значений, соответствующий техническим характеристикам современных систем обнаружения вторжений и межсетевых экранов, и составляют:

$$\mu_j^i = 0.0003\ldots0.1;$$
$$\beta_j^i = \left\{5*10^{-5},5*10^{-6},5*10^{-7},5*10^{-8},5*10^{-9}\right\}$$

Результаты нормирования требований к ПСЗИ

В результате решения задачи нормирования требований к ПСЗИ получены значения норм (таблица 2).

Представленные в таблице 2 значения доли необнаруживаемых ПСЗИ реализаций угроз БИ j-го типа i-го этапа реализации μ_i^j и параметр экспоненциального времени нейтрализации ПСЗИ реализованной угрозы БИ β_i^j являются количественными требованиями к системе защиты. Техническая реализация ПСЗИ, а также настройка параметров функционирования (правила фильтрации межсетевых экранов, различные правила (сигнатуры) систем обнаружения вторжений, обеспечивающая достижение значений, представленных в таблице 2, обеспечивает оптимальные по критериям Лапласа, Вальда и Сэвиджа значения эффективности СЗИ при предложенной к рассмотрению в статье содержательной и статистической модели угроз ИБ. При этом значения величин μ_i^j и β_i^j можно интерпретировать как количественные значения остаточных рисков. В методах, основанных на анализе рисков Octave, RiskWatch, Cramm и др., таблица 2 может стать основой для процедуры принятия остаточных рисков. Использование критериев Лапласа, Вальда и Сэвиджа существенно расширяет возможности применения полученных норм БИ, т. к. позволяет получить нормы, отличающиеся по степени консерватизма в отношении неопределенности исходных данных в части характеристик угроз БИ в соответствии с выбранными критериями.

Таблица 2.

Результаты нормирования требований к ПСЗИ

Table 2.

End result of justification of information security requirements

Нормированный параметр ПСЗИ времени парирования угрозы БИ | Normalized parameter	Значение нормированного параметра ПСЗИ | The value of the normalized parameter	Нормированный параметр ПСЗИ вероятности парирования угрозы БИ | The normalized probability parameter of countering threat	Значение нормированного параметра ПСЗИ | The value of the normalized parameter
1	2	3	4
Нормированные требования к ПСЗИ по критерию Лапласа Normalized requirements for protection system by Laplace criterion			
μ_1^1 μ_1^2 . . μ_3^9	0.1	β_1^1 β_1^2 . . . β_3^9	$5*10^{-8}$

Продолжение табл. 2 | Continuation of table 2

1	2	3	4
Нормированные требования к ПСЗИ по критерию Вальда Normalized requirements for protection system by Wald criterion			
μ_1^1 μ_1^2 . . . μ_3^9	0.1	β_1^1 β_1^2 . . . β_3^9	$5*10^{-8}$
Нормированные требования к ПСЗИ по критерию Сэвиджа Rated protection system Requirements for Savage Criteria			
μ_1^1 μ_1^2 . . . μ_3^9	0.1	β_1^1 β_1^2 . . . β_3^9	$5*10^{-6}$

Заключение

Статья посвящена решению научной проблемы разработки теоретических основ и технологии обоснования количественных требований (норм) к ПСЗИ.

Предложенная технология обоснования количественных требований обеспечивает возможность синтеза и анализа ПСЗИ на основе использования количественных показателей эффективности решения задачи обеспечения БИ, учитывает архитектуру АС, а также особенности реализации защищаемой системы. В качестве исходных данных использовано множество реализаций угроз БИ, имеющих вероятностные и временные параметры. К достоинствам технологии можно отнести возможность учета многоэтапности и многовариантности реализации угроз БИ.

В качестве примера использования технологии обоснования количественных требований к ПСЗИ проведены расчеты и обоснованы количественные требования к ПСЗИ с использованием данных базы данных угроз безопасности информации Агентства передовых оборонных исследовательских проектов Министерства обороны США. Получены количественные требования (нормы) к характеристикам ПСЗИ (нормированный параметр ПСЗИ времени парирования угрозы БИ, нормированный параметр ПСЗИ вероятности парирования угрозы БИ) по критериям Лапласа, Вальда и Сэвиджа, позволяющие сформировать требования к ПСЗИ.

Дальнейшим направлением исследований в рамках рассмотренной научной проблемы является детализация требований к ПСЗИ с использованием анализа особенностей технической реализации межсетевых экранов, систем обнаружения вторжений и других типов ПСЗИ.

ЛИТЕРАТУРА

1 ФСТЭК РФ. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2

2 ФСТЭК РФ. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/ dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g

3 ФСТЭК РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/ dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g

4 ФСТЭК РФ. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/381-rukovodyashchij-dokument

5 Макаров О.Ю., Хвостов В.А., Хвостова Н.В. Методика нормирования требований к информационной безопасности автоматизированных систем // Вестник Воронежского государственного технического университета. 2010. Т.6. № 11. С. 47–51.

6 Балдин К.В., Воробьев С.Н., Уткин В.Б. Управленческие решения: учебник. 7-е изд. М.: Дашков и К, 2012. 496 с.

7 Волошин Г.Я. Методы оптимизации в экономике: учебное пособие. М.: Издательство «Дело и сервис», 2004 320 с.

8 Воробьев С.Н. Управленческие решения: Теория и технологии принятия: учебник для вузов. М.: Проект, 2004. 495 с.

9 Макаров О.Ю., Хвостов В.А., ХвостоваН.В. Метод построения формальных моделей реализации угроз информационной безопасности автоматизированных систем // Вестник Воронежского государственного технического университета. 2010. Т.6. № 11. С. 22–24.

10 ФСТЭК РФ. Руководящий документ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008 год URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god

11 ФСТЭК РФ. Руководящий документ. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008 год URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god

12 Зима В.М., Котухов М.М., Ломако А.Г., Марков А.С. и др. Разработка систем информационно-компьютерной безопасности. СПб.: Военно-космическая академия им. А.Ф. Можайского, 2003. 327 с.

13 Гудков С.Н., Гудкова О.И., Хвостов В.А. Модель полного множества реализаций угроз информационной безопасности в ИТКС // Вестник Воронежского государственного технического университета. 2011. Т.7. № 6. С. 126–130.

14 Мельников В. Защита информации в компьютерных системах. М.: Финансы и статистика, 1997. 368 с.

15 Дружинин В.В, Конторов Д.С. Введение в теорию конфликта. М.: Радио и связь, 1989. 288 с.

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

17 Кисляк А.А., Макаров О.Ю., Рогозин Е.А., Хвостов В.А. Методика оценки вероятности несанкционированного доступа в автоматизированные системы // Информация и безопасность. 2009. № 2. С. 285–288.

18 Климов С.М. Методы и модели противодействия компьютерным атакам. Люберцы.: КАТАЛИТ, 2008. 316 с.

19 Yang J., Zhou C., Yang Sh., Xu H. et al. Anomaly detection based on zone partition for security protection of industrial cyber-physical systems // IEEE Transactions on Industrial Electronics. 2018. V. 65. № 5. P. 4257–4267.

20 Макаров О.Ю., Рогозин Е.А., Хвостов В.А., Коробкин Д.И. и др. Метод построения информационной структуры автоматизированной системы при нормировании требований к информационной безопасности // Вестник воронежского технического университета. 2011. № 9. С. 61–64.

21 Макаров О.Ю., Рогозин Е.А., Хвостов В.А., Коробкин Д.И. и др. Функция связи показателей информационной безопасности элементов типовой многоуровневой архитектуры web сайта с его показателями эффективности // Вестник воронежского технического университета. 2011. № 9. С. 29–32.

22 Агентство передовых оборонных исследовательских проектов Министерства обороны США URL: https://www.fbo.gov/index? s=opportunity&mode=form&id=4ebb7ba441be3ed21322ac135e528a3e&tab=core&_cview=0

23 Saltzer J.H., Schroeder M.D. Theprotection of information in computer systems // Proceedings of the IEEE. 1975. V. 63. № 9.

24 Yang Z., Cheng P., Chen J. Differential-privacy preserving optimal power flow in smart grid // IET Generation, Transmission & Distribution. 2017. V. 11. № 15. P. 3853–3861.

25 Valdevies F. A Single platform approach for the management of emergency in complex environments such as large events, digital cities, and networked regions // Internet of Things and Data Analytics Handbook. 2017. P. 643–664.

26 Guizani S. Internet-of-things (IoT) feasibility applications in information Centric Networking System // 13th International Wireless Communications and Mobile Computing Conference. 2017. P. 2192–2197. doi: 10.1109/IWCMC.2017.7986623

REFERENCES

1 FSTEHK RF. Rukovodyashchij dokument. Koncepciya zashchity sredstv vychislitel'noj tekhniki i avtomatizirovannyh sistem ot nesankcionirovannogo dostupa k informacii [FSTEC RF. Guidance document. The concept of protection of computer equipment and automated systems from unauthorized access to information]. Available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2 (in Russian)

2 FSTEHK RF. Rukovodyashchij dokument. Sredstva vychislitel'noj tekhniki. Zashchita ot nesankcionirovannogo dostupa k informacii. Pokazateli zashchishchennosti ot nesankcionirovannogo dostupa k informaci [FSTEC RF. Guidance document. Computing facilities. Protection against unauthorized access to information. Indicators of security against unauthorized access to information]. Available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g (in Russian)

3 FSTEHK RF. Rukovodyashchij dokument. Avtomatizirovannye sistemy. Zashchita ot nesankcionirovannogo dostupa k informacii. Klassifikaciya avtomatizirovannyh sistem i trebovaniya po zashchite informacii [FSTEC RF. Guidance document. Automated systems. Protection against unauthorized

access to information. Classification of automated systems and information security requirements]. Available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g (in Russian)

4 FSTEHK RF. Rukovodyashchij dokument. Bezopasnost' informacionnyh tekhnologij. Kriterii ocenki bezopasnosti informacionnyh tekhnologij [FSTEC RF. Guidance document. Security information technology. Criteria for assessing the security of information technology]. Available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/381-rukovodyashchij-dokument (in Russian)

5 Makarov O.Yu., Hvostov V.A., Hvostova N.V. Methodology of rationing requirements for information security of automated systems. *Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta* [Bulletin of the Voronezh State Technical University]. 2010. vol. 6. no. 11. pp. 47–51. (in Russian)

6 Baldin K.V., Vorob'ev S.N., Utkin V.B. Upravlencheskie resheniya [Management decisions]. Moscow, Dashkov i K, 2012.496 p. (in Russian)

7 Voloshin G.Ya. Metody optimizacii v ehkonomike [Optimization methods in economics]. Moscow, Publishing "Business and Service", 2004. 320 p. (in Russian)

8 Vorob'ev S.N. Upravlencheskie resheniya: teoriya i tekhnologii prinyatiya [Management decisions: theory and technology adoption]. Moscow, Project, 2004. 495 p. (in Russian)

9 Makarov O.Yu., Hvostov V.A., Hvostova N.V. The method of constructing formal models for the implementation of threats to information security of automated systems. *Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta* [Bulletin of the Voronezh State Technical University]. 2010. vol.6. no. 11. pp. 22–24. (in Russian)

10 FSTEHK RF. Rukovodyashchij dokument. Bazovaya model' ugroz bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sis-temah personal'nyh dannyh (vypiska). FSTEHK Rossii, 2008 god [FSTEC RF. Guidance document. The basic model of threats to the security of personal data when they are processed in personal data information systems (extract). FSTEC of Russia, 2008]. Available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god (in Russian)

11 FSTEHK RF. Rukovodyashchij dokument. Metodika opredeleniya aktual'nyh ugroz bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh. FSTEHK Rossii, 2008 god [FSTEC RF. Guidance document. The method of determining the actual threats to the security of personal data during their processing in personal data information systems. FSTEC of Russia, 2008]. Available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god (in Russian)

12 Zima V.M., Kotuhov M.M., Lomako A.G., Markov A.S. et al. Razrabotka system informacionno-komp'yuternoj bezopasnosti [Development of information and computer security systems]. St. Petersburg, Military Space Academy. A.F. Mozhaisky, 2003. 327 p. (in Russian)

13 Gudkov S.N., Gudkova O.I., Hvostov V.A. Model of a complete set of implementations of information security threats in ITKS. *Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta* [Bulletin of the Voronezh State Technical University]. 2011. vol.7. no. 6. pp. 126–130. (in Russian)

14 Mel'nikov V. Zashchita informacii v komp'yuternyh sistemah [Information security in computer systems]. Moscow, Finance and Statistics, 1997. 368 p. (in Russian)

15 Druzhinin V.V, Kontorov D.S. Vvedenie v teoriyu konflikta [Introduction to the theory of conflict]. Moscow, Radio and communication, 1989. 288 p. (in Russian)

16 Kislyak A.A., Makarov O.Yu., Rogozin E.A., Hvostov V.A. About one way to formalize the concept of the durability of the security function of GOST ISO/MEK 15408. *Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta* [Bulletin of the Voronezh State Technical University]. 2009. no. 2. pp. 94–98. (in Russian)

17 Kislyak A.A., Makarov O.YU., Rogozin E.A., Hvostov V.A. Methodology for estimating the probability of unauthorized access to automated systems. *Informaciya i bezopasnost'* [Information and security]. 2009. no. 2. pp. 285–288. (in Russian)

18 Klimov S.M. Metody I modeli protivodejstviya komp'yuternym atakam [Methods and models of countering computer attacks]. Lyubercy, KATALIT, 2008. 316 p. (in Russian)

19 Yang J., Zhou C., Yang Sh., Xu H. et al. Anomaly detection based on zone partition for security protection of industrial cyber-physical systems. IEEE Transactions on Industrial Electronics. 2018. vol. 65. no. 5. pp. 4257–4267.

20 Makarov O.Yu., Rogozin E.A., Hvostov V.A., Korobkin D.I. et al. The method of constructing the information structure of an automated system when rationing the requirements for information security. *Vestnik voronezhskogo tekhnicheskogo universiteta* [Bulletin of the Voronezh Technical University]. 2011. No. 9. pp. 61–64. (in Russian)

21 Makarov O.Yu., Rogozin E.A., Hvostov V.A., Korobkin D.I. et al. The function of communication of information security indicators of elements of a typical multi-level architecture of a web site with its performance indicators. *Vestnik voronezhskogo tekhnicheskogo universiteta* [Bulletin of the Voronezh Technical University]. 2011. no. 9. pp. 29–32. (in Russian)

22 Agentstvo peredovyh oboronnyh issle-dovatel'skih proektov Ministerstva oborony SSHA [Agency of Advanced Defense Research Projects of the US Department of Defense]. Available at: https://www.fbo.gov/index? s=opportunity& mode=form&id=4ebb7ba441be3ed21322ac135e528a3e&tab= core&_cview=0 (in Russian)

23 Saltzer J.H., Schroeder M.D. Theprotection of information in computer systems. Proceedings of the IEEE. 1975. vol. 63. no. 9.

24 Yang Z., Cheng P., Chen J. Differential-privacy preserving optimal power flow in smart grid. IET Generation, Transmission & Distribution. 2017. vol. 11. no. 15. pp. 3853–3861.

25 Valdevies F. A Single platform approach for the management of emergency in complex environments such as large events, digital cities, and networked regions. Internet of Things and Data Analytics Handbook. 2017. pp. 643–664.

26 Guizani S. Internet-of-things (IoT) feasibility applications in information Centric Networking System. 13th International Wireless Communications and Mobile Computing Conference. 2017. pp. 2192–2197. doi: 10.1109/IWCMC.2017.7986623

СВЕДЕНИЯ ОБ АВТОРАХ

Алексей В. Скрыпников д.т.н., профессор, Кафедра информационной безопасности, Воронежский государственный университет инженерных технологий, пр-т Революции, 19, г. Воронеж, 394036, Россия, skrypnikovvsafe@mail.ru

Виктор А. Хвостов к.т.н., доцент, Кафедра информационной безопасности, Воронежский государственный университет инженерных технологий, пр-т Революции, 19, г. Воронеж, 394036, Россия, hvahva1@mail.ru

Елена В. Чернышова к.т.н., доцент, кафедра информационной безопасности, Воронежский государственный университет инженерных технологий, пр-т Революции, 19, г. Воронеж, 394036, Россия

Вадим В. Самцов экстерн, кафедра информационной безопасности, Воронежский государственный университет инженерных технологий, пр-т Революции, 19, г. Воронеж, 394036, Россия, samcovVV@mail.ru

Максим А. Абасов экстерн, кафедра информационной безопасности, Воронежский государственный университет инженерных технологий, пр-т Революции, 19, г. Воронеж, 394036, Россия, maxAb@mail.ru

КРИТЕРИЙ АВТОРСТВА

Авторы в равной степени принимали участие в написании рукописи и несут ответственность за плагиат

КОНФЛИКТ ИНТЕРЕСОВ

Авторы заявляют об отсутствии конфликта интересов.

ПОСТУПИЛА 08.10.2018
ПРИНЯТА В ПЕЧАТЬ 09.11.2018

INFORMATION ABOUT AUTHORS

Alexey V. Skrypnikov Dr. Sci. (Engin.), professor, Information security department, Voronezh state university of engineering technologies, Revolution Av., 19 Voronezh, 394036, Russia, skrypnikovvsafe@mail.ru

Victor A. Khvostov Cand. Sci. (Engin.), associate professor, Information security department, Voronezh state university of engineering technologies, Revolution Av., 19 Voronezh, 394036, Russia, hvahva1@mail.ru

Elena V. Chernyshova Cand. Sci. (Engin.), associate professor, Information security department, Voronezh state university of engineering technolo-gies, Revolution Av., 19 Voronezh, 394036, Russia

Vadim V. Samtsov extern, Information security department, Voronezh state university of engineering technolo-gies, Revolution Av., 19 Voronezh, 394036, Russia, samcovVV@mail.ru

Maxim A. Abasov extern, Information security department, Voronezh state university of engineering technolo-gies, Revolution Av., 19 Voronezh, 394036, Russia, maxAb@mail.ru

CONTRIBUTION

Authors are equally involved in the writing of the manuscript and are responsible for plagiarism

CONFLICT OF INTEREST

The authors declare no conflict of interest.

RECEIVED 10.8.2018
ACCEPTED 11.9.2018