УДК 681.518

Ю.И. Синещук, Т.И. Давыдова

МЕТОДИКА ОБОСНОВАНИЯ РАЦИОНАЛЬНОГО СОСТАВА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ С УЧЕТОМ РЕСУРСНЫХ ОГРАНИЧЕНИЙ

Синещук Юрий Иванович, доктор технических наук, профессор, заслуженный работник высшей школы РФ, окончил факультет боевых информационных управляющих систем Высшего военно-морского училища радиоэлектроники им. А.С. Попова. Профессор Санкт-Петербургского университета МВД России. Специализируется в области анализа и обеспечения информационной безопасности, устойчивости функционирования сложных систем. [e-mail: sinegal53@mail.ru].

Давыдова Татьяна Ивановна, кандидат технических наук, окончила радиотехнический факультет Ульяновского государственного технического университета. Ведущий инженер ФНПЦ АО «НПО «Марс». Имеет статьи и монографию в области расчетов надежности и эксплуатации радиотехнических средств. [e-mail: tasha_dav@inbox.ru].

Аннотация

Поиск оптимальной структуры системы информационной безопасности является важной задачей, сложность которой обусловлена ее неопределенным, вероятностным и нелинейным характером, особенно при наличии ресурсных ограничений. В статье рассмотрена математическая модель определения стоимости ущерба, предотвращенного средствами защиты информации, и затрат на их установку и техническое обслуживание. Критерием оптимизации является минимальная стоимость предотвращенного ущерба. Переменными задачи являются количества средств защиты различных типов, установленных в системе безопасности. Предложена методика обоснования рационального состава средств защиты информации с учетом экономических ограничений.

Ключевые слова: принятие решения, угроза информационной безопасности, система защиты информации, математическая модель, ущерб.

doi: 10.35752/1991-2927-2021-1-63-13-19

THE TECHNIQUE OF SUBSTANTIATING THE RATIONAL COMPOSITION OF INFORMATION SECURITY TOOLS WITH CONSTRAINED RESOURCES

Iurii Ivanovich Sineshchuk, Doctor of Sciences in Engineering, Professor; Honored Worker of the Higher School of the Russian Federation; graduated from the Faculty of Combat Information Management Systems of the A.S. Popov Higher Naval Academy of Radio Electronics; Professor of the St. Petersburg University of the MIA of Russia; specializes in the field of information analysis and security, stability of complex systems. e-mail: sinegal@rambler.ru.

Tatiana Ivanovna Davydova, Candidate of Sciences in Engineering; graduated from the Radioengineering Faculty of Ulyanovsk State Technical University; Leading Engineer at FRPC JSC 'RPA 'Mars'; an author of articles and monograph in the field of calculations of radio equipment performance reliability. e-mail: tasha_dav@inbox.ru.

Abstract

Finding the optimal structure of an information security system is an important task complicated by its uncertain, stochastic and nonlinear nature especially, if resources are constrained. The article considers a mathematical model for determining the cost of damage prevented by information security tools, and the cost of their installation and maintenance. The optimization criterion is the minimum cost of the damage prevented. Task variables are the number of different types of security features installed in the security system. The authors propose a methodology to substantiate rational composition of information security tools, taking into account economic constraints.

Keyword: decision-making, threat to information security, information security system, mathematical model, damage.

ВВЕДЕНИЕ

С развитием информационных технологий проблемы обеспечения безопасности информации в процессе обработки, передачи, хранения в информационных (автоматизированных) и телекоммуникационных системах становятся все более актуальными.

Наиболее эффективным способом решения проблем информационной безопасности является обеспечение надлежащего уровня защиты информации путем создания системы информационной безопасности (Information Security System – ISS) как от случайного, так и от преднамеренного искажения, уничтожения или хищения информации. ISS состоит из ряда подсистем, в основе которых лежат комплексы организационных, законодательных, физических, аппаратных методов и средств [1–3]. Динамичность развития (изменения) информационной среды неизбежно приводит к необходимости модернизации или замены ISS. Основная трудность в работе по созданию ISS и управлению информационной безопасностью организации связана с выбором рационального набора методов и средств защиты информации каждого вида в составе ISS.

Обоснование состава методов и средств защиты информации предполагает проведение предварительного анализа возможных угроз информационной безопасности. В общем случае, негативные воздействия на информационную систему по своей природе могут быть различными: внешние физические деструктивные факторы; внутренние деструктивные факторы, исследуемые в рамках анализа надежности; электромагнитные помехи; программно-информационные воздействия, или кибератаки [4, 5]. Последняя группа факторов характерна именно для компьютерных сетей, так как именно компьютерная обработка информации является средой распространения кибератак ISS, как разновидность сложной кибернетической системы, взаимодействующей с различными физическими объектами (источники угроз, сами угрозы информационной безопасности, формы реализации атак). Ее можно рассматривать как киберфизическую систему (Cyber-Physical System – CPS), или как одну из компонент CPS более высокого уровня, например АСУ [6, 7].

Обоснование рационального состава элементов ISS, как сложной системы с элементами неопределенности, связанными с нечеткой информацией, характеризующей реальные кибератаки, предполагает использование методов моделирования как основного средства количественного обоснования принимаемых решений. Характерные требования к оценке эффективности функционирования сложных технических систем по целому ряду конфликтующих друг с другом показателей качества приводят к актуальной задаче многокритериальной оптимизации. Известно достаточно много моделей и методик, позволяющих получить оценку защищенности. Однако большинство из них не рассматривают в явном виде вопросы стоимости внедряемых средств защиты и получаемого эффекта, вопросы оптимизации создаваемой ISS [8, 9].

1 Постановка задачи

Одной из важнейших задач построения комплексной ISS является выбор из множества существующих средств такого набора, который позволит обеспечить нейтрализацию всех возможных угроз с лучшим качеством и низким уровнем затраченных на это ресурсов [10–12].

Рис. 1. График зависимости ожидаемых суммарных затрат от затрат на защиту и ожидаемых потерь

Пусть мы имеем возможность оценить ожидаемые финансовые потери на объекте от инцидентов, связанных с информационной безопасностью, за определенный отрезок времени, например за год, при условии, что средств защиты информации нет. Точка 1 графика на рисунке 1 [13].

Сложив ожидаемые потери от атак при заданных вариантах затрат на систему защиты информации, получим кривую ожидаемых суммарных затрат, точки 2, 3, 4 и 5 на рисунке 1. Тогда идеальным будет набор средств защиты информации, соответствующий минимуму функции «ожидаемые суммарные затраты» (точка 3 графика).

Пусть в результате анализа защищаемого объекта выявлен перечень защищаемых ресурсов и перечень возможных угроз этим ресурсам. Пусть число этих угроз равно m . Обозначим интенсивность возникновения угрозы типа i символом λ_i , ущерб от однократной реализации угрозы типа i – символом R_i . Будем считать, что λ_i и R_i – величины постоянные. Количество различных типов средств защиты информации – n . Стоимость j -го элемента равна C_j , а интенсивность расходов на его обслуживание в момент времени t – $D_j(t)$. Зависимость интенсивности расходов на обслуживание от времени связана в основном с инфляцией – h . Обозначим $P_{ij}(t)$ – вероятность предотвращения угрозы типа i элементом типа j в момент времени t . Неизвестное пока количество элементов типа j в составе ISS обозначим X_j . Множество переменных X_j состоит из двух

разновидностей: целочисленные и двоичные переменные. Переменная X_j является целочисленной, если при увеличении числа элементов типа j в составе ISS эффективность ее работы возрастает. К таким элементам относится, например, число символов пароля или ключа при криптографическом закрытии информации.

Переменная X_j является двоичной (может принимать только два значения: ноль и единица). При увеличении числа элементов типа j в составе ISS свыше единицы эффективность ее остается постоянной. К числу таких элементов относятся: система обнаружения вторжений (Intrusion Detection System – IDS), сетевая система управления событиями информационной безопасности (Security Information and Event Management – SIEM), антивирусные программы и тому подобное [14–16].

В качестве критерия эффективности выберем величину убытков, предотвращенных в результате использования ISS, Z . В общем случае эта величина равна величине предотвращенного ущерба минус затраты на установку ISS и ее сопровождение.

Рассчитаем математическое ожидание суммарной величины предотвращенного ущерба

$$Z(T) = R(T) - M(T), \quad (1)$$

где $R(T)$ – предотвращенный ущерб;

$M(T)$ – затраты на установку системы защиты информации и ее сопровождение.

Будем считать, что при отсутствии ISS каждая информационная атака заканчивается успешно. Допустим, что вероятность возникновения двух и более угроз в один момент времени пренебрежимо мала (условие ординарности потока угроз). Обозначим $X = (X_1, X_2, \dots, X_n)$ – вектор, j -я компонента которого равна числу элементов типа j в составе ISS.

Найдем среднюю вероятность обнаружения i -й угрозы j -м средством за время T :

$$\bar{P}_{ij}(T) = \frac{1}{T} \cdot \int_0^T P_{ij}(t) \cdot dt. \quad (2)$$

Среднюю вероятность того, что ни одно из X_j средств типа j не обнаружит i -й угрозы, найдем из соотношения:

$$Q_{ij}(X_j, T) = (1 - \bar{P}_{ij}(T))^{X_j}. \quad (3)$$

Тогда средняя вероятность того, что хоть одно из средств обнаружит i -ю угрозу на отрезке времени T , может быть подсчитана по формуле:

$$P_i(X, T) = 1 - \prod_{j=1}^n Q_{ij}(X_j, T), \quad (4)$$

а математическое ожидание величины предотвращенного ущерба за время T может быть вычислено по формуле:

$$R(X, T) = \sum_{i=1}^n R_i \cdot \lambda_i \cdot T \cdot P_i(X, T). \quad (5)$$

Рассчитаем суммарные ожидаемые расходы на установку и сопровождение ISS. Стоимость покупки и сопровождения средств в течение интервала времени T составляет

$$M_j(X_j, T) = \left[C_j + \int_0^T D_j(t) \cdot dt \right] \cdot X_j. \quad (6)$$

Следовательно, общая сумма расходов на создание и сопровождение ISS в течение интервала времени T равна:

$$M(X, T) = \sum_{j=1}^n \left[C_j + \int_0^T D_j(t) \cdot dt \right] \cdot X_j. \quad (7)$$

Вычтя из величины предотвращенного ущерба (5) величину расходов на создание и сопровождение ISS (7), получим ожидаемую величину убытков, предотвращенных в результате использования ISS за время T ,

$$Z(X, T) = \sum_{i=1}^4 R_i \cdot \lambda_i \cdot T \cdot P_i(X, T) - M(X, T). \quad (8)$$

В качестве ограничений примем: пусть расходы на приобретение и установку элементов ISS не должны превышать C_0 , а расходы на обслуживание ISS в начальный момент времени – D_0 . Этим двум условиям соответствуют ограничения:

$$\sum_{j=1}^n C_j \cdot X_j \leq C_0, \quad (9)$$

$$\sum_{j=1}^n D_j(0) \cdot X_j \leq D_0. \quad (10)$$

Кроме того, на основании физического смысла, сформулируем еще два ограничения:

$$X_j - \text{целые, для } j = 1, 2, \dots, k, \quad (11)$$

$$X_j - \text{булевы, для } j = k + 1, \dots, n. \quad (12)$$

Таким образом, задача выбора рационального состава ISS может быть записана в виде задачи математического программирования:

$$\begin{aligned} \max_{X, T} Z(X, T) = \\ = \sum_{i=1}^4 R_i \cdot \lambda_i \cdot T \cdot P_i(X, T) - M(X, T), \end{aligned} \quad (13)$$

при ограничениях (9)–(12), где $P_i(X, T)$ и $M(X, T)$ вычисляются соответственно по (4) и (7).

2 ИСХОДНЫЕ ДАННЫЕ

Рассмотрим процесс решения сформулированной выше задачи выбора состава ISS с помощью програм-

мной надстройки «Поиск решения» электронных таблиц Excel.

Сложность решения этой задачи зависит от количества возможных угроз – m , от количества возможных элементов ISS – n , от вида функций $P_{ij}(t)$, $D_j(t)$ и тому подобное.

Пусть число возможных угроз (m) равно четырем, а число возможных элементов ISS (n) – пяти. Допустим, что

$$P_{ij}(t) = P_{ij}(0) \cdot \alpha_{ij}^t. \quad (14)$$

Это предположение основано на очевидных аксиомах:

- функция $P_{ij}(t)$ находится в пределах от нуля до единицы;

- функция $P_{ij}(t)$ является невозрастающей функцией от t .

Пусть:

$$\|P_{ij}(0)\| = \begin{pmatrix} 0,934 & 0,907 & 0,958 & 0,876 & 0,907 \\ 1 & 0 & 0,432 & 0,578 & 0,911 \\ 0,234 & 0,907 & 0,786 & 0 & 0,211 \\ 0 & 1 & 0 & 0,902 & 0 \end{pmatrix},$$

$$\|\alpha_{ij}\| = \begin{pmatrix} 0,993 & 0,989 & 0,989 & 0,991 & 0,977 \\ 0,917 & 0,01 & 0,926 & 0,935 & 0,991 \\ 0,811 & 0,954 & 0,863 & 0,01 & 0,745 \\ 0,01 & 0,971 & 0,01 & 0,995 & 0,01 \end{pmatrix}.$$

Допустим также, что

$$D_j(t) = D_j(0) \cdot (1+h)^t. \quad (15)$$

Это допущение исходит из того, что расходы на обслуживание ISS растут в разной пропорции для каждого ISS.

Зададим векторы:

$$h = \begin{pmatrix} 0,014 \\ 0,009 \\ 0,012 \\ 0,011 \\ 0,012 \end{pmatrix}, D(0) = \begin{pmatrix} 100 \\ 70 \\ 90 \\ 80 \\ 60 \end{pmatrix}, R = \begin{pmatrix} 10550 \\ 38166,67 \\ 59000 \\ 74666,67 \end{pmatrix},$$

$$\lambda = \begin{pmatrix} 0,011 \\ 0,0204 \\ 0,0288 \\ 0,0385 \end{pmatrix}, C = \begin{pmatrix} 1000 \\ 850 \\ 900 \\ 1200 \\ 1350 \end{pmatrix}.$$

Пусть $C_0 = 9000$, а $D_0 = 600$ условных единиц. Кроме того, пусть переменные X_1, X_2, X_3 являются целочисленными, а переменные X_4, X_5 – булевыми.

Подставив эти данные в (13), (14) и (15) и выполнив ряд преобразований, получим задачу целочисленного программирования:

$$\max_{X,T} Z(X,T) = \sum_{i=1}^4 R_i \cdot \lambda_i \cdot T \cdot P_i(X,T) - M(X,T), \quad (16)$$

$$P_i(X,T) = 1 - \prod_{j=1}^5 Q_{ij}(X_j, T), \quad (17)$$

$$Q_{ij} = \left[1 - \frac{P_{ij}}{T \cdot \ln(a_{ij})} \cdot (a_{ij}^T - 1) \right]^{X_j}, \quad (18)$$

$$M(X,T) = \sum_{i=1}^5 \left\{ C_j + \frac{D_j}{\ln(1+h_j)} \cdot \left[(1+h_j)^T - 1 \right] \right\} \cdot X_j, \quad (19)$$

$$\sum_{j=1}^5 C_j \cdot X_j \leq 9000, \quad (20)$$

$$\sum_{j=1}^5 D_j(0) \cdot X_j \leq 600. \quad (21)$$

3 ЭКСПЕРИМЕНТАЛЬНЫЕ РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

Пример ввода исходных данных, промежуточные результаты в соответствии с выражениями (16)–(19), ограничения, вычисленные в соответствии с (20), а также конечный результат решения оптимизационной задачи показаны на рисунке 2.

Из рисунка 2 видно, что для решения задачи потребовалось модельное время t , равное 100 итерациям. Кроме того, все значения, соответствующие стоимости, округлены до целых значений, а значения вектора X в рассмотренном примере являются дробными. Следовательно, необходимо провести дополнительные исследования, связанные с вычислением целевой функции и ограничений для целых значений вектора X , которые являются соседями для результирующих дробных значений. Для этих целей может использоваться та же самая электронная таблица, в которой следует ввести новые целые значения вектора X и получить для них значения целевой функции и ограничений. Результаты этих вычислений представлены в таблице.

Результаты, представленные в строках 1–8 в таблице, получены следующим образом. Для бинарных переменных были получены следующие решения: $X_4 = 1$, $X_5 = 0$. Это означает, что в ISS необходимо включить средство защиты четвертого типа, но, в силу ограничений по затратам на эксплуатацию ISS, средство защиты пятого типа из ISS исключается. Для подтверждения это-

Выбор рационального состава системы защиты информации						
1. Исходные данные						
Угрозы		4		Типов средств		5
Количество средств		Стоимость средств		Начальн. расх. на обслух		Инфляция
X1	0,202416794	C1	1000	D1(0)	100	1,014
X2	2,451122029	C2	850	D2(0)	70	1,009
X3	3,28352728	C3	900	D3(0)	90	1,012
X4	1	C4	1200	D4(0)	80	1,011
X5	0	C5	1350	D5(0)	60	1,012
t	89,51557684					
Ущерб от угрозы		Интенсивность угрозы				
R1	10550	L1	0,011			
R2	38166,67	L2	0,0204			
R3	59000	L3	0,0288			
R4	74666,67	L4	0,0385			
Начальная вероятность отвода i-й угрозы j-м средством						
Pij	1	2	3	4	5	
1	0,934	0,907	0,958	0,876	0,907	
2	1	0	0,432	0,528	0,911	
3	0,234	0,907	0,788	0	0,211	
4	0	1	0	0,902	0	
Интенсивность создания средств нападения aij						
aj	1	2	3	4	5	
1	0,993	0,989	0,989	0,991	0,997	
2	0,917	0,01	0,926	0,935	0,911	
3	0,811	0,954	0,863	0,01	0,991	
4	0,01	0,971	0,01	0,955	0,01	
2. Расчет целевой функции						
Вероятность неотведения i-й угрозы Xj средствами типа j						
Qij	1	2	3	4	5	
1	0,787220783	0,8406852	0,827288	0,8304756	0,725391309	
2	0,713072771	1	0,853223	0,7968574	0,75328474	
3	0,959607407	0,457371	0,817299	1	0,598663824	
4	1	0,6476406	1	0,7847048	1	
Вероятность отведения i-й угрозы Xj средствами типа j						
хоть одним из средств C3ij			M(Xj, T)			
P1(X, T)			3800,4476			
P2(X, T)			25639,372			
P3(X, T)			50247,4			
P4(X, T)			13357,862			
P5(X, T)			0			
Целевая функция Z			204089,05			
Уравнения ограничений						
Значения			Пределы			
c1x1+c2x2+c3x3+c4x4+c5x5			8441,0451 9000			
D1x1+D2x2+D3x3+D4x4+D5x5			567,33768 600			

Рис. 2. Исходные данные, промежуточные и конечные результаты решения задачи

го вывода в таблице включены строки 9–10, в которых $X_5 = 0$. Видно, что в этих случаях нарушаются требования по ограничению D_0 , определяющему допустимые затраты, равные 600. При этом если положить, что предельное значение этого ограничения равняется не 600, а 630, то в этом случае целевая функция принимает самое малое значение из значений, представленных в таблице. Следовательно, анализ результатов решения

задачи полностью исключает использование средства защиты пятого типа.

Для целочисленных переменных X_1 , X_2 , и X_3 , как видно из рисунка 2, оптимальные значения находятся в следующих диапазонах: для X_1 – в диапазоне [0; 1], для X_2 – в диапазоне [2; 3], для X_3 – в диапазоне [3; 4]. Поэтому в таблице в строках 1–8 находятся решения, в которых значения этих переменных соответствуют границам указанных выше интервалов. Эти решения соответствуют идеям применения метода ветвей и границ и метода отсечений, очень часто применяющегося для решения целочисленных оптимизационных задач. Перебор возможных комбинаций допустимых значений переменных X_1 , X_2 , и X_3 (значения переменных X_4 и X_5 не изменяются) приводит к появлению решений задачи, приведенных в строках 1–8 таблицы.

Анализ решений в строках 1–8 таблицы показывает, что четвертый, шестой, седьмой и восьмой варианты решения являются недопустимыми. В этих вариантах затраты на эксплуатацию ISS превышают допустимые затраты. Из допустимых решений максимальное значение целевой функции достигается в первом варианте решения. Следовательно, первый вариант следует считать оптимальным целочисленным вариантом [16].

ЗАКЛЮЧЕНИЕ

Предложенная модель выбора рационального варианта системы защиты информации позволяет рассчитать наиболее приемлемый (по выбранному критерию эффективности и при заданной системе ограничений) вариант системы защиты информации. В модели учитываются как стоимостные характеристики создаваемой (модернизируемой) системы защиты информации, так и показатели защищенности.

Данная модель может быть использована при составлении плана работ по созданию ISS и при принятии решения о том, следует действующую ISS менять на

Таблица

Оценка оптимальности вариантов целочисленного решения задачи

№ варианта	Целочисленные переменные					$Z(X)$	$C(X)$	$D(X)$
	X_1	X_2	X_3	X_4	X_5			
1	0	2	3	1	0	200147	5600	490
2	1	2	3	1	0	191796	6600	590
3	0	3	3	1	0	200025	6450	560
4	1	3	3	1	0	191674	7450	660
5	0	2	4	1	0	198807	6500	580
6	1	2	4	1	0	190456	7500	680
7	0	3	4	1	0	198685	7350	650
8	1	3	4	1	0	190334	8350	750
8	1	3	4	1	0	190334	8350	750
10	0	3	4	1	1	183259	8700	710

новую или достаточно ее модернизировать. При этом решение о модернизации или замене принимает руководитель организации с учетом результатов моделирования и ряда других факторов.

СПИСОК ЛИТЕРАТУРЫ

1. Котенко И.В., Саенко И.Б., Юсупов Р.М. Аналитический обзор докладов Международного семинара «Научный анализ и поддержка политик безопасности в киберпространстве» (SA&PS4CS 2010) // Труды СПИИРАН. Вып. 13. СПб. : Наука, 2010. С. 226–248.
2. Luvanda A., Kimani S., Kimwele M. Identifying Threats Associated With Man-In-The Middle Attacks during Communications between a Mobile Device and the Back End Server in Mobile Banking Applications // *IOSR Journal of Computer Engineering (IOSR-JCI)*. 2014. 12(2). pp. 35–42.
3. Чобанян В.А., Шахалов И.Ю. Анализ и синтез требований к системам безопасности объектов критической информационной инфраструктуры // *Вопросы кибербезопасности*. 2013. № 1 (1). С. 17–27.
4. Синешчук Ю.И., Яковлев О.В., Терехин С.Н. Информационный риск в условиях электромагнитного терроризма // *Вестник Санкт-Петербургского университета ГПС МЧС России*. 2012. № 3. С. 15–18. URL: <https://vestnik.igps.ru/wp-content/uploads/V43/3.pdf>.
5. Синешчук Ю.И., Примакин А.И., Яковлева Н.А. Основные угрозы и направления обеспечения безопасности единого информационного пространства // *Вестник Санкт-Петербургского университета МВД*. 2013. № 2. С. 150–154.
6. Peter W. Singer and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2014.
7. Edward A. Lee. The Past, Present and Future of Cyber-Physical Systems: A Focus on Models // *Sensors (Basel)*. 2015. 15(3). pp. 4837–4869.
8. Методы и алгоритмы решения многокритериальных задач – Классификационный подход / М. Салуквадзе, Н. Джигладзе, В. Майсурадзе, А. Топчишвили // *Model Assisted Statistics and Applications*. 2007. 2(4). С. 239–251. DOI: 10.3233/MAS-2007-2406.
9. A method of constructing a structured database of the typical objects of protection on the basis of cluster analysis / D. Minkin, Yu. Sineshchuk, S. Terekhin, K. Yusharov // *Journal of Theoretical and Applied Information Technology*. 31st October 2017. Vol. 95, № 20. pp. 5331–5339.
10. Implementing «method of successive concessions» in selecting the optimal variant to protect a corporate network / A.B. Diallo, D.T. Dim, S.R. Bakasov, V.N. Bogatkov // *The Eurasian Scientific Journal*. 2018. 1 (10). URL : <https://cyberleninka.ru/article/v/implementing-method-of-successive-concessions-in-selecting-the-optimal-variant-to-protect-a-corporate-network>.
11. Попова Е.В. Выбор системы защиты информации путем обеспечения конкурентоспособности предприятий // *Научно-технический вестник информационных технологий, механики и оптики*. 2014. № 2 (90). С. 155–160.
12. Kotenko I., Sineshchuk Yu., Saenko I. Optimizing Secure Information Interaction in a Distributed Computing System by the Method of Sequential Concessions // *Proceedings – 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, PDP 2020, Vasteras, Sweden Conference Paper, March 2020*.
13. Boehmer W. Cost-benefit trade-off analysis of an ISMS based on ISO 27001 // *The Forth International Conference on Availability, Reliability and Security (ARES 2009)*, 2009. pp. 392–399.
14. Проблема обоснования рационального состава средств системы защиты информации / А.И. Примакин, В.И. Куватов, Ю.И. Синешчук, М.Ю. Синешчук // *Вестник Санкт-Петербургского университета МВД*. 2017. № 4. С. 130–135.
15. Синешчук Ю.И., Куватов В.И., Синешчук М.Ю. Модель выбора рационального состава системы защиты информации критически важных, потенциально опасных объектов // *Региональная информатика и информационная безопасность : сб. тр. Вып. 2 / СПОИСУ*. СПб., 2016. С. 249–255.
16. An Approach to Optimization of Information Security System Based on Accounting of the Prevented Damage Cost / I. Kotenko, I. Saenko, Yu. Sineshchuk, V. Kuvatov, O. Chudakov // *Proceedings of ACM 12th International Conference on Security of Information and Networks, Sochi, Russia, September 12–15, 2019 (SIN 2019)*, Article No. 7.

REFERENCES

1. Kotenko I.V., Saenko I.B., Yusupov R.M. Analiticheskiy obzor dokladov Mezhdunarodnogo seminar "Nauchnyi analiz i podderzhka politik bezopasnosti v kiberprostranstve" (SA&PS4CS 2010) [Analytical Review of Talks on the Internet Conference "Mathematical Methods and Architectures for Computer Network Security" (MMM-ACNS-2010)]. *Trudy SPIIRAN* [Informatics and Automation. SPIIRAS Proc.]. St. Petersburg, Nauka Publ., 2010, iss. 13. pp. 226–248.
2. Luvanda A., Kimani S., Kimwele M. Identifying Threats Associated with Man-In-The Middle Attacks during Communications between a Mobile Device and the Back End Server in Mobile Banking Applications. *IOSR Journal of Computer Engineering (IOSR-JCI)*, 2014, 12(2), pp. 35–42.
3. Chobanian V.A., Shakhlov I.Iu. Analiz i sintez trebovaniy k sistemam bezopasnosti obektov kriticheskoi informatsionnoi infrastruktury [Analysis and Synthesis of the Requirements to the Systems of Safety of Objects of the Critical Information Infrastructure]. *Voprosy kiberbezopasnosti* [Cybersecurity Issues], 2013, no. 1 (1), pp. 17–27.
4. Sineshchuk Iu.I., Yakovlev O.V., Terekhin S.N. Informatsionnyi risk v usloviakh elektromagnitnogo terrorizma [Information Risk under Electromagnetic Terrorism]. *Vestnik Sankt-Peterburgskogo universiteta GPS MChS Rossii* [Proc. of the Saint-Petersburg University of State Fire Service of EMERCOM of Russia], 2012, no. 3, pp. 15–18. Available at: <https://vestnik.igps.ru/wp-content/uploads/V43/3.pdf>.

5. Sineshchuk Iu.I., Primakin A.I., Yakovleva N.A. Osnovnye ugrozy i napravleniia obespecheniia bezopasnosti edinogo informatsionnogo prostranstva [Basic Threats and Directions of Providing Safety of Single Informative Space]. *Vestnik Sankt-Peterburgskogo universiteta MVD* [Proc. of the Saint-Petersburg University of the MIA of Russia], 2013, no. 2, pp. 150–154.
6. Peter W. Singer and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2014.
7. Edward A. Lee. The Past, Present and Future of Cyber-Physical Systems: A Focus on Models. *Sensors (Basel)*, 2015, no. 15 (3), pp. 4837–4869.
8. Salukvadze M., Jibladze N., Maisuradze V., Topchishvili A. Metody i algoritmy resheniia mnogokriterialnykh zadach – Klassifikatsionnyi podkhod [Methods and Algorithms for Solving Multicriteria Problems – Classification Approach]. *Model Assisted Statistics and Applications*, 2007, iss. 2(4), pp. 239–251. DOI: 10.3233/MAS-2007-2406.
9. Minkin D., Sineshchuk Iu., Terekhin S., Yusharov K. A Method of Constructing a Structured Database of the Typical Objects of Protection on the Basis of Cluster Analysis. *Journal of Theoretical and Applied Information Technology*, 31st October, 2017, vol. 95, no. 20, pp. 5331–5339.
10. Diallo A.B., Dim D.T., Bakasov S.R., Bogatkov V.N. Implementing “Method of Successive Concessions” in Selecting the Optimal Variant to Protect a Corporate Network. *The Eurasian Scientific Journal*, 2018, no. 1 (10). Available at: <https://cyberleninka.ru/article/v/implementing-method-of-successive-concessions-in-selecting-the-optimal-variant-to-protect-a-corporate-network>.
11. Popova E.V. Vybory sistem zashchity informatsii putem obespecheniia konkurentosposobnosti predpriatii [Selection of Information Protection System by Ensuring the Competitiveness of Enterprises]. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologiy, mekhaniki i optiki* [Sci. and Tech. Journal of Information Technologies, Mechanics and Optics], 2014, no. 2 (90), pp. 155–160.
12. Kotenko I., Sineshchuk Yu., Saenko I. Optimizing Secure Information Interaction in a Distributed Computing System by the Method of Sequential Concessions. *Proceedings – 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, PDP 2020*. Vasteras, Sweden Conference Paper, March 2020.
13. Boehmer W. Cost-Benefit Trade-off Analysis of an ISMS based on ISO 27001. *The Forth International Conference on Availability, Reliability and Security (ARES 2009)*. 2009, pp. 392–399.
14. Primakin A.I., Kuvatov V.I., Sineshchuk Iu.I., Sineshchuk M.Iu. Problema obosnovaniia ratsionalnogo sostava sredstv sistemy zashchity informatsii [The Problem of Substitution of Rational Structure of System of Information Security]. *Vestnik Sankt-Peterburgskogo universiteta MVD* [Proc. of the Saint-Petersburg University of the MIA of Russia], 2017, no. 4, pp. 130–135.
15. Sineshchuk Iu.I., Kuvatov V.I., Sineshchuk M.Iu. Model vybora ratsionalnogo sostava sistemy zashchity informatsii kriticheski vazhnykh, potentsialno opasnykh obektov [Models Selection Rational Structure of Information Protection of Critical, Potentially Dangerous Objects]. *Regionalnaia informatika i informatsionnaia bezopasnost. Sb. tr.* [Proceedings. Regional Informatics and Information Security]. St. Petersburg, SPOISU Publ., 2016, iss. 2, pp. 249–255.
16. Kotenko I., Saenko I., Sineshchuk Iu., Kuvatov V., Chudakov O. An Approach to Optimization of Information Security System Based on Accounting of the Prevented Damage Cost. *Proceedings of ACM 12th International Conference on Security of Information and Networks (SIN 2019)*. Sochi, Russia, September 12–15, 2019, Article No. 7.