Научная статья
УДК 005.3:004.056:51
doi: 10.34987/vestnik.sibpsa.2024.85.25.006

Управление системой обеспечения информационной безопасности посредством выбора и формирования оптимального набора средств защиты объекта информатизации в подразделениях силовых ведомств на основе применения алгоритмов теории игр

Сергей Алексеевич Воронов[1]
Алексей Иванович Примакин[1]
Дмитрий Николаевич Саратов[2]

[1]*Санкт-Петербургский военный ордена Жукова институт войск национальной гвардии Российской Федерации, Санкт-Петербург, Россия*
[2]*Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия*
Автор ответственный за переписку: *Дмитрий Николаевич Саратов, saratovdn@mail.ru*

Аннотация. В статье рассматривается вопрос управления системой обеспечения информационной безопасности посредством выбора и формирования оптимального набора средств защиты объекта информатизации. Для решения данной задачи предлагается применение алгоритмов теории игр, платежные матрицы которых сводятся к моделированию конфликтных ситуаций и выбору оптимальных стратегий на основании критериев Байеса, Вальда, Гурвица и Лапласа. Приводится пример применения указанных критериев для выбора стратегий, построенный на результатах анализа статистического материала по актуальным киберугрозам и вероятностям их отражения различными средствами защиты объекта информатизации, что позволяет обеспечить необходимый уровень информационной безопасности в структурных подразделениях силовых ведомств.

Ключевые слова: информационная безопасность, математические методы, теория игр, критерии Вальда и Гурвица.

Для цитирования: Воронов С.А., Примакин А.И., Саратов Д.Н. Управление системой обеспечения информационной безопасности посредством выбора и формирования оптимального набора средств защиты объекта информатизации в подразделениях силовых ведомств на основе применения алгоритмов теории игр // Сибирский пожарно-спасательный вестник. 2024. № 1 (32). С. 48-57. https://doi.org/ 10.34987/vestnik.sibpsa.2024.85.25.006

Administration of a system for information security system for election and facilitation of the protection measures for information in the power bodies under the application of the agricultural arrangements of the game theory

Sergey A. Voronov[1]
Alexey I. Primakin[1]
Dmitry N. Saratov[2]

[1]*Saint-Petersburg military order of Zhukov institute of national guard Troops of the Russian Federation, Saint-Petersburg, Russia*
[2]*Saint-Petersburg university of State fire service EMERCOM of Russia, Saint-Petersburg, Russia*
Corresponding author: *Dmitry N. Saratov, saratovdn@mail.ru*

Abstract. The article deals with the issue of managing the information security system through the selection and formation of an optimal set of means of protecting the object of informatization. To solve this problem, the use of game theory algorithms is proposed, payment matrices of which are reduced to modeling conflict situations and choosing optimal strategies based on Bayes criteria, Valda, Hurwitz and Laplace. An example of the application of these criteria for the selection of strategies, based on the results of the analysis of statistical material on current cyber threats and the probabilities of their reflection by various means of protecting the object of informatization, which allows to provide the necessary level of information security in the structural units of law enforcement agencies.

Keywords: information security, mathematical methods, game theory, Wald and Hurwitz criteria.
For citation: Voronov S.A., Primakin A.I., Saratov D.N. Administration of a system for information security system for election and facilitation of the protection measures for information in the power bodies under the application of the agricultural arrangements of the game theory // Siberian Fire and Rescue Bulletin.2024; 1(32): P. 48-57. (In Russ.). https://doi.org/ 10.34987/vestnik.sibpsa.2024.85.25.006

Введение

Актуальность темы определяется необходимостью решения задач по управлению системой обеспечения информационной безопасности в структурных подразделениях силовых ведомств, что в значительной степени продиктовано сложившимися военно-политическими условиями в стране и мире [1, 2, 3].

Решение этих задач связано с обеспечением конфиденциальности, доступности и целостности информационных потоков, что обеспечивается благодаря правовым, организационно-техническим и экономическим методам защиты информации [4].

Интересующая нас (в рамках данной статьи) область организационных методов защиты, в первую очередь, связана с определением направлений и методик разработки политики безопасности структурных подразделений силовых ведомств. Для решения ряда частных задач в этой области, например, выбор и формирование оптимального набора средств защиты объектов информатизации ведомства от различного рода кибератак, необходим соответствующий математический инструментарий. Задачи, требующие оперативного и рационального принятия решений, могут быть лучше решены с помощью теории игр, которая первоначально предназначалась для решения проблем в экономике, тем не менее, она хорошо зарекомендовала себя во многих других областях, решив достаточное количество разнообразных задач, в том числе и по обеспечению защиты информации [5, 6, 7].

Теория игр, как раздел прикладной математики, сводится к моделированию ситуации, в которой противостоящие друг другу стороны (обычно их называют игроками) принимают связанные и зависимые друг от друга решения, называемые стратегиями. В этой ситуации каждый игрок, вырабатывая и принимая ту или иную стратегию, учитывает возможные стратегии, принимаемые другим игроком. Успех в подобном противостоянии зависит от анализа и угадывания стратегии противника, необходимо «думать, как противник», что позволит выбрать оптимальную стратегию в соответствующей ситуации.

Для поиска оптимального набора средств защиты объектов информатизации структурного подразделения силового ведомства от различного рода кибератак можно предложить двухстороннюю

математическую игру, в которой одним из игроков выступает сама система защиты объекта информатизации, а в качестве игрока-противника – возможные атаки нарушителя-хакера. Поскольку цель данной статьи – это определение оптимальной стратегии, принимаемой администратором сети, при которой возможные потери от нападения на объект информатизации нарушителем-хакером будут минимальны, будем считать, что цель противника в этой ситуации – нанести как можно больший ущерб атакуемому объекту. Эту ситуацию можно определить формулой: возможный «выигрыш» хакера равносилен «проигрышу» администратора сети.

Часто возникают ситуации, когда один из игроков, допустим «защитник» объекта информатизации, имеет не полную информацию о действиях противника, может только предполагать о принимаемых нарушителем-хакером решениях и стратегиях. В этом случае для практического применения теории игр необходим набор конечных и предсказуемых хакерских стратегий, построенных на вероятностных моделях, сформированных на результатах анализа статистических данных за предшествующий период времени, например, по киберпреступлениям.

Решение задач по обеспечению информационной безопасности, в основе которых лежит применение математического аппарата теории игр, условно можно разделить на две группы [8].

Первая группа (назовем ее группа А) описывает взаимодействие между игроками «нападение-защита». Дается вероятностная оценка той или иной стратегии, принимаемой противником, и вероятность принимаемых в этом случае ответных мер со стороны защиты.

Вторая группа (группа В) формирует количественные оценки уровня защиты объекта информатизации на основе вероятностного прогноза выбора стратегий со стороны нападающего и ответных действий защиты. В данном случае для оценки уровня информационной безопасности используют понятие риска, как метрики.

Первую группу игр А можно условно разделить на две подгруппы игр – А1 и А2.

Первая подгруппа А1 связана с игровыми ситуациями, когда у каждого из игроков имеются только по две возможные стратегии (альтернативные): «нападать» – «не нападать», «защищаться» – «не защищаться». Эта подгруппа связана с обобщенной и в значительной степени упрощенной конфликтной ситуацией между игроками. Эти игры (байесовские игры) рассматриваются, как статические игры с двумя игроками, они считаются «классическими», соответствующий математический аппарат разработан и проверен на практике. По этой причине результат игры подгруппы А1 легко просчитывается.

Подгруппа А2 связана с учетом большего количества внешних факторов, а значит и более сложной для математического моделирования игровой ситуацией. В этом случае, как правило, учитываются дополнительные параметры, например, технические характеристики объекта информатизации или параметры информационной сети, в которой происходит взаимодействие конфликтующих сторон. Очевидно, что моделирование игр подгруппы А2 более реалистично, однако требование описания динамики действий противников значительно усложняет и увеличивает объем проводимых математических вычислений и не всегда обеспечивает необходимый уровень точности.

В рамках статьи предлагается рассмотреть методику применения теории игр относительно защиты объектов информатизации структурных подразделений силовых ведомств от различного рода кибератак с использованием алгоритмов расчета критериев Байеса, Лапласа, Вальда и Гурвица.

Предлагаемые алгоритмы относятся к подгруппе А1 теории игр.

Подгруппа А1 предполагает наличие «защитника» информации и «нарушителя» ее целостности, конфиденциальности и доступности. Или так: «защитник» – это используемые средства защиты информации, а «нарушитель» – типы атак на объект информатизации со стороны нарушителя-хакера. Взаимосвязь между игроками определяется платежной матрицей, в этом случае игра называется «матричной» и считается статистической игрой. Общепринято одного из игроков, в нашем случае «защитника» информации, называть лицом, принимающим решение (ЛПР).

Схематично структура платежной матрицы представлена на Рис. 1.

	S1	S2	…	Sj
Стратегия 1 ЛПР	ω_{11}	ω_{12}	⋯	ω_{1j}
Стратегия 2 ЛПР	ω_{21}	ω_{22}	⋯	ω_{2j}
…	…	…	…	…
Стратегия i ЛПР	ω_{i1}	ω_{i2}	⋯	ω_{ij}

Рис.1. Структура платежной матрицы статистической игры

В данной игре строки матрица – стратегии, принимаемые «защитником» объекта информатизации, т.е. ЛПР, а столбцы матрицы S_1, S_2, …, S_j – состояния «окружающей среды» (разновидности угроз на объект информатизации, стратегии нарушителя-хакера); ω_{ij} – ожидаемый проигрыш (потери) при использовании стратегии i ЛПР, если «окружающая среда» находится в состоянии S_j (j угроза на объект информатизации). В качестве коэффициентов платежной матрицы ω_{ij} возможно рассматривать, например, финансовые или материальные потери для всех вариантов комбинаций S_j и выбираемой в этом случае ЛПР соответствующей стратегии. Проведя анализ платежной матрицы, можно заранее оценить затраты каждой стратегии по защите объекта информатизации и выбрать наиболее эффективные варианты для всего диапазона угроз S_j.

Если в сформированной платежной матрице ω_{ij} отражает материальные потери от атак нарушителя-хакера, то наилучшей в этом случае стратегией ЛПР будет та, в которой средние потери от ее принятия будут минимальные, т.е., когда $\sum_{i=1}^{m} \omega_{ij}$ будет минимальна.

Цели нарушителя-хакера и «защитника» объекта информатизации антагонистичны: первый стремится получить больший выигрыш, а цель «защитника» – минимизировать его выигрыш. В этом случае, оптимальная стратегия ЛПР определяется значением элемента матричной игры, называемым критерием «минимакса»:

$$\omega_{i_0 j_0} = minmax\omega_{ij}. \quad (1)$$

Для обеспечения информационной безопасности в подразделениях силовых ведомств возможно применение и других критериев, помимо критерия «минимакса» [9].

Поставим в соответствие каждой стратегии i, которую выбирает ЛПР, некоторое число W, вычисляемое с помощью платежной матрицы (Рис. 1). Именно алгоритмы расчета данного числа W определяют методику применения того или иного критерия для выбора соответствующей стратегии.

Критерий Вальда, называемый иногда критерием «максимина», гарантирует выбор наилучшей стратегии из всех наихудших, т.е. обеспечивает выбор «осторожно-пессимистической» стратегии, когда полностью исключают какой-либо риск.

$$W = maxmin\omega_{ij}, \quad (2)$$

где $i = \overline{1,m}$; $j = \overline{1,n}$.

Обычно критерий Вальда применяют в случаях, когда наблюдаются различные внешние состояния S_j (т.е. проявляются различные виды угроз для объекта информатизации), ЛПР определяет стратегию только один раз и намерено полностью исключить какой-либо риск. Критерий уместен в тех случаях, когда ЛПР не столько хочет выиграть (ущерб от проникновения нарушителя-хакера на объект информатизации минимальный из всех возможных), сколько не хочет проиграть, т.е. что бы потери от проникновения нарушителя-хакера на объект информатизации не были бы самыми большими из всех возможных вариантов. Выбранную стратегию условно можно охарактеризовать, как «пессимистическую».

Если ЛПР известна информация о вероятностях проявления различного вида угроз p_j, хотя бы на основании статистических исследований проявления различного вида угроз за определенный

промежуток времени [10], возможно применение критерия экстремального математического ожидания Байеса, где алгоритм расчета числа *W* по каждой из стратегий ЛПР определяется формулой:

$$W_i = \sum_{j=1}^{n} p_j \cdot \omega_{ij}. \quad (3)$$

В этом случае оптимальной считается стратегия, удовлетворяющая условию:

$$W_{i_{\text{опт}}} = min_i \sum_{j=1}^{n} p_j \cdot \omega_{ij}. \quad (4)$$

С предполагаемыми вероятностями разновидности атак со стороны нарушителя-хакера p_j связан еще один критерий – критерий недостаточного основания Лапласа. Он принимается за основу выбора стратегии ЛПР, когда информация о p_j неполная, когда считается, что все угрозы, количество которых *n*, равновероятны ($p_j = \frac{1}{n}$). Тогда, согласно данному критерию, алгоритм расчета числа *W* определяется формулой:

$$W_i = \frac{1}{n} \cdot \sum_{j=1}^{n} \omega_{ij}. \quad (5)$$

Оптимальная стратегия удовлетворяет условию:

$$W_{i_{\text{опт}}} = min_i \frac{1}{n} \cdot \sum_{j=1}^{n} \omega_{ij}. \quad (6)$$

Критерием Гурвица предпочитают пользоваться в ситуации, когда ЛПР пытается определить степень риска с помощью задаваемого α-коэффициента в ходе выбора стратегии. Другими словами, ЛПР ориентируется на некоторый средний результат эффективности (или показатель эффективности g_i) выбранной стратегии, лежащий между «пессимизмом» и «оптимизмом» (между «максимином» и «минимаксом»).

В случае чистых стратегий показатель эффективности g_i определяется по формуле.

$$gi = \alpha * max\omega_{ij} + (1 - \alpha) * min\omega_{ij}, \quad (7)$$

где $i = \overline{1,m}$.

Критерий Гурвица определяет оптимальной ту стратегию, у которой показатель эффективности g_i принимает максимальное значение.

$$W = maxgi = max\left[\alpha * max\omega_{ij} + (1 - \alpha) * min\omega_{ij}\right], \quad (8)$$

где $i = \overline{1,m}$; $j = \overline{1,n}$.

Обычно, α-коэффициент принимают равным 0,5, т.к. для выбираемой стратегии сложно определить доли пессимизма и оптимизма; выбор α-коэффициента носит субъективный характер.

Легко заметить, что в случае, когда α=0, то критерий Гурвица превращается в критерий Вальда (случай крайнего пессимизма).

В случае, когда α=1, то наблюдается «крайний оптимизм» – игрок считает, что риск оправдан и ему максимально повезет.

Критерий Гурвица применяют в случаях, когда наблюдаются различные внешние состояния S_j (т.е. проявляются различные виды угроз для объекта информатизации, о вероятностях появления которых ничего неизвестно), с которыми необходимо считаться; ЛПР может выбирать некоторое количество решений и допускается некоторый риск при выборе стратегии.

Рассмотрим методику применения теории игр для обеспечения информационной безопасности в структурных подразделениях силовых ведомств на примере решения практической задачи по выбору средства эффективной защиты информационных систем от различного рода кибератак, когда ЛПР при выборе оптимальной стратегии будет руководствоваться критериями Вальда и Гурвица.

Для формирования платежной матрицы воспользуемся результатами анализа статистического материала по актуальным киберугрозам за 2022 год и частично за 2023 год [11]. Специалисты в области защиты объектов информатизации утверждают, что в области киберугроз таких, как DoS (Denial of

Service – отказ в обслуживании) и DDoS (Distributed Denial of Service – распределенный отказ в обслуживании) преобладают следующие разновидности с соответствующими вероятностями их проявления: Smurf-ping (31%), ICMP flood (10%), UDP flood (14%), TCP flood (11%), TCP SYN flood (31%) и прочие (3%) [12].

Чаще всего используемые средства защиты объекта информатизации следующие: файрволл (со стандартными настройками) – (1), средства обнаружения вторжения – (2), резервирование канала связи – (3) и их сочетания друг с другом: (1+2), (1+3) или (1+2+3) [13]. Необходимо определить наиболее эффективное средство защиты объекта информатизации от представленных выше киберугроз.

В платежной матрице представлена информация, а точнее, вероятности использования нарушителем-хакером различных видов кибератак (киберугроз) и вероятности их отражения различными средствами защиты объекта информатизации (Рис. 2).

Атаки/Защита	Smurf-ping	ICMP flood	UDP flood	TCP flood	TCP SYN flood
	0,31	0,1	0,14	0,11	0,31
Защиты нет [0]	0	0	0	0	0
Файрвол [1]	0,7	0,8	0,8	0,8	0,6
Ср-ва обн. вторжения [2]	0,9	0,95	0,95	0,99	0,93
Резерв. каналов связи [3]	0,8	0,83	0,8	0,8	0,75
[1]+[2]	0,92	0,97	0,96	0,995	0,95
[1]+[3]	0,9	0,87	0,85	0,9	0,8
[1]+[2]+[3]	0,98	0,995	0,98	0,999	0,98

Рис. 2. Платежная матрица, содержащая вероятности возможных угроз и их отражения средствами защиты объекта информатизации

Для решения поставленной задачи необходимо оценить, хотя бы в условных единицах (у.е.), стоимость средств защиты объекта информатизации от киберугроз. Необходимая информация представлена на Рис. 3.

Атаки/защита	Стоимость средств защиты
Защиты нет [0]	0
Файрвол [1]	1
Ср-ва обн. вторжения [2]	50
Резерв. каналов связи [3]	20
[1]+[2]	51
[1]+[3]	21
[1]+[2]+[3]	71

Рис. 3. Стоимость средств защиты объекта информатизации

Условно будем считать, что в случае не отражения кибератаки, т.е. нарушителю-хакеру удалось обойти средства защиты объекта информатизации, ущерб составит 50 у.е. В платежной матрице («матрице потерь») это обстоятельство учитывается с помощью знака «минус» (Рис. 4).

		Атаки/Защита	Smurf-ping	ICMP flood	UDP flood	TCP flood	TCP SYN flood	MIN
Ущерб:	50	Защиты нет [0]	-15,500	-5,000	-7,000	-5,500	-15,500	-15,500
		Файрвол [1]	-5,650	-2,000	-2,400	-2,100	-7,200	-7,200
		Ср-ва обн. вторжения [2]	-51,550	-50,250	-50,350	-50,055	-51,085	-51,550
		Резерв. каналов связи [3]	-23,100	-20,850	-21,400	-21,100	-23,875	-23,875
		[1]+[2]	-52,240	-51,150	-51,280	-51,028	-51,775	-52,240
		[1]+[3]	-22,550	-21,650	-22,050	-21,550	-24,100	-24,100
		[1]+[2]+[3]	-71,310	-0,025	-0,140	-0,006	-0,310	-71,310
						Критерий Вальда: MAX		-7,2

Рис. 4. Платежная матрица («матрица потерь»), когда возможный ущерб оценивается в 50 у.е.

Анализ результатов потерь, представленных в платежной матрице (матрице «потерь»), на основании критерия Вальда (критерия «максимина») позволяет сделать вывод, что в данном случае оптимальной стратегией для ЛПР является применение файрвола для защиты объекта информатизации.

$$W_{i_{\text{опт}}} = maxmin\omega_{ij} = -7{,}2. \quad (9)$$

Если предположить, что ущерб от проникновения на объект информатизации незначительный и равен 4 у.е., то анализ платежной матрица на основании критерия Вальда (см. рис. 5) позволяет ЛПР выбрать стратегию, которая рекомендует вообще отказаться от какой-либо защиты, поскольку стоимость защиты объекта информатизации выше, чем возможный ущерб от проникновения на объект нарушителя-хакера (10).

$$W_{i_{\text{опт}}} = maxmin\omega_{ij} = -1{,}24. \quad (10)$$

		Атаки/Защита	Smurf-ping	ICMP flood	UDP flood	TCP flood	TCP SYN flood	MIN
Ущерб:	4	Защиты нет [0]	-1,240	-0,400	-0,560	-0,440	-1,240	-1,240
		Файрвол [1]	-1,372	-1,080	-1,112	-1,088	-1,496	-1,496
		Ср-ва обн. вторжения [2]	-50,124	-50,020	-50,028	-50,004	-50,087	-50,124
		Резерв. каналов связи [3]	-20,248	-20,068	-20,112	-20,088	-20,310	-20,310
		[1]+[2]	-51,099	-51,012	-51,022	-51,002	-51,062	-51,099
		[1]+[3]	-21,124	-21,052	-21,084	-21,044	-21,248	-21,248
		[1]+[2]+[3]	-71,025	-0,002	-0,011	0,000	-0,025	-71,025
						Критерий Вальда: MAX		-1,24

Рис. 5. Платежная матрица («матрица потерь»), когда возможный ущерб оценивается в 4 у.е.

В этом проявляется один из принципов обеспечения информационной безопасности объекта информатизации – принцип «разумной достаточности», т.е. стоимость защиты не должна превышать стоимости возможного ущерба от проникновения злоумышленника на объект.

Результаты расчета критерия Гурвица для определения оптимальной стратегии по формуле (8) при различных значениях α-коэффициента (коэффициента степени риска), стоимости возможного ущерба в случае проникновения на объект информатизации нарушителя-хакера и применяемых средствах защиты объекта информатизации представлены на Рис. 6.

	Возможный ущерб, у.е.				
α	5	50	1000	2000	2500
0	-2,05	-9,20	-115,00	-152,70	-155,78
Защита	0	1	1+3	1+2	1+3+2
0,2	-1,74	-7,76	-98,40	-132,58	-140,48
Защита	0	1	1+3	1+2	1+3+2
0,4	-1,43	-6,32	-81,80	-112,46	-120,18
Защита	0	1	1+3	1+2	1+3+2
0,5	-1,28	-5,60	-73,50	-102,40	-108,88
Защита	0	1	1+3	1+2	1+3+2
0,6	-1,12	-4,88	-65,20	-92,34	-97,58
Защита	0	1	1+3	1+2	1+3+2
0,8	-0,81	-3,44	-46,00	-72,00	-74,98
Защита	0	1	1	1+2	1+3+2
1	-0,50	-2,00	-21,00	-41,00	-48,50
Защита	0	1	1	1	1+3

Рис. 6. Платежная матрица («матрица потерь») при различных стратегиях по критерию Гурвица в зависимости от α-коэффициента, вариантов защиты объекта информатизации и величины возможного ущерба.

Анализ платежной матрицы («матрицы потерь») позволяет ЛПР выбрать оптимальную игровую стратегию, которая соответствовала бы возможностям системы защиты объекта информатизации и степени важности защищаемой информации с учетом степени риска.

Необходимо отметить, что в Интернете представлен on-line калькулятор, который значительно упрощает расчеты по соответствующим критериям выбора оптимальной стратегии в теории игр в зависимости от внешних исходных условий [14].

Заключение

Таким образом, применяя теорию матричных игр и руководствуясь различными критериями, например, Вальда или Гурвица (в зависимости от внешних условий игры), можно обеспечить наиболее оптимальный выбор средств защиты объекта информатизации от различного рода кибератак, обеспечив необходимый уровень информационной безопасности в структурных подразделениях силовых ведомств.

Список источников

1. Директива Росгвардии от 28 октября 2021 г. № Д-2 «О приоритетных направлениях деятельности войск национальной гвардии Российской Федерации в 2022 году» // Сайт Росгвардии. URL: https://rosguard.gov.ru/ (дата обращения: 28.09.2023).

2. Воронов С.А., Ушаков М.В., Черных А.К. Перспективы совершенствования профессиональной подготовки военнослужащих и сотрудников к формированию готовности (устойчивости) к информационному воздействию деструктивных сил / Научные труды Северо-Западного управления РАНХиГС, 2022, Т 13, № 2 (54). С. 13-21.

3. Воронов С.А. О формируемых профессиональных компетенций л/с правоохранительных органов в сфере информационного противоборства / Морально-психологическое обеспечение деятельности органов внутренних дел: современные подходы и перспективы развития [Электронный ресурс]: материалы всероссийской научно-практической конференции, 15.12.2021. – СПб.: СПб Университет МВД России, 2021. С. 28-31.

4. Доктрина информационной безопасности Российской Федерации // URL: https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 09.10.2023).

5. Басараб М.А. Теория игр в информационной безопасности: учебно-методическое пособие / М.А. Басараб, Н.С. Коннова. – Москва: МГТУ им. Н.Э. Баумана, 2019. – 80 с. // URL: https://ibooks.ru/bookshelf/374903/reading (дата обращения: 28.09.2023).

6. Викснин И.И., Мариненков Е.Д., Чупров С.С. Применение теории игр для обеспечения безопасности коммуникации киберфизической системы с использованием механизмов репутации и

доверия // Научно-технический вестник информационных технологий, механики и оптики. 2022. Т. 22, № 1. С. 47-59.

7. Alpcan T., Başar T. Network Security: A Decision and Game Theoretic Approach. Cambridge University Press, 2010. // URL: https://dl.acm.org/doi/book/10.5555/1951874 (дата обращения: 28.09.2023).

8. Лаврентьев А.В., Зязин В.П. О применении методов теории игр для решения задач компьютерной безопасности // Безопасность информационных технологий: электрон. науч. журн. 2013. № 3. URL: https://bit.mephi.ru/index.php/bit/article/view/312 (дата обращения: 28.09.2023).

9. Вахний Т.В., Гуц А.К., Новиков Н.Ю. Матрично-игровая программа с выбором критерия для оптимального набора средств защиты компьютерной системы // Математические структуры и моделирование. 2016. № 2 (38). С. 103-115.

10. Вахний Т.В., Гуц А.К., Бондарь С.С. Учет вероятностей хакерских атак в игровом подходе к подбору программных средств защиты компьютерной информации // Математические структуры и моделирование. 2015. № 3 (35). С. 91-105.

11. Актуальные киберугрозы: итоги 2022 года // URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/#id1 (дата обращения: 28.09.2023).

12. Число кибератак на информационные системы России выросло на 65%. URL: https://www.vedomosti.ru/technology/news/2023/03/03/965181-chislo-kiberatak (дата обращения: 28.09.2023).

13. Основные методы и способы защиты информации. URL: https://itsec2012.ru/osnovnye-metody-i-sposoby-zashchity-informacii (дата обращения: 28.09.2023).

14. On-line калькулятор для расчета критериев в теории игр. URL: https://math.semestr.ru/games/horowitz.php (дата обращения: 28.09.2023).

References

1. Rosgvardia Directive No. D-2 of 28 October 2021 "On Priority Areas of Activity of the National Guard Troops of the Russian Federation in 2022" // Rosgvardia website. URL: https://rosguard.gov.ru/ (date of circulation: 28.09.2023).

2. Voronov S.A., Ushakov M.V., Chernykh A.K. Prospects for improving the professional training of servicemen and staff to form readiness (resistance) to the information impact of destructive forces / Scientific Proceedings of the North-West Department of the Russian Academy of National Guard, 2022, Vol. 13, No. 2 (54). C. 13-21.

3. Voronov S.A. About the formed professional competences of l/s of law enforcement agencies in the sphere of information confrontation / Moral-psychological support of activity of bodies of internal affairs: modern approaches and prospects of development [Electronic resource]: materials of the All-Russian scientific-practical conference, 15.12.2021. - St. Petersburg: St. Petersburg University of the Ministry of Internal Affairs of Russia, 2021. C. 28-31.

4. Doctrine of information security of the Russian Federation // URL: https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html (date of reference: 09.10.2023).

5. Basarab, M.A. Game theory in information security: textbook / M.A. Basarab, N.S. Konnova. - Moscow: Bauman Moscow State Technical University, 2019. - 80 c. // URL: https://ibooks.ru/bookshelf/374903/reading (date of reference: 28.09.2023).

6. Viksnin I.I., Marinenkov E.D., Chuprov S.S. Application of game theory to ensure the security of cyber-physical system communication using reputation and trust mechanisms // Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics. 2022. T. 22, № 1. C. 47-59.

7. Alpcan T., Başar T. Network Security: A Decision and Game Theoretic Approach. Cambridge University Press, 2010. // URL: https://dl.acm.org/doi/book/10.5555/1951874 (date of reference: 28.09.2023).

8. Lavrentiev A.V., Zyazin V.P. About application of game theory methods for solving computer security problems // Information technology security: electronic scientific journal. 2013. № 3. URL: https://bit.mephi.ru/index.php/bit/article/view/312 (date of address: 28.09.2023).

9. Vakhniy, T.V.; Guts, A.K.; Novikov, N.Yu. Matrix-game program with criterion selection for the optimal set of computer system protection means // Mathematical Structures and Modelling. 2016. № 2 (38). C. 103-115.

10. Vakhniy, T.V.; Guts, A.K.; Bondar, S.S. Accounting of hacker attack probabilities in the game approach to the selection of software means of computer information protection (in Russian) // Mathematical Structures and Modelling. 2015. № 3 (35). C. 91-105.

11. Current cyber threats: results of 2022 // URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/#id1 (date of address: 28.09.2023).

12. The number of cyber attacks on Russian information systems increased by 65%. URL: https://www.vedomosti.ru/technology/news/2023/03/03/965181-chislo-kiberatak (access date: 28.09.2023).
13. Main methods and ways of information protection. URL: https://itsec2012.ru/osnovnye-metody-i-sposoby-zashchity-informacii (access date: 28.09.2023).
14. On-line calculator for calculating criteria in game theory. URL: https://math.semestr.ru/games/horowitz.php (access date: 28.09.2023).

Информация об авторах
С.А. Воронов - кандидат педагогических наук
А.И. Примакин - доктор технических наук, профессор
Д.Н. Саратов - кандидат технических наук, доцент
Information about the author
S.A. Voronov - Ph.D. of Pedagogic Sciences
A.I. Primakin - Holder of an Advanced Doctorate (Doctor of Science) in Engineering Sciences, full professor
D.N. Saratov - Ph.D. of Engineering Sciences, docent

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.
Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.

Статья поступила в редакцию 26.01.2024; одобрена после рецензирования 05.02.2024; принята к публикации 26.02.2024.
The article was submitted 26.01.2024, approved after reviewing 05.02.2024, accepted for publication 26.02.2024.