ISSN 1992-6502 (Print) Вестник УГАТУ ISSN 2225-2789 (Online)
2015. Т. 19, № 1 (67).С. 248–253 http://journal.ugatu.ac.ru

УДК 004.056.5

РАЗРАБОТКА МОДЕЛИ ПЛАНИРОВАНИЯ ИСПОЛЬЗУЕМЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ЭЛЕКТРОННОЙ ТОРГОВОЙ ПЛОЩАДКИ

Э. Э. ЯНДЫБАЕВА[1], И. В. МАШКИНА[2]

[1]emma.yandybaeva@gmail.com, [2]mashkina.vtzi@gmail.com

ФГБОУ ВПО «Уфимский государственный авиационный технический университет» (УГАТУ)

Поступила в редакцию 5 ноября 2014 г.

Аннотация. Разработана модель планирования на основе адаптированного метода принятия решений по выбору рационального модульного состава средств защиты информации в информационной системе электронной торговой площадки. Решается задача выбора дополнительного набора средств защиты информации, включающего в себя подсистему распределенной фильтрации трафика, подсистему предотвращения вторжений и антивирусное средство. Описанный метод позволяет автоматизировать процесс выбора средств защиты информации для рассматриваемого объекта защиты.

Ключевые слова: система защиты информации; модель планирования; электронная торговая площадка.

Планирование используемых средств защиты информации (СрЗ) представляет собой процесс снятия неопределенности относительно модульного состава системы защиты информации (СЗИ) и точек установки, необходимых для использования СрЗ [1]. Планирование предложено выполнить в три этапа. Во-первых, составляется перечень требований к состоянию защищенности объекта защиты. Во-вторых, определяется модульный состав СЗИ. В-третьих, осуществляется процедура выбора СрЗ, необходимость внедрения которых была выявлена на предыдущем этапе.

В работе в качестве объекта защиты рассматривается информационная система (ИС) электронной торговой площадки (ЭТП). В общем случае на объекте защиты может присутствовать минимальный базовый состав СрЗ. Для повышения защищенности ИС ЭТП необходимо расширение модульного состава СЗИ, т.е. необходимо осуществить выбор дополнительных СрЗ, которые будут выступать барьерами на путях реализации актуальных угроз информационной безопасности (ИБ).

ОПРЕДЕЛЕНИЕ МОДУЛЬНОГО СОСТАВА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Решение задачи определения модульного состава СЗИИС ЭТП сводится к определению перечня дополнительных функциональных подсистем защиты информации, которые позволят повысить защищенность системы за счет нейтрализации актуальных угроз ИБ.

Авторами в работах [2, 3] разработана модель угроз ИБ в ИС ЭТП, на основании которой получены численные оценки угроз и определены следующие актуальные угрозы:

- хищение ключа электронной подписи;
- хищение логина и пароля от личного кабинета;
- срыв нормального функционирования сайта ЭТП.

Установлена необходимость введения дополнительных функциональных подсистем защиты информации с учетом актуальных угроз ИБ:

- подсистемы предотвращения вторжений (для локально-вычислительной сети оператора ЭТП);
- подсистемы распределенной фильтрации трафика (для фильтрации трафика, входящего в локально-вычислительную сеть оператора ЭТП);
- антивирусного средства (для рабочих станций клиентов ЭТП).

МЕТОД ВЫБОРА СРЕДСТВЗАЩИТЫ ИНФОРМАЦИИ

Для каждой из перечисленных выше функциональных подсистем существует конечное множество альтернатив с широким набором критериев их оценки. Следовательно, для реализации третьего этапа планирования необходим аналитический метод, позволяющий осуществлять многокритериальный выбор СрЗ для СЗИ. В работе для решения данной задачи разработан адаптированный метод принятия решений, базирующийся на методе ELECTRE1 Бернарда Руа [4]. Метод основан на попарном сравнении альтернатив по критериям выбора. Выявление критериев выбора СрЗ является творческой неформализуемой задачей, которая выполняется экспертом в области ИБ на основе его знаний, опыта и характеристик, декларируемых производителями СрЗ. Для каждого вида СрЗ, принадлежащих различным функциональным подсистемам, выявлен набор критериев качества, на основании которого будет осуществляться выбор лучшей альтернативы, а также разработаны иерархические структуры критериев качества.

В результате исследования сайтов производителей систем предотвращения вторжений выявлено 13 критериев. Для выявленных критериев разработана иерархическая структура, приведенная на рис. 1. Критерии обозначены переменными I_1, I_2, …,I_{13}.

Аналогично разработаны иерархические структуры критериев выбора подсистемы распределенной фильтрации трафика и антивирусного средства, включающие 10 и 31 критерий соответственно. В качестве примера приведена иерархическая структура критериев выбора подсистемы распределенной фильтрации трафика (рис. 2).

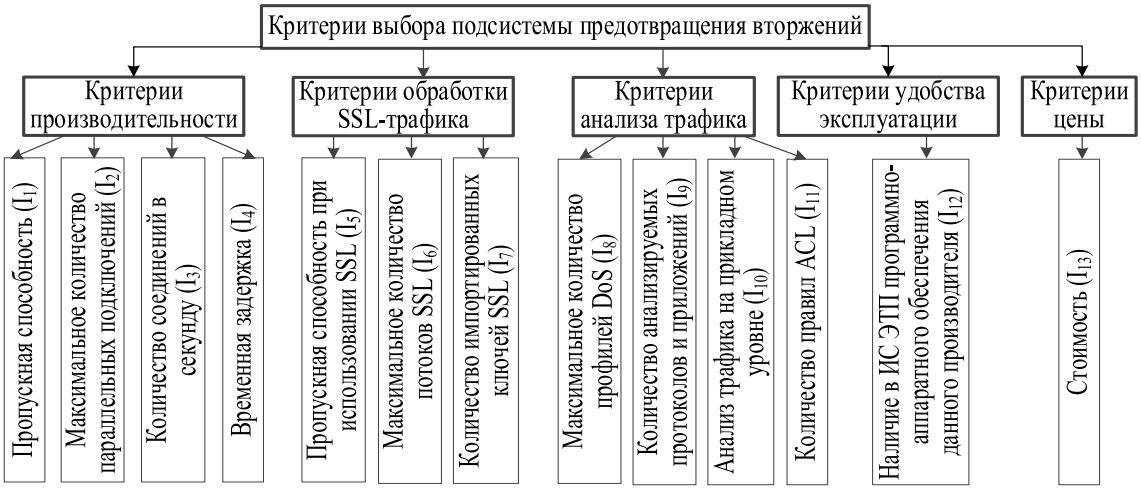

Рис. 1. Иерархическая структура критериев выбора подсистемы предотвращения вторжений

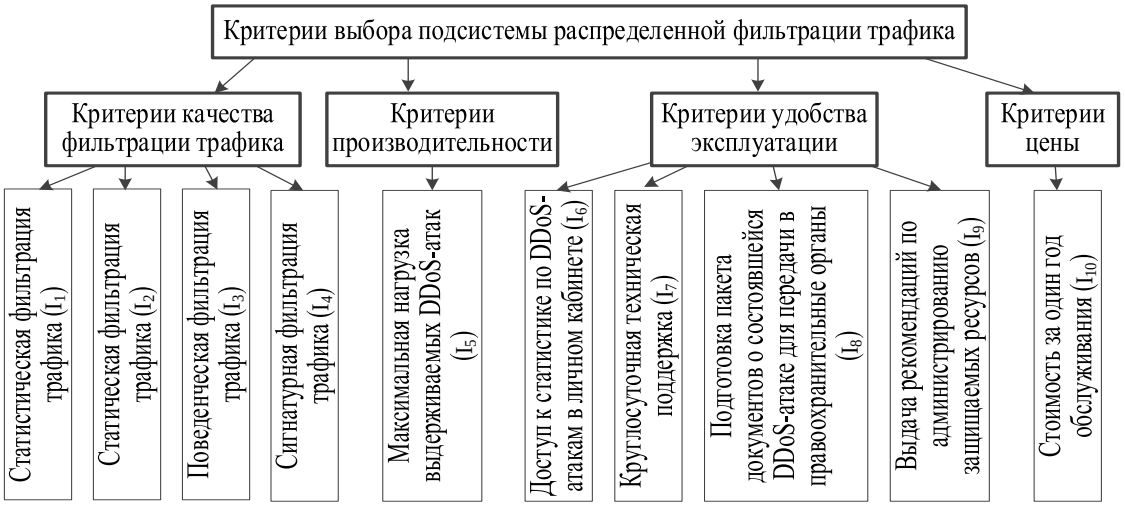

Рис. 2. Иерархическая структура критериев выбора подсистемы распределенной фильтрации трафика

В табл. 1 представлена проведенная оценка длин шкал выявленных критериев выбора подсистемы предотвращения вторжений, где в качестве граничных значений шкал берутся значения критериев, самые лучшие из всех предлагаемых производителями СрЗи самые худшие из допустимых для рассматриваемого объекта защиты. В случае наличия или отсутствия у рассматриваемого средства защиты – альтернативы того или иного функционала, выступающего в роли критерия, значение критерия принимается равным «1» или «0» соответственно. Длина шкалы критерия L_i вычисляется как разность между наилучшим и наихудшим значениями критерия. Каждому критерию присвоен вес – целое число w_i, характеризующее важность критерия.

Таблица 1

Оценка длин шкал критериев выбора подсистемы предотвращения вторжений

Критерий	Наилучшее значение	Наихудшее значение	Длина шкалы	Вес
I_1	x_1	y_1	L_1	w_1
I_2	x_2	y_2	L_2	w_2
I_3	x_3	y_3	L_3	w_3
I_4	x_4	y_4	L_4	w_4
I_5	x_5	y_5	L_5	w_5
I_6	x_6	y_6	L_6	w_6
I_7	x_7	y_7	L_7	w_7
I_8	x_8	y_8	L_8	w_8
I_9	x_9	y_9	L_9	w_9
I_{10}	Наличие функционала (1)	Отсутствие функционала (0)	1	w_{10}
I_{11}	x_{11}	y_{11}	L_{11}	w_{11}
I_{12}	Наличие функционала (1)	Отсутствие функционала (0)	1	w_{12}
I_{13}	x_{13}	y_{13}	L_{13}	w_{13}

Аналогично проведена оценка длин шкал выявленных критериев выбора подсистемы распределенной фильтрации трафика и антивирусного средства. Матрицы оценки отличаются размерностью, в зависимости от количества критериев.

Обозначим рассматриваемые функциональные подсистемы защиты информации следующими переменными:

- Ф1 – подсистема распределенной фильтрации трафика, входящего в локально-вычислительную сеть оператора ЭТП;
- Ф2 – подсистема предотвращения вторжений для локально-вычислительной сети оператора ЭТП;
- Ф3 – антивирусное средство для рабочей станции клиента ЭТП.

Обозначим альтернативы СрЗ для каждой из трех функциональных подсистем переменными $A_{11}, \ldots, A_{1K}$, $A_{21}, \ldots, A_{1L}$ и $A_{31}, \ldots, A_{3M}$, где K, L, M – количество рассматриваемых альтернатив для каждой функциональной подсистемы соответственно.

Согласно методу Бернарда Руа, если выдвигается гипотеза о превосходстве альтернативы A над альтернативойB, то множество I, состоящее из N критериев, разбивается на три подмножества:

- I^+– подмножество критериев, по которым А предпочтительнее B;
- $I^=$– подмножество критериев, по которым А равноценно B;
- I^-– подмножество критериев, по которым B предпочтительнее A.

Формируется индекс согласия c_{AB}с гипотезой о превосходстве A над B. Он подсчитывается на основе весов критериев и определяется как отношение суммы весов критериев I^+ и $I^=$ к общей сумме весов [4]:

_____.

В работе метод Бернарда Руа адаптирован и формализован в матричном виде для решения задачи многокритериального и многоальтернативного выбора набора СрЗ, входящих в состав нескольких функциональных подсистем. Результаты формализованного подхода представлены в виде матрицы для проведения расчетов индексов согласия (табл. 2).

Формируется индекс несогласия d_{AB} с гипотезой превосходства A над альтернативой B. Он определяется на основе самого «противоречивого» критерия – критерия, по которому B в наибольшей степени превосходит A:

_____,

где – значения альтернатив A и B по i-му критерию; L_i – длина шкалы i-го критерия [4].

По аналогии с табл. 2 составлена матрица для проведения расчетов индексов несогласия, представленная в табл. 3.

Далее требуется задание уровня согласия c и уровня несогласия d для определения бинарных отношений превосходства. Если $c_{A_1A_2} \geq c$ и $d_{A_1A_2} \leq d$, то альтернатива A_{11} объявляется лучшей по сравнению с альтернативой A_{12}. Аналогично сравниваются между собой остальные альтернативы.

Таблица 2

Матрица индексов согласия

		A_{11}	A_{12}	…	A_{1K}
Ф1	A_{11}	*	———	…	———
	A_{12}	———	*	…	———
	…	…	…	*	…
	A_{1K}	———	———	…	*
		A_{21}	A_{22}	…	A_{2L}
Ф2	A_{21}	*	———	…	———
	A_{22}	———	*	…	———
	…	…	…	*	…
	A_{2L}	———	———	…	*
		A_{31}	A_{32}	…	A_{3M}
Ф3	A_{31}	*	———	…	———
	A_{32}	———	*	…	———
	…	…	…	*	…
	A_{3M}	———	———	…	*

Таблица 3

Матрица индексов несогласия

		A_{11}	A_{12}	…	A_{1K}
Ф1	A_{11}	*	———	…	———
	A_{12}	———	*	…	———
	…	…	…	*	…
	A_{1K}	———	———	…	*
		A_{21}	A_{22}	…	A_{2L}
Ф2	A_{21}	*	———	…	———
	A_{22}	———	*	…	———
	…	…	…	*	…
	A_{2L}	———	———	…	*
		A_{31}	A_{32}	…	A_{3M}
Ф3	A_{31}	*	———	…	———
	A_{32}	———	*	…	———
	…	…	…	*	…
	A_{3M}	———	———	…	*

При этом возможно, что заданные уровни согласия и несогласия не позволят выделить одну лучшую альтернативу, а сформируют ядро из нескольких альтернатив. Для такого случая требуется введение более «слабых» значений уровней согласия и несогласия (меньший по значению уровень согласия и большей уровень несогласия), при которых выделяются ядра с меньшим количеством альтернатив (с одной альтернативой). Задача определения значений уровней согласия и несогласия является серьезной проблемой. Для ее решения возможно использование лишь знаний эксперта, который основывается в своих суждениях на сведениях о возможных длинах шкал критериев и на реальном опыте выбора СрЗ с помощью описанного выше метода.

Составим целевую функцию превосходства одной альтернативы над другой:

$$f = (c_{AB} \geq c_i) \ \& \ (d_{AB} \leq d_i).$$

Если $f = 1$, то альтернатива A объявляется лучшей по сравнению с альтернативой B. Если $f = 0$, то при заданных уровнях согласия и несогласия сравнить альтернативы не удалось.

Целевая функция выбора СрЗ из произвольного количества альтернатив для заданного множества функциональных подсистем защиты информации ИС ЭТП может быть описана в виде программного кода, включающего в себя множество циклов логических операций.

При проведении практических расчетов для апробации адаптированного метода Бернарда Руа в решении задачи определения состава СЗИ ИС ЭТП на основе анализа длин шкал критериев и опыта выбора СрЗ были выбраны значения уровней согласия и несогласия $c = 0{,}5$, $d = 0{,}1$.

Для антивирусного средства на основе заданных значений было определено ядро из нескольких лучших альтернатив. Для данной функциональной подсистемы выявилась необходимость понижения уровня согласия и повышения уровня несогласия, приняв $c = 0{,}3$ и $d = 0{,}2$, что позволило определить одну наилучшую альтернативу.

ЗАКЛЮЧЕНИЕ

Предложен и опробован на практике адаптированный метод выбора дополнительного набора СрЗ в ИС ЭТП, основанный на разработанной ранее модели угроз ИБ в ИС ЭТП и выявленных актуальных угрозах, а также на методе Бернарда Руа, базирующемся на попарном сравнении альтернатив, отличающийся осуществлением выбора целостного набора СрЗ, что потребовало разработки системы иерархических структур критериев качества СрЗ различных функциональных подсистем, определения размерности матрицы оценки длин шкал критериев выбора, составления матрицы индексов согласия и несогласия для функциональных подсистем, входящих в состав СЗИ.

Описанный выше метод позволяет сделать рациональный выбор дополнительного набора СрЗ для рассматриваемого в настоящей работе объекта защиты – ИС ЭТП. Однако приведенные расчеты являются очень трудоемкими и в свою очередь требуют автоматизации данного процесса. Предполагается продолжить работу в направлении разработки автоматизированного программного средства выбора СрЗ для ИС ЭТП.

СПИСОК ЛИТЕРАТУРЫ

1. **Гузаиров М. Б., Машкина И. В.** Управление защитой информации на основе интеллектуальных технологий: учебное пособие. М.: Машиностроение, 2013. 241 с. [[M. B. GuzairovandI. V. Mashkina, *Information protection management on a basis ofintellectual technologies*, (in Russian). Moscow: Mechanical Engineering, 2013.]]

2. **Яндыбаева Э. Э., Машкина И. В.** Модель угроз информационной безопасности электронной торговой площадки // ИБ-2013: XIII Междунар. науч.-практ. конф. Таганрог: Изд-во ЮФУ, 2013. С. 215–219. [[E. E. Yandybaeva and I. V. Mashkina, “The model of information security threats in the information system of electronic trading platform,” (in Russian), in *Proc. 13th Int. Workshop (Information Security-2013)*, Taganrog, Russia, 2013, pp. 215-219.]]

3. **Яндыбаева Э. Э., Машкина И. В.** Оценка актуальности угроз информационной безопасности в информационной системе электронной торговой площадки. // Безопасность информационных технологий. 2014. № 1. С. 41–44 [[E. E. YandybaevaandI. V. Mashkina, “The relevance assessment of information security threats in the information system of electronic trading platform”, (in Russian), in*Security of Information Technology*, no.1, pp. 41-44, 2014.]]

4. **Ларичев О. И.** Теория и методы принятия решений, а также Хроника событий в Волшебных Странах. М.: Логос, 2000. 296 с. [[O. I. Larichev, *Theory and methods of decision-making, as well as the Chronicle of events in Finding Neverland*, (in Russian). Moscow: Logos, 2000.]]

ОБАВТОРАХ

ЯНДЫБАЕВА Эмма Эмануиловна, асп. каф. вычислительной техники и защиты информации. Дипл. спец. по защите информации (УГАТУ, 2010). Готовит дис. Об управлении инф. безопасностью в системе эл. торг. площадок.

МАШКИНА Ирина Владимировна, проф. каф. вычислительной техники и защиты информации. Дипл. инж.-э/мех. (УГАТУ, 1974). Д-р техн. наук по методам и системам защиты информации, информационной безопасности (УГАТУ, 2009). Иссл. в обл. управления защитой информации на основе интеллектуальной технологии.

METADATA

Title: Development planning model of used information protection means for electronic trading platform information system.

Authors: E. E. Yandybaeva[1], I. V. Mashkina[2]

Affiliation:
Ufa State Aviation Technical University (UGATU), Russia.

Email: [1]emma.yandybaeva@gmail.com,
[2] mashkina.vtzi@gmail.com.

Language: Russian.

Source: Vestnik UGATU (scientific journal of Ufa State Aviation Technical University), vol. 19, no. 1 (67), pp. 248-253, 2015. ISSN 2225-2789 (Online), ISSN 1992-6502 (Print).

Abstract: The planning model on a basis of adapted decision-making method for rational choice of modular information protection means for electronic trading platform information system is developed. We solve the problem to choice additional set of information security means including intrusion prevention system, traffic distributed filtering system and antivirus. The described method allows to automate the process of information protection means choice for the object of protection under consideration.

Key words: information security system, planning model, electronic trading platform.

About authors:

YANDYBAEVA, Emma Emanuilovna, Postgrad. (PhD) Student, Dept. of Computing Equipment and Information Protection. Specialist of information protection (UGATU, 2010).

MASHKINA, Irina Vladimirovna, Prof., Dept. of Computing Equipment and Information Protection. Dipl. Electrical engineer (UGATU, 1974). Dr. of Tech. Sci. (UGATU, 2009).