Инженерный вестник Дона, №1, ч.2 (2015)
ivdon.ru/ru/magazine/archive/n1y2015/2868

Постановка и формализация задачи формирования информационной защиты распределённых систем

А.А. Кацупеев, Е.А. Щербакова, С.П. Воробьёв

[1]*Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова, Новочеркасск*

Аннотация: В данной статье рассмотрено понятие информационной безопасности, её структура и этапы развития, показано многообразие и эквивалентность используемых средств защиты, а также рассмотрены существующие подходы к формированию защиты корпоративных систем, на основании которых было предложено решение данной проблемы, базирующееся на методах теории принятия решений.
Ключевые слова: защита информации, информационная безопасность, средства защиты информации, задача о рюкзаке, точки размещения средств защиты, формирование информационной защиты, распределённые системы, математическая модель.

Под безопасностью информации в распределённой системе прежде всего понимается такое состояние всех компонент, при котором обеспечивается защита от возможных угроз на требуемом уровне.

Защита ресурсов организации достигается путём проведения руководством предприятия соответствующей политики информационной безопасности. Основным документом, на основе которого проводится данная политика, является программа информационной безопасности. Этот документ разрабатывается и принимается руководством предприятия. В программе приводятся цели политики информационной безопасности и основные направления решения задач защиты информации в системе.

Целью защиты информации является предотвращение ущерба собственнику, владельцу или пользователю системы. Главной характеристикой защиты является эффективность, под которой понимается степень соответствия результатов защиты поставленной цели. Объектом защиты может быть информация, ее носитель или информационный процесс.

Можно выделить следующие этапы развития информационной безопасности:

I этап — до 1816 года — характеризуется использованием естественно возникавших средств информационных коммуникаций. В это время суть информационной безопасности состояла в защите сведений о событиях, фактах, имуществе, местонахождении и других данных, имеющих для человека лично или сообщества, к которому он принадлежал, жизненно важное значение.

II этап — начиная с 1816 года — связан с началом использования искусственно созданных технических средств электро- и радиосвязи. Основной задачей информационной безопасности в этот период стало обеспечение скрытности и помехозащищённости радиосвязи. Это достигалось использованием новых технологий: стали применяться помехоустойчивое кодирование сигнала и последующее декодирование принятого сообщения или сигнала.

III этап — начиная с 1935 года — связан с появлением радиолокационных и гидроакустических средств, наиболее распространённых в военной сфере. Основным направлением обеспечения информационной безопасности в этот период было повышение защищённости радиолокационных средств от радиоэлектронных помех.

IV этап — начиная с 1946 года — начался вместе с изобретением и внедрением в практическую деятельность предприятий электронно-вычислительных машин (компьютеров). В этот период задачи информационной безопасности состояли в обеспечении физического ограничения к средствам переработки и передачи информации.

V этап — начиная с 1965 года — обусловлен созданием и развитием локальных информационно-коммуникационных сетей. Как и в предыдущем периоде, задачи информационной безопасности также состояли, прежде всего, в ограничении физического доступа к средствам обработки

информации, объединённым в локальные сети. Это достигалось путём администрирования и управления доступом к сетевым ресурсам.

VI этап — начиная с 1973 года — связан с использованием сверхмобильных коммуникационных устройств с широким спектром задач. Угрозы информационной безопасности в этот период стали гораздо серьёзнее по сравнению с предыдущими периодами. Именно в это время появились хакеры – люди, ставящие себе цель нанести ущерб информационной безопасности разнообразных организаций, отдельных пользователей и даже целых стран. Информационный ресурс стал одним из важнейших в любом государстве, а обеспечение его защиты – обязательной составляющей национальной безопасности. Также в этом периоде международное право было расширено с помощью новой отрасли: информационного права.

VII этап — начиная с 1985 года — связан с созданием и развитием глобальных информационно-коммуникационных сетей. Можно предположить, что следующий этап развития информационной безопасности будет связан с широким использованием сверхмобильных коммуникационных устройств с широким спектром задач и глобальным охватом в пространстве и времени, обеспечиваемым космическими информационно-коммуникационными системами. Для решения задач информационной безопасности на этом этапе необходимо создание макросистемы информационной безопасности человечества под эгидой ведущих международных форумов [1].

В систему обеспечения безопасности данных входят механизмы защиты – совокупности средств защиты, функционирующих совместно и выполняющих определённую задачу по защите данных [2].

Концептуальная схема информационной безопасности представлена на рисунке 1.

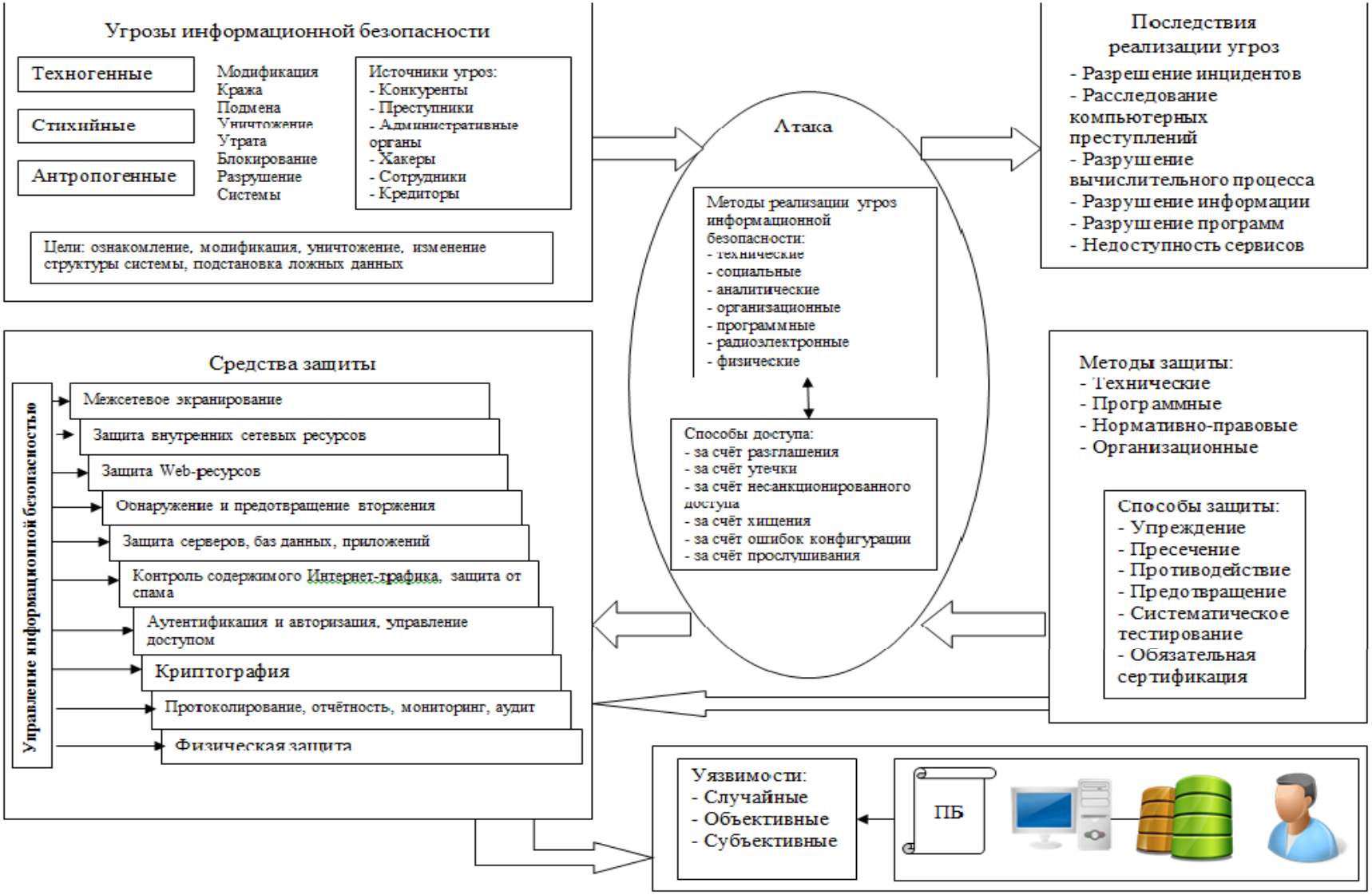

Рис. 1 - Концептуальная схема информационной безопасности

Обеспечивать защиту информации должен механизм, включающий в себя различные средства обеспечения безопасности: аппаратные, программные, организационные. Существует огромное множество различных вариантов построения информационной защиты, базирующееся на многообразии средств защиты. При проектировании защиты необходимо выбрать из эквивалентных средств наиболее эффективные относительно конкретной информационной системы.

К аппаратным средствам защиты относятся различные электронные, электронно-механические и электронно-оптические устройства. Примерами аппаратных средств являются устройства измерения индивидуальных характеристик человека (например, голоса, сетчатки глаза, отпечатков пальцев) с целью его идентификации, устройства для шифрования информации (криптографические методы), электронные ключи Соболь, eToken, SenseLock, Guardant, HASP.

К преимуществам аппаратных средств можно отнести их надежность, независимость от субъективных факторов, высокая устойчивость к модификации. Слабыми сторонами, в свою очередь, являются недостаточная гибкость, относительно большие объем и масса, высокая стоимость.

К программным средствам относятся программы для идентификации и аутентификации пользователей, контроля доступа, шифрования информации, тестирования информационной безопасности и др. Преимуществами программных средств являются универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатками — ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств). Можно выделить следующие виды средств программной защиты:

1) Антивирусная программа (антивирус) — программа для обнаружения наличия компьютерных вирусов в системе и их устранения без нанесения ущерба другим объектам системы, а также для профилактики — предотвращения проникновения вредоносного кода в файлы или операционную систему. Примерами антивирусных продуктов являются Panda компании «Panda Security», Dr. Web компании «Доктор Веб», Avira компании «Avira», Антивирус Касперского компании «Лаборатория Касперского», Avast компании «AVAST», AVG компании «AVG» и др.

2) Межсетевые экраны (также называемые брандмауэрами) – это специальные промежуточные серверы, размещаемые между локальной и глобальной сетями. Их целью является анализ и фильтрация проходящего через них трафика на сетевом и транспортном уровнях. Брандмауэры снижают угрозу несанкционированного доступа в систему извне, однако не устраняют вероятность угрозы полностью. Производителями межсетевых экранов являются фирмы Cisco, D-Link, Netgear, Zyxel, Fortinet, TP-Link и др.

3) Прокси-серверы – программные средства, которые полностью запрещают любой трафик на сетевом и транспортном уровнях между локальной и глобальной сетями. Вместо этого все обращения из локальной сети в глобальную проходят через специальные серверы-посредники. Недостатком этого метода является то, что он не дает достаточной защиты против атак на более высоких уровнях — например, на уровне приложения (вирусы, код Java и JavaScript). Примерами прокси-серверов являются 3proxy, CoolProxy, Eserv, HandyCache, nginx, Squid, Kerio Control.

4) VPN (виртуальная частная сеть) позволяет передавать секретную информацию через сети, в которых возможно прослушивание трафика посторонними людьми. Используемые технологии: PPTP, PPPoE, IPSec [3]. Примерами VPN являются FineVPN, ZorroVPN, HideMyAss, HotVPN, CryptoVPN, HotVPN, HideMe и др.

Организационные средства - это мероприятия, которые проводятся на протяжении всего цикла жизни распределённой системы с целью обеспечения защиты информации. Организационные мероприятия можно разделить на следующие группы:

1) мероприятия, осуществляемые при создании системы: проектирование системы защиты информации, её последующее тестирование и ввод в эксплуатацию;

2) мероприятия, осуществляемые в процессе эксплуатации информационной системы. В эту группу входят управление доступом (распределение паролей, полномочий и т.п.), организация пропускного режима и технологий автоматизированной обработки информации;

3) мероприятия общего характера: организация плановых и превентивных проверок механизма защиты, планирование мероприятий по защите информации и т.п.

Чтобы сделать информационную защиту наиболее эффективной, необходимо определить оптимальный набор используемых программно-аппаратных средств защиты информации. Для этого целесообразно использовать математическое моделирование, позволяющее формализовать параметры безопасности распределенных систем и выбрать наиболее подходящий вариант, основанный на конкретных условиях работы системы.

Наиболее часто в публикациях по заданной тематике используются механизмы нечёткой логики. Например, в работе [4] ставится задача повышения эффективности процесса управления рисками безопасности информационных систем и обоснованности выбора защитных мероприятий в нечетких условиях. В результате разработана методика оценки рисков безопасности, предложены алгоритмы для оценки свойств элементов систем, а также предложен метод согласования мнений экспертов.

Механизмы нечетких множеств также используются и для смежных задач информационного синтеза, возникающих при построении защиты. Данный подход применяется в [5]. В данной работе модифицирован метод нечеткого программирования и предложены алгоритмы, позволяющие осуществить выбор оптимальных структур многоуровневого информационного комплекса. В [6] разработан механизм многокритериального выбора системы управления базами данных с помощью метода анализа иерархий.

Также методы нечёткой логики используются для оценивания качества информационной защиты в распределённых системах. Например, в [7] разработан комплексный подход к оценке проектирования системы защиты информации; прогноз ее эффективности, анализ всех возможных слабых мест системы и оценка её устойчивости.

Также для анализа защиты информации используются алгебраические методы, позволяющие оценить криптографическую надёжность системы. Данный задача описана в работе [8].

Другой подход к оцениванию средств информационной защиты отражён в [9]. В данной работе предложена и исследована математическая модель выбора средств защиты персональных данных, основанная на решении задачи многокритериальной оценки альтернатив в условиях различной важности критериев.

Также в различных публикациях встречается нейросетевой подход к решению задачи обеспечения информационной безопасности. Наиболее ярко он выражен в [10]. В данной работе показано, что возможность определения состава средств защиты может быть обеспечена путем решения ряда задач целочисленной оптимизации с применением обработки многомерных данных в нейросетевом базисе.

Подобный подход используется и в [11]. В данной работе предложена комбинированная модель и алгоритмы защиты компьютерных сетей от инфраструктурных атак на основе подхода «нервная система сети».

Таким образом, можно сделать вывод, что наиболее часто используемыми подходами, используемыми при решении задач построения информационной защиты распределенных систем, являются механизмы нечеткой логики и нейросетевой подход. Основным недостатком систем, построенных с использованием нечеткой логики, является меньшая точность вычислений по сравнению с вероятностным подходом. Что касается использования нейросетевых механизмов, то их явным недостатком является скрытный характер функционирования, так как не всегда можно точно отследить критерии, которые нейронная сеть использует при работе. Интересным представляется подход, который заключается в применении более строгих и формализованных методов теории принятия решений. В случае использования данного подхода может быть получено более точное и обоснованное решение.

Наиболее оправданным видится рассмотрение поставленной задачи формирования информационной безопасности как задачи о рюкзаке - одной из задач комбинаторной оптимизации. Это связано со схожестью задач в формализованном виде и простотой интерпретации задачи формирования информационной защиты в терминах задачи о рюкзаке. Так, в качестве рюкзаков выступают точки размещения средств защиты (например, серверы, рабочие станции, маршрутизаторы), а в качестве предметов - средства защиты (антивирусы, межсетевые экраны и др). Задача построения информационной безопасности интерпретируется как укладка предметов в рюкзак: необходимо «уложить» как можно больше средств защиты, имеющих лучшую эффективность, при этом не превысив заданных ограничений.

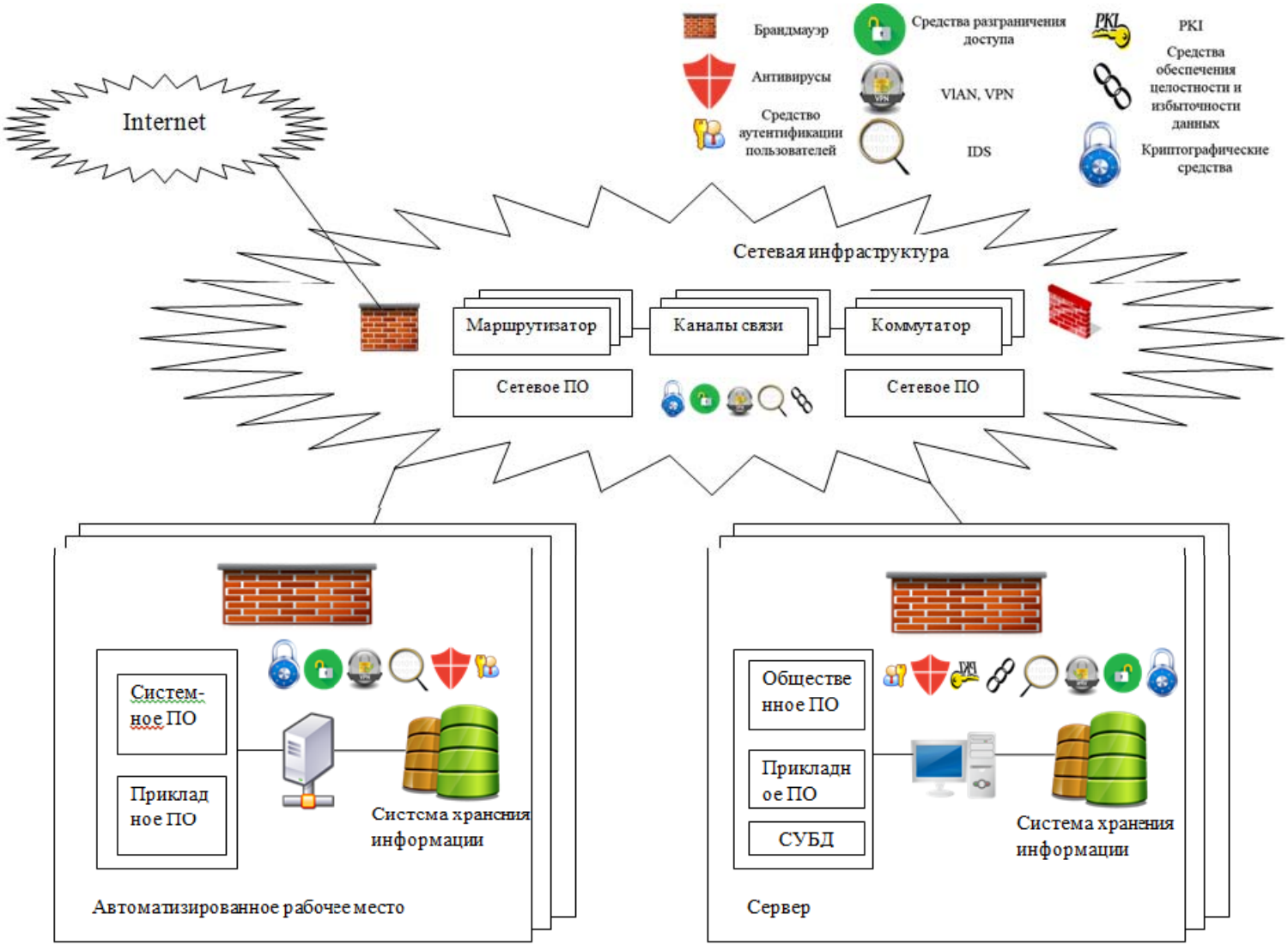

Рис. 2 - Структура точек размещения средств защиты информации

В математическом виде задачу о рюкзаке можно представить так: имеется n грузов. Для каждого j-го груза определён вес w_j и ценность p_j, $j = 1,...,n$. Дана вместимость c. Выбрать подмножество грузов, так чтобы их общий вес не превышал c, а суммарная их ценность была бы максимальной. Наиболее распространённой формой задачи является рюкзак 0-1: необходимо максимизировать

$$\sum_{j=1}^{n} p_j x_j \rightarrow max$$

таким образом, чтобы выполнялись условия:

$$\sum_{j=1}^{n} w_j x_j \leq c$$

$$x_j \in \{0,1\}, j = 1,...,n,$$

где x_j принимает значения 1 либо 0 и обозначает укладку предмета j в рюкзак.

Наиболее подходящими разновидностями задачи о рюкзаке для решения поставленной задачи формирования информационной защиты являются задача о рюкзаке с мультивыбором и задача о мультипликативном рюкзаке [12].

Суть задачи о рюкзаке с мультивыбором заключается в том, что все предметы разделены на k классов $N_{1,...,}N_k$, объединяющих в себе эквивалентные предметы, схожие по своему назначению. Обязательным является условие выбора предмета из каждого класса. Для каждого j-го груза, принадлежащего i-му классу, определён вес w_{ij} и ценность p_{ij}, $j = 1,...,n$. Необходимо найти количество x_{ij} предмета j, принадлежащего классу i.

Математически постановка задачи выглядит так:

$$z = \sum_{i=1}^{k} \sum_{j \in N_i} p_{ij} x_{ij} \rightarrow max$$

таким образом, чтобы выполнялись условия:

$$\sum_{i=1}^{k} \sum_{j \in N_i} w_{ij} x_{ij} \leq c$$

$$\sum_{j \in N_i} w_{ij} x_{ij} = 1, \quad i = 1, \ldots, k$$

$x_{ij} \in \{0,1\}$, $i = 1,\ldots,k$, j $\in N_i$

Задача о мультипликативном рюкзаке (или задача о нескольких рюкзаках) имеет следующую постановку [13]:

Пусть есть n предметов и m рюкзаков. У каждого предмета, как и раньше, есть ценность $p_j > 0$ и вес w_j. У каждого рюкзака есть своя вместимость c_i, $i = 1,\ldots,m$. Необходимо найти количество x_{ij} предмета j, укладываемого в рюкзак i. Задача:

$$\sum_{i=1}^{m} \sum_{j=1}^{n} p_{ij} x_{ij} \rightarrow max$$

так, чтобы выполнялись следующие условия:

$$\sum_{j=1}^{n} w_j x_{ij} \leq c_i, \quad i = 1, \ldots, m$$

$$\sum_{i=1}^{m} x_{ij} \leq 1, \quad j = 1, \ldots, n$$

$$x_{ij} \in \{0,1\},\ i = 1,\ldots,m,\ j = 1,\ldots,n$$

Таким образом, задачу формирования средств информационной защиты можно представить так: имеется m точек, на которых могут быть размещены средства информационной защиты. Каждая точка принадлежит одному из z классов. В качестве данных точек могут выступать серверы, рабочие станции и другие элементы распределённой сети.

На данных точках необходимо разместить средства информационной защиты. Всего имеется n средств информационной защиты. Каждое средство принадлежит какому-либо классу. Всего имеется k классов $N_{1,\ldots,}N_k$. Класс объединяет в себе эквивалентные средства защиты, одно из которых должно обязательно присутствовать в системе. Каждое средство имеет стоимость w_j и ресурсозатратность q_j.

Предлагается составить таблицу эффективности E, которая будет показывать эффективность e_{ijl} конкретного средства защиты l, принадлежащего классу j, относительно размещения на i-том классе точек. Цена не должна превышать фиксированную сумму C, а ресурсозатратность - значение Q.

Необходимо найти оптимальное количество x_{ijl} каждого средства защиты l из класса j, размещаемого на точке i.

Таким образом, задачу оптимизации средств размещения информационной защиты можно сформулировать так:

$$\sum_{i=1}^{z}\sum_{j=1}^{k}\sum_{l\in N_t} e_{ijl}x_{ijl} \rightarrow max$$

так, чтобы выполнялись следующие условия:

$$\sum_{i=1}^{k}\sum_{j\in N_t}\sum_{l\in N_t} w_{ijl}x_{ijl} \leq C$$

$$\sum_{i=1}^{k}\sum_{j\in N_t}\sum_{l\in N_t} q_{ijl}x_{ijl} \leq Q$$

$$\sum_{j\in N_t}\sum_{l\in N_t} x_{ijl} \geq 1$$

Таким образом, в данной статье было проведено описание понятия информационной безопасности и её составляющих, показано многообразие и эквивалентность используемых средств защиты. Кроме того, были рассмотрены существующие решения и подходы к построению структуры информационной безопасности, а также предложено решение данной проблемы, базирующееся на использовании методов теории принятия решений, в частности, задачи о рюкзаке.

Литература

1. Либкинд А.С. Информационная безопасность – история проблемы и ее решение. - Москва, 2009. - 20 с.

2. Варлатая С.К., Шаханова М.В. Аппаратно-программные средства и методы защиты информации. - Владивосток, 2007. - 318 с.

3. Платонов В.В. Программно-аппаратные средства защиты информации. - Москва, 2013. - 306 с.

4. Гильмуллин Т. М. Модели и комплекс программ процесса управления рисками информационной безопасности: Автореф. дис. канд. техн. наук: 05.13.18. - Казань, 2010. - 21 с.

5. Ширинкин М. С. Модели и методы синтеза оптимальной иерархической структуры многоуровневого информационного комплекса промышленного предприятия: Автореф. дис. канд. техн. наук: 05.13.01. - Москва, 2011. - 21 с.

6. Земцов А.Н., Болгов Н.В., Божко С.Н. Многокритериальный выбор оптимальной системы управления базы данных с помощью метода анализа иерархий // Инженерный вестник Дона, 2014, №2 URL: ivdon.ru/ru/magazine/archive/n2y2014/2360.

7. Тихонов Д. В. Модели оценки эффективности систем информационной безопасности: Автореф. дис. канд. эк. наук: 08.00.13. - Санкт-Петербург, 2009. - 19 с.

8. Маро Е.А. Алгебраический анализ стойкости криптографических систем защиты информации // Инженерный вестник Дона, 2013, №4 URL: ivdon.ru/magazine/archive/n4y2013/1996.

9. Голембиовская О. М. Автоматизация выбора средств защиты персональных данных на основе анализа их защищённости: Автореф. дис. канд. техн. наук: 05.13.19. - Брянск, 2013. - 19 с.

10. Асмолов Т. А. Защита информационных систем музейных и библиотечных фондов на основе решений задач комбинаторной оптимизации: Автореф. дис. канд. техн. наук: 05.13.19. - Москва, 2012. - 24 с.

11. Шоров А. В. Имитационное моделирование механизмов защиты компьютерных сетей от инфраструктурных атак на основе подхода "Нервная

система сети": Автореф. дис. канд. техн. наук: 05.13.19. - Санкт-Петербург, 2012. - 24 с.

12. Martelo S., Toth P. Knapsack problems - Wiley, 1990 – 1995. - 306 p.

13. Pisinger D. Knapsack problems. - Copenhagen, 1995. – 199 p.

References

1. Libkind A.S. Informacionnaja bezopasnost' – istorija problemy i ee reshenie. [Information security - history of the problem and its solution]. Moscow, 2009. 20 p.

2. Varlataja S.K., Shahanova M.V. Apparatno-programmnye sredstva i metody zashhity information. [Hardware and software tools and methods of information protection]. Vladivostok, 2007. 318 p.

3. Platonov V.V. Programmno-apparatnye sredstva zashhity informacii. [Software and hardware protection of information] Moscow, 2013. 306 p.

4. Gil'mullin T. M. Modeli i kompleks programm processa upravlenija riskami informacionnoj bezopasnosti. [Model and a set of programs process information security risk management]. Kazan, 2010. 21 p.

5. Shirinkin M. S. Modeli i metody sinteza optimal'noj ierarhicheskoj struktury mnogourovnevogo informacionnogo kompleksa promyshlennogo predprijatija. [Models and methods for the synthesis of optimal multi-level hierarchical structure information complex industrial plant]. Moscow, 2011. 21 p.

6. Zemcov A.N., Bolgov N.V., Bozhko S.N. Inženernyj vestnik Dona (Rus), 2014, №2 URL: ivdon.ru/ru/magazine/archive/n2y2014/2360.

7. Tihonov D. V. Modeli ocenki jeffektivnosti sistem informacionnoj bezopasnosti. [Models of evaluating the effectiveness of information security systems]. Saint-Petersburg, 2009. 19 p.

8. Maro E.A. Inženernyj vestnik Dona (Rus), 2013, №4 URL: ivdon.ru/magazine/archive/n4y2013/1996.

9. Golembiovskaja O. M. Avtomatizacija vybora sredstv zashhity personal'nyh dannyh na osnove analiza ih zashhishhjonnosti. [Automation of choice of means of protection of personal data on the basis of their security]. Bryansk, 2013. 19 p.

10. Asmolov T. A. Zashhita informacionnyh sistem muzejnyh i bibliotechnyh fondov na osnove reshenij zadach kombinatornoj optimizacii. [Protection of information systems museum and library collections based on the decisions of combinatorial optimization problems]. Moscow, 2012. 24 p.

11. Shorov A. V. Imitacionnoe modelirovanie mehanizmov zashhity komp'juternyh setej ot infrastrukturnyh atak na osnove podhoda "Nervnaja sistema seti. [Simulation of the protection of computer networks from infrastructure attacks based on approach "Nervous system network"]. Saint-Petersburg, 2012. 24 p.

12. Martelo S., Toth P. Knapsack problems. Wiley, 1990. 1995. 306 p.

13. Pisinger D. Knapsack problems.Copenhagen, 1995. 199p.