Инженерный вестник Дона, №1 (2017)
ivdon.ru/ru/magazine/archive/n1y2017/4078

Модификация математической модели выбора оптимальной стратегии информационной защиты распределённых систем

А.А. Кацупеев, Е.А. Щербакова, С.П. Воробьёв, Р.К. Литвяк

Южно-Российский Государственный Политехнический Университет (НПИ) имени М.И. Платова

Аннотация: В статье предлагается новая постановка задачи о рюкзаке, а также рассматривается математическая модель, используемая для решения задачи выбора оптимальной стратегии информационной защиты распределённых систем. Суть новой задачи выражается в использовании набора целей при комплектовании рюкзака.
Ключевые слова: информационная безопасность, защита информации, распределённая система, комбинаторная задача, математическое моделирование, задача о рюкзаке, эквивалентность, модель угроз.

Практическая реализация задачи построения оптимальной стратегии информационной защиты распределённой системы потребовала модификации, поскольку описанная в работе [1] модель информационной безопасности достаточно тяжело ассоциировалась с элементами реальной вычислительной сети. Целью данной работы является устранение проблемных мест в математической модели, что позволит лучше адаптировать модель под требования и особенности информационных систем.

В первую очередь, необходимо модифицировать исходную задачу о рюкзаке [2-3], поскольку задача о мультипликативном рюкзаке с мультивыбором не отражает возможности замещения предмета из одного класса предметом из другого класса, выполняющего сходные функции. Добавить такую возможность можно, если заменить общую ценность, относительно которой характеризуется каждый предмет, множеством целей. В таком случае каждый предмет будет иметь различную ценность для каждой из целей. Это позволяет отразить эквивалентность и взаимозаменяемость предметов. Так, благодаря такому дополнению задачи

мы можем заменить предмет из одного класса предметом из другого класса, если его ценность для достижения конкретной цели будет выше.

В математическом виде задача о мультипликативном рюкзаке с мультивыбором и эквивалентами выглядит так:

Пусть есть N предметов, разделенных на k классов, содержащих в себе соответственно $N_1,\ldots,N_k$ предметов, m рюкзаков и q целей. Для каждого j-го груза, принадлежащего l-му классу, определён вес w_{lj} и ценность относительно цели h p_{ljh}, $l = 1,\ldots,n$, $h = 1,\ldots,q$. У каждого рюкзака есть своя вместимость c_i, $i = 1,\ldots,m$. Необходимо найти количество x_{ilj} предмета j, принадлежащего классу l и укладываемого в рюкзак i. Задача:

$$\sum_{i=1}^{m}\sum_{h=1}^{q}\sum_{l=1}^{k}\sum_{j=1}^{N_l} p_{ljh}x_{ilj} \to max$$

$$\sum_{i=1}^{m}\sum_{l=1}^{k}\sum_{j=1}^{N_l} w_{lj}x_{ilj} \le c_i$$

$$\sum_{i=1}^{m}\sum_{l=1}^{k}\sum_{j=1}^{N_l} x_{ilj} \le 1$$

$$x_{ilj} = \begin{cases} 0, если\ не\ размещается \\ 1, если\ размещается \end{cases}, \; l = 1,\ldots,k, \; j \in N_l, \; i = 1,\ldots,m;$$

Таким образом, модель информационной защиты, аспекты которой рассмотрены также в работах [4-10], может быть представлена как задача о мультипликативном рюкзаке с мультивыбором и эквивалентами. Мультипликативность отражена в том что, существует множество элементов сети, на которых требуется разместить средства защиты (например, серверы, рабочие станции, активное сетевое оборудование (коммутаторы, маршрутизаторы) и т.д.). Данные элементы выступают в качестве «рюкзаков». Мультивыбор означает возможность выбора средств защиты из

нескольких классов. Классы объединяют в себе сходные по назначению контрмеры по противодействию угрозам. Так, классами являются антивирусы, межсетевые экраны и др., а «предметами» - непосредственно средства защиты. Эквиваленты в данной задаче отражают возможность противодействия каждой конкретной угрозе с помощью контрмер из различных классов. В общем виде 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. В формализованном виде модель выглядит следующим образом:

1) Множество элементов распределённой системы

K = $\{K_i = < LLK_1,...,LLK_K, CNT_i, KPR_i>, \ i = 1,...,KCOUNT\}$, где

$KCOUNT$ – количество элементов распределённой системы;

LLK_k, $k = 1,...,LCOUNT_i$ – показатели локальных ограничений, накладываемых на инструментарий узла сети.

$LCOUNT_i$ – количество локальных ограничений на узле сети K_i;

CNT_i – количество узлов типа K_i.

KPR_i – номер родительского узла в архитектуре сети. $KPR_i = 0$, если узел K_i является корневым.

2) Множество классов контрмер N = $\{N_m = <C_{ml}, O_{mz}, O_{mz}^{lim}, O_{mz}^{sign}, EKN_{mi}, ND_m, IND_{mzj}, PRDC_{mzj}, DRDC_{mzj}>, m = 1,...,NCOUNT,$ где

C_{ml}, $l = 1,...,CCOUNT_m$, $m = 1,..., NCOUNT$ – контрмеры, принадлежащие данному классу;

O_{mz}, $z = 1,...,OCOUNT_m$, $m = 1,..., NCOUNT$ – критерии, отражающие характеристики, по которым сравниваются элементы данного класса.

O_{mz}^{lim}, $z = 1,...,OCOUNT_m$, $m = 1,..., NCOUNT$ - предельное (идеальное) значение по критерию O_{mz}.

O_{mz}^{sign} = {-1;1}, $z = 1,...,OCOUNT_m$, $m = 1,..., NCOUNT$ – значение, отражающее показатель того, стремится ли значения критерия O_{mz} к минимуму или максимуму.

EKN_{mi}, $i = 1,...,KCOUNT$ – эффективность средств данного класса защиты относительно точки размещения контрмер K_i на элементе распределённой системы.

$NCOUNT$ – количество классов средств защиты.

ND_m = {-1;1} – показатель, отражающий, снижают ли средства защиты данного класса вероятность реализации угрозы, или же снижают потенциальный ущерб.

IND_{mzj} = [0,1] показатель участия критерия O_{mz} в противодействии угрозе D_j;

$PRDC_{mzj}$– максимальное уменьшение вероятности реализации угрозы D_j при предельном значении по критерию O_{mz}.

$DRDC_{mzj}$ – максимальное уменьшение потенциального ущерба в случае реализации угрозы D_j при предельном значении по критерию O_{mz}.

3) Контрмеры $C_{ml} = <OC_{mlz}, LLC_{mli}, ULC_{mlj}, KS_{ml}, IUL_{ml}>$, $l = 1,....CCOUNT_m$, где

$CCOUNT_m$ – количество контрмер по противодействию угрозам класса N_m;

OC_{mlz} – показатель данного средства защиты по критерию O_{mz};

LLC_{mli} – показатель данного средства защиты по расходу локального ресурса $LL_{i.}$;

ULC_{mlj} – показатель данного средства защиты по расходу общего ресурса $UL_{i.}$;

KS_{ml} = [-1;1] – коэффициент связности средства защиты C_{ml}, отражающий, снижается ли эффективность средства защиты на узле в случае наличия такого же средства защиты на вышестоящем узле сети (в случае

отрицательного значения), увеличивается (в случае положительного значения), или же эффективность остаётся неизменной (коэффициент связности равен нулю);

$IUL_{ml} = \{-1;1\}$ – показатель, отражающий, рассчитывается ли расход общего ресурса ULC_{mlj} как фиксированное для всей системы значение или как зависящее от количества элементов, на которых размещено средство защиты $C_{ml.}$;

4) Угрозы D представляются в виде следующего кортежа данных: $D_j = <K_i, P_{ji}, DMG_{ji}>, j = 1,...,DCOUNT$, где

$DCOUNT$ – количество угроз облачной системе;

$K_i, i = 1,...,KCOUNT$ – объекты воздействия;

$P_{ij}, \quad j = 1,...,DCOUNT, \quad i = 1,...,KCOUNT$ - вероятность угрозы D_j на объекте K_i;

$DMG_{ij}, \quad j = 1,...,DCOUNT, \quad i = 1,...,KCOUNT$ – ущерб объекту K_i в случае осуществления угрозы D_j.

5) Показатели общих ограничений, накладываемых на систему

$UL_j, j = 1,...,ULCOUNT,$ где

$ULCOUNT$ – количество общих ограничений.

Существует ряд особенностей, которые нужно учитывать при проектировании информационной безопасности. Можно выделить следующие ключевые моменты:

1) Угрозы воздействуют не целиком на распределённую систему, а на отдельные её элементы. В таком случае при успешной реализации угрозы j на узле сети i с вероятностью P_{ij}^0 вычислительной сети в целом будет нанесён ущерб DMG_{ij}^0. Поэтому необходимо определить индивидуальный набор средств защиты таким образом, чтобы минимизировать потенциальный ущерб системе PDU, представляющий из себя сумму локальных показателей

потенциального ущерба на каждом из элементов сети PDL_i. Принято решение суммировать показатели локального ущерба, потому что они выражены в условных денежных единицах и уже зависят от важности положения узла в сети.

2) Эффективность одного и того же средства защиты будет различаться в зависимости от места его размещения. В связи с этим целесообразно выражать эффективность контрмеры, исходя из критериев оценки класса защиты, к которому она относится. (E_{mlz} – значение средства защиты c по критерию O). Критерии оценки, в свою очередь, связаны с угрозами с помощью показателей $PRDC_{mzj}$ и $DRDC_{mzj}$, отражающими уменьшение вероятности реализации и потенциального ущерба соответственно от угрозы j при максимальном значении критерия O.

3) Элементы из некоторых классов защиты не могут быть размещены на определённых узлах сети. Для учёта таких случаев в модели введён показатель EKN_{im}, показывающий эффективность средств из класса защиты m на узле i.

4) Против одной и той же угрозы могут применяться средства из различных классов защиты. Подход с использованием критериев для оценки контрмер и связей между критериями и угрозами позволяет обеспечить решение с учётом эквивалентности средств защиты.

5) Поскольку некоторые средства защиты не имеет смысла дублировать на различных узлах системы, другие, напротив, показывают наибольшую эффективность только в том случае, если размещены на большом количестве элементов сети, целесообразно добавить в модель коэффициент связности KS_{ml}, отражающий показатель средства защиты l из класса m. В случае отрицательного значения эффективность средств защиты l, расположенных на нижестоящих узлах сети, уменьшается, в случае положительного – увеличивается, если на вышестоящем узле расположено средство защиты l.

Схематично задача оптимизации информационной безопасности изображена на рис. 1.

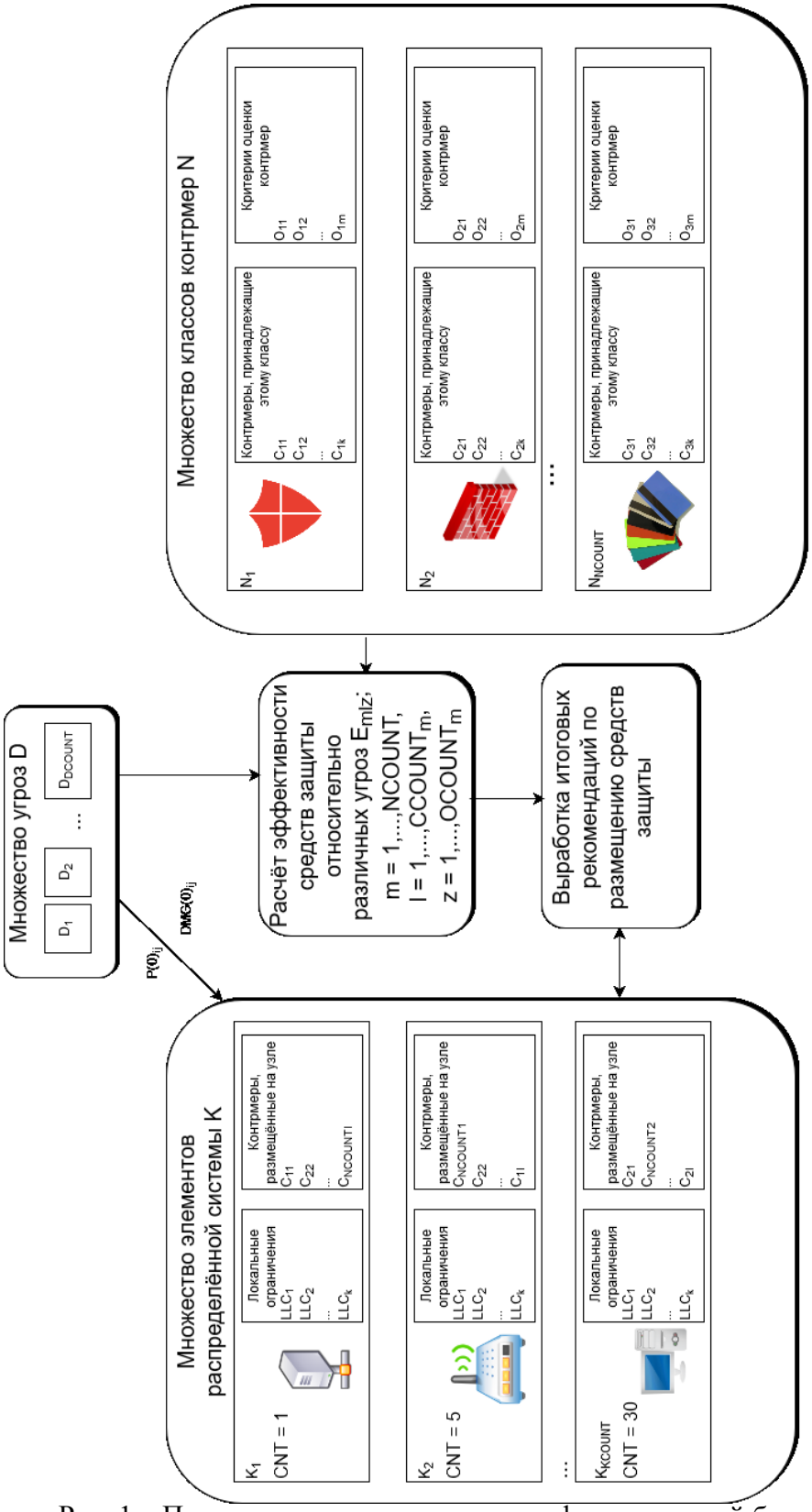

Рис. 1 – Пример схемы оптимизации информационной безопасности

Ключевым критерием является суммарный показатель потенциального ущерба системе, который рассчитывается как сумма показателей потенциального ущерба *PDL* узлов сети.

$$PDU = \sum_{i=1}^{KCOUNT} PDL_i;$$

Показатель потенциального ущерба PDL рассчитывается в отдельности для каждого элемента информационной системы и представляет собой произведение вероятности реализации угрозы на узле и потенциального ущерба в случае её реализации.

$$PDL_i = CNT_i * (\sum_{j=1}^{DCOUNT} (P_{ji} * DMG_{ij}));$$

Вероятность реализации угрозы P_{ij} рассчитывается по следующей формуле:

$P_{ij} = P_{ij}^0 - PRD_{ij}$, где

P_{ij}^0 – начальная вероятность реализации угрозы D_j на узле K_i;

PRD_{ij} – изменение вероятности реализации угрозы D_j на узле K_i вследствие размещённых на узле K_i мер противодействия угрозам C_l. Показатель PRD_{ij} рассчитывается следующим образом:

$$PRD_{ij} = \sum_{m=1}^{NCOUNT} \sum_{z=1}^{OCOUNT_m} \sum_{j=1}^{DCOUNT} (IND_{mzj} * PRDC_{mzj} * \sum_{l=1}^{CCOUNT_m} E_{mlz} * x_{mli});$$

, где

E_{mlz} – эффективность средства защиты по противодействию угрозе D_j на узле K_i по критерию O_z.

$$E_{mlz} = \frac{OC_{mlz}}{O_{mz}^{lim}};$$

x_{mli} – показатель наличия или отсутствия предмета C_l из класса N_m на узле K_i.

Объём потенциального ущерба DMG_{ij} рассчитывается по формуле:

$$DMG_{ij} = DMG_{ij}^0 - DRD_{ij}, \text{ где}$$

DMG_{ij}^0 – начальная вероятность реализации угрозы D_j на узле K_i;

DRD_{ij} – изменение потенциального ущерба в случае реализации угрозы D_j на узле K_i вследствие размещённых на узле K_i мер противодействия угрозам C_l. Показатель DRD_{ij} рассчитывается следующим образом:

$$DRD_{ij} = \sum_{m=1}^{NCOUNT} \sum_{z=1}^{OCOUNT_m} \sum_{j=1}^{DCOUNT} (IND_{mzj} * DRDC_{mzj} * \sum_{l=1}^{CCOUNT_m} E_{mlz} * x_{mli});$$

Таким образом, целевая функция выражена таким образом: необходимо минимизировать показатель общего потенциального ущерба:

$$PDU = \sum_{i=1}^{KCOUNT} (CNT_i * (\sum_{j=1}^{DCOUNT} (P_{ij}^0 - (\sum_{m=1}^{NCOUNT} \sum_{z=1}^{OCOUNT_m} \sum_{j=1}^{DCOUNT} (IND_{mzj} *$$

$$* PRDC_{mzj} * \sum_{l=1}^{CCOUNT_m} E_{mlz} * x_{mli})) * (DMG_{ij}^0 - \sum_{m=1}^{NCOUNT} \sum_{z=1}^{OCOUNT_m} \sum_{j=1}^{DCOUNT} (IND_{mzj} *$$

$$* DRDC_{mzj} * \sum_{l=1}^{CCOUNT_m} E_{mlz} * x_{mli}))))) \to min;$$

Безусловно, достижение максимальной эффективности возможно лишь при неограниченном запасе финансовых и аппаратных ресурсов, что в реальных условиях практически неосуществимо. Поэтому другим важным критерием оптимизации структуры безопасности является минимизация затрат по введению контрмер. Формализованно этот критерий выглядит следующим образом: необходимо свести к минимуму суммы расхода ресурсов по локальным и общим ограничениям, вызванных введением контрмер на узлах системы.

$$\sum_{i=1}^{KCOUNT} \sum_{j=1}^{NCOUNT} \sum_{l=1}^{CCOUNT} LLC_{ijl} \to min;$$

$$\sum_{i=1}^{KCOUNT}\sum_{j=1}^{NCOUNT}\sum_{l=1}^{CCOUNT} ULC_{ijl} \to min;$$

Таким образом, в данной статье представлена модификация задачи о рюкзаке, позволяющая учитывать множество целей при комплектовании рюкзака. На основании новой задачи предлагается модификация модели информационной безопасности.

Литература

1. Кацупеев А.А., Щербакова Е.А., Воробьёв С.П. Постановка и формализация задачи формирования информационной защиты распределённых систем // Инженерный вестник Дона. 2015. №1-2. URL: ivdon.ru/ru/magazine/archive/n1p2y2015/2868

2. Pisinger D. Knapsack problems. - Copenhagen, 1995. 199p.

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

4. 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.

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

6. 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.

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

8. 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.

9. 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.

10. 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.

References

1. Katsupeev A.A., Shcherbakova E.A., Vorobyev S.P. Inzhenernyj vestnik Dona (Rus), 2015, №1-2. URL: ivdon.ru/ru/magazine/archive/n1p2y2015/2868.

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

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

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

5. Gil'mullin T. M. Modeli i kompleks programm processa upravlenija riskami informacionnoj bezopasnosti [Models and a complex of programs of process of management of risks of information safety]: Avtoref. dis. kand. tehn. nauk: 05.13.18. Kazan', 2010. 21 p.

6. Shirinkin M. S. Modeli i metody sinteza optimal'noj ierarhicheskoj struktury mnogourovnevogo informacionnogo kompleksa promyshlennogo predprijatija [Models and methods for synthesizing the optimal hierarchical structure of a multilevel information complex of an industrial enterprise]: Avtoref. dis. kand. tehn. nauk: 05.13.01. Moskva, 2011. 21 p.

7. Tihonov D. V. Modeli ocenki jeffektivnosti sistem informacionnoj bezopasnosti [Models for assessing the effectiveness of information security systems]: Avtoref. dis. kand. jek. nauk: 08.00.13. Sankt-Peterburg, 2009. 19 p.

8. Golembiovskaja O. M. Avtomatizacija vybora sredstv zashhity personal'nyh dannyh na osnove analiza ih zashhishhjonnosti [Automation of the choice of means of protecting personal data on the basis of analysis of their security]: Avtoref. dis. kand. tehn. nauk: 05.13.19. Brjansk, 2013. 19 p.

9. Asmolov T. A. Zashhita informacionnyh sistem muzejnyh i bibliotechnyh fondov na osnove reshenij zadach kombinatornoj optimizacii [Protection of Information Systems of Museum and Library Collections on the Basis of Solving Combinatorial Optimization Problems]: Avtoref. dis. kand. tehn. nauk: 05.13.19. Moskva, 2012. 24 p.

10. Shorov A. V. Imitacionnoe modelirovanie mehanizmov zashhity komp'juternyh setej ot infrastrukturnyh atak na osnove podhoda "Nervnaja sistema seti" [Simulation modeling of mechanisms of protection of computer networks from infrastructural attacks on the basis of the approach "Nervous system of a network"]: Avtoref. dis. kand. tehn. nauk: 05.13.19. Sankt-Peterburg, 2012. 24 p.