(ACS). A prototype of a competitive SDMS was developed and tested. The proposed solution can be implemented using any device that has a browser and the ability to connect to a wireless Wi-Fi network. The developed QMS has no analogues in the market of Kazakhstan. It is shown that a forged approach, unlike the existing ones, takes into account current trends in the total digitalization of business processes in the enterprise. Using minimal resources, enterprises can implement effective ACS in their protection zones of information resources.

Key words: *cybersecurity, access control and management system, software implementation.*

МРНТИ: 50.41.23

Б.Т. Ахметов[1], Д.Т. Курушбаева[2]
[1]Алматинский университет энергетики и связи имени Г. Даукеева
[2]Университет имени Шакарима города Семей

МОДЕЛЬ АДАПТИВНОГО УПРАВЛЕНИЯ ПРАВАМИ ДОСТУПА В СЕТИ

Аннотация: *Описана концептуальная модель адаптивного управления киберзащитой информационно-вычислительной сети (ИВС). Рассмотрен пример решения задачи адаптивного управления правами доступа пользователей с использованием аппарата сетей Петри. Реализована соответствующая модель и выполнено имитационное моделирование в пакетах PIPE v4.3.0 и Petri.Net Simulator. 2.017. Как и любой объект информатизации ИВС требует решения задач по защите информации и кибербезопасности (КрБ). Общей первоначальной задачей при построении эффективных систем защиты и КрБ ИВС ОБИ, остается задача обследования конкретного объекта защиты, формирование моделей потенциального нарушителя (компьютерного злоумышленника – КЗЛ) и киберугроз. По мнению большого числа специалистов, достаточно перспективным представляется возможность описания функциональных моделей различных систем защиты ИВС в терминах теории сети Петри. Реализация вышеуказанных шагов позволит в конечном итоге получить адекватные требования к системам защиты информации (СЗИ) ИВС ОБИ.*

Ключевые слова: *кибербезопасность, защите информации, сеть Петри, киберугроза.*

Введение. Современный уровень применения информационных технологий (ИТ) и систем (ИТС) в экономике достиг высочайшего уровня. При этом, появился новый термин – информационно-вычислительная сеть объекта информатизации (ИВС ОБИ).

В условиях усложнения сценариев кибератак аналитикам служб информационной безопасности (ИБ) необходимо достаточно оперативно реагировать на кибератаки, аномалии угрозы. Это делает актуальной задачу поиска новых способов повышения результативности принятия решений в заданиях реагирования на попытки деструктивного вмешательства со стороны КЗЛ или недобросовестного персонала в работу объектов информатизации, в том числе, ИВС.

Такое представление позволит аналитикам ИБ и ЗИ детализировать киберугрозы в ИВС. Кроме того, в последующем, возможно определение состояний, которые потенциально определяют уязвимости ИВС перед новыми киберугрозами. Также рассматривается перспективность применения данной модели основе сетей Петри (и Петри-Маркова) и раскрашенных сетей Петри в качестве математической и алгоритмической составляющих, проектируемой интеллектуализтрованной системы поддержки принятия решений (ИСППР) в процессе анализа кибеугроз для ИВС.

Основываясь на работах, модели угроз возможно построить, используя достаточно наглядную табличную форму отображения угроз при актуализации вопроса оценки защищенности ИВС. Но как было указанно ранее, данный подход к составлению моделей угроз трудоемок.

Сети Петри (и Петри-Маркова) успешно использовались и для описания моделей нарушителя. Однако, авторы не рассматривали возможность корректировки модели нарушителя (КЗЛ) в ИВС, в частности путем объединения ее с моделями на основе теории графов, что позволило бы более точно описать переходы состояний в процессе вероятного преодоления КЗЛ периметров (рубежей) киберзащиты ИВС.

В работах, также предлагались модели, основанные на сетях Петри и описывающие процессы реализации угроз в информационных системах (ИС). И ходя данные модели

позволяли провести оценку многих параметров защищенности объектов, в частности, вероятности реализации угроз, времени на реализацию угроз, согласованность действий КЗЛ они представляются не до конца завершенными.

Таким образом, синтез новых моделей, а также дополнение существующих моделей и методов адаптивного управления киберзащитой ИВС с использованием возможностей аппарата сетей Петри и учитывая потенциал визуализации сетей Петри, может стать эффективным инструментарием для прогнозирования состояния защищенности для ИВС и других крупных учебных заведений. Это позволит значительно упростить понимание для новых киберугроз и в дальнейшем возможно результативное применение предлагаемых подходов аналитиками служб ЗИ, ИБ и КрБ различных объектов информатизации.

Основной материал статьи

Рассмотрим конкретный пример решения задачи адаптивного управления правами доступа пользователей с использованием аппарата сетей Петри и соответствующего программного обеспечения, которое позволяет автоматизировать корректировку профиля пользователя ИВС, а также с помощью интеграции модуля ИСППР рекомендовать способы нейтрализации киберугроз в ИВС.

Постановку задач управления правами доступа сформулируем так:

1) построить модель разграничения доступа для заданной ИВС;

2) определить управляемые параметры модели;

3) выполнить параметризацию риска нарушения конфиденциальности информации для ИВС.

Формальная математическая постановка задачи по оптимизации схемы разграничения доступа в ИВС.

Исходные данные:

1) Объекты доступа в ИВС – $AO = \{ao_i\}, i = \overline{1, I}$;

2) субъекты доступа в ИВС – $SA = \{sa_j\}, j = \overline{1, J}$;

3) коммуникационные узлы (КУ) в ИВС – $CN = \{cn_k\}, k = \overline{1, K}$;

4) адаптивный механизм, который отвечает позволяет поддерживать метрики безопасности доступа в ИВС на заданном уровне – $AM^0 = \{am^0_{i,j}\}, i = \overline{1, I}, \ j = \overline{1, J}$.

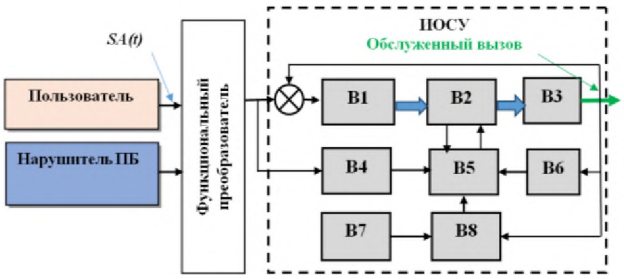

Рисунок 1 – Схема концептуальной модели адаптивного управления киберзащитой ИВС

Принятые обозначения на рисунке 1: В1 – блок информационно-измерительные устройства в ИВС; В2 – блок многоканальных управляющих устройств; В3 – ИВС как объект управления доступом к ресурсам; В4 – блок прогнозирования состояний в ИВС; В5 – блок принятия решений о праве доступа; В6 – блок расчета эффективности по количеству реализованных угроз, связанных с нарушением доступа в ИВС; В7 – блок априорной информации; В8 – блок переменных моделей.

Будем полагать, что приемлемый уровень защиты ИВС достигнут если выполняются условия, описанные в таблице 1.

Условия, при которых достигнут приемлемый уровень защиты ИВС (для задания оптимизации управления доступом на ИВС) рассматривается в последующем в совокупности с данными таблицы 2.

Будем полагать, что целевой функцией является величина вероятных ожидаемых финансовых или иных потерь (ущерба) нанесённых ОБИ, в результате несанкционированного доступа к информационным ресурсам (ИР) ИВС (далее ИР ИВС).

Таблица 1 – Условия, при которых достигнут приемлемый уровень защиты ИВС (*для задания оптимизации управления доступом на ИВС*)

No	Параметр	Условие
1	Адаптивный механизм, который отвечает позволяет поддерживать метрики безопасности доступа в ИВС на заданном уровне.	$am_{i,j} = \begin{cases} 1, \text{ if } am_i \text{ it is placed on} \\ \text{a node } cm_k; \\ 0, \text{ Otherwise.} \end{cases}$
2	Ущерб, от вероятного несанкционированного доступа к ресурсам – $DA^0 = \{da^0_{i,j}\}, i = \overline{1,I},\ j = \overline{1,J}$ [8, 12].	*Смотри примечание.*
3	Структуры вычислительной сети ИВС – $NS = \{ns_{m,n}\}, m,n = \overline{1,K}$	$ns_{m,n} = \begin{cases} 1, \text{ if } (cn_m \in NS_o)\& \\ (cn_n \in NS_o); \\ 0, \text{ Otherwise.} \end{cases}$ *where* NS_o – Network objects.
Управляемые параметры (задаются администратором ЗИ и КрБ)		
1	Признаки общего доступа к ресурсам ИВС – $SV = \{sv_i\}$ [6, 9].	$sv_i = \begin{cases} 1, \text{ if the general access} \\ \text{to a node } sv_i \\ \text{is allowed;} \\ 0, \text{ Otherwise.} \end{cases}$
2	Размещение AO на узлах ИВС – $MP^1 = \left\|mp^1_{i,k}\right\|$	$mp^1_{i,k} = \begin{cases} 1, \text{ if } ao_i \in cn_k; \\ 0, \text{ Otherwise.} \end{cases}$
3	Размещение SA на узлах ИВС – $MP^2 = \left\|mp^2_{j,k}\right\|$.	$mp^2_{j,k} = \begin{cases} 1, \text{ if } sa_j \in cn_k; \\ 0, \text{ Otherwise.} \end{cases}$
Примечание: Ущерб, от вероятного несанкционированного доступа к ресурсам (строка 2) определим степенью информационных ресурсов на узле ИВС, а также профилем пользователя (с учетом характеристик вероятных нарушителей, см. таблицу 2).		

Таблица 2 – Характеристики вероятных нарушителей

Классификация	Характеристика
По мотивам нарушения	Нарушение целостности, конфиденциальности, доступности с корыстной или иной целью.
По уровню информированности и квалификации КЗЛ	Нарушитель (или КЗЛ): 1) высокий уровень знаний; 2) достаточные знания для сбора информации, применение известных эксплойтов и написание собственного программного обеспечения для осуществления кибератаки; 3) КЗЛ не является авторизованным пользователем в ИВС.
По месту действия	Без непосредственного (физического) доступа на территорию ИВС. Нарушитель действует удаленно, например, через сети общего пользования.

Данный параметр определим в рамках статьи как меру расхождения между реальным и рациональным размежеванием доступа пользователей к информационным ресурсам для конкретной ИВС.

$$TF = \sum_{i=1}^{I}\sum_{j=1}^{J} da^0_{i,j} \cdot \left|am_{i,j} - am^0_{i,j}\right|, \quad (1)$$

где $\{am_{i,j}\}$ – элементы множества, которое отображает уже реализованные права доступа.

Постоянная корректировка профиля активного пользователя предполагала применение специального итерационного алгоритма. Данный алгоритм базируется на неявной обратной связи сервера с пользователем ресурсами конкретной ИВС. Ключевым фактором является статистика запросов.

Принято: а) пользователь; б) потенциально опасный пользователь; в) опасный пользователь; г) нарушитель.

Оптимизация настроек процедур управления доступом осуществлялась на основе определения таких параметров:

1) Интенсивность переходов $\lambda_{i,j}(t)$ (определены на основе регрессионных моделей) [14];

2) параметризация риска, который связан с нарушением политики информационной безопасности (рассматривались все свойства: конфиденциальность, целостность и доступность) информации в ИВС.

Была разработана модель адаптивного ролевого управления доступом к ресурсам ИВС (Система управления доступом – СУД). И выполнено имитационное моделирование в пакетах PIPE v4.3.0 (Platform Independent Petri net Editor) и Petri.Net Simulator. 2.017.

На рисунках 2-4 показаны схемы имитационных моделей и формализованные результаты моделирования.

Схемы отображают логическую структуру операционной модели системы правами доступа (для варианта трёхступенчатого управления).

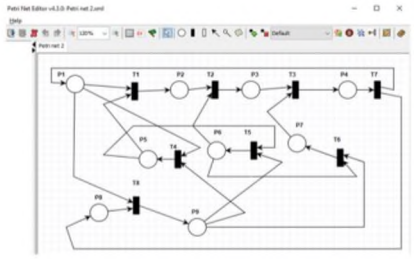

Рисунок 2 – Имитационная модель адаптивного управления доступом в ИВС PIPE v4.3.0 (с учетом регулирования роли абонента)

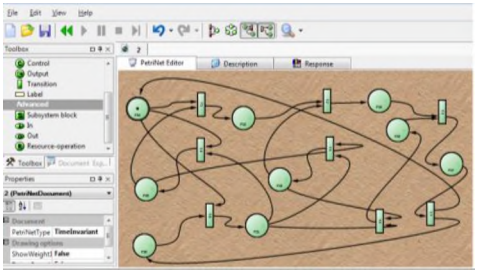

Рисунок 3 – Имитационная модель адаптивного управления доступом в ИВС Petri.Net Simulator. 2.017

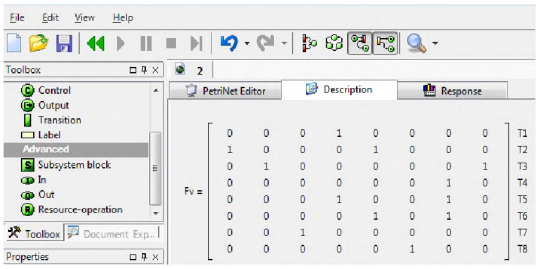

Рисунок 4 – Формализация позиций в модели адаптивного управления доступом в ИВС

Выводы

Описана концептуальная модель адаптивного управления киберзащитой информационно-вычислительной сети (ИВС);

рассмотрен пример решения задачи адаптивного управления правами доступа пользователей с использованием аппарата сетей Петри. Реализована соответствующая модель и выполнено имитационное моделирование в пакетах PIPE v4.3.0 и Petri.Net Simulator. 2.017.

Литература

1. Gupta, Brij, Dharma P. Agrawal, and Shingo Yamaguchi, eds. Handbook of research on modern cryptographic solutions for computer and cyber security. IGI Global, 2016.

2. Liu, X., Zhu, P., Zhang, Y., & Chen, K. (2015). A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure. IEEE Transactions on Smart Grid, 6(5), pp. 2435-2443.
3. Jasiul, B., Szpyrka, M., & Śliwa, J. (2014). Detection and modeling of cyber attacks with Petri nets. Entropy, 16(12), pp. 6602-6623.
4. Liu, X., Zhang, J., & Zhu, P. (2017). Modeling cyber-physical attacks based on probabilistic colored Petri nets and mixed-strategy game theory. International Journal of Critical Infrastructure Protection, 16, pp. 13-25.
5. Jasiul, B., Szpyrka, M., & Śliwa, J. (2015). Formal specification of malware models in the form of colored Petri nets. In Computer Science and its Applications (pp. 475-482). Springer, Berlin, Heidelberg.
6. Akhmetov, B., Lakhno, V., Boiko, Y., & Mishchenko, A. (2017). Designing a decision support system for the weakly formalized problems in the provision of cybersecurity. Eastern-European Journal of Eenterprise Technologies, (1(2)), pp. 4-15.
7. Arendt, D. L., Burtner, R., Best, D. M., Bos, N. D., Gersh, J. R., Piatko, C. D., & Paul, C. L. (2015, October). Ocelot: user-centered design of a decision support visualization for network quarantine. In Visualization for Cyber Security (VizSec), 2015 IEEE Symposium on (pp. 1-8).
8. Alheeti, K. M. A., Gruebler, A., McDonald-Maier, K. D., & Fernando, A. (2016, January). Prediction of DoS attacks in external communication for self-driving vehicles using a fuzzy petri net model. In Consumer Electronics (ICCE), 2016 IEEE International Conference on (pp. 502-503).
9. de Carvalho, M. A., & Bandiera-Paiva, P. (2017, October). Evaluating ISO 14441 privacy requirements on role based access control (RBAC) restrict mode via Colored Petri Nets (CPN) modeling. In Security Technology (ICCST), 2017 International Carnahan Conference on (pp. 1-8).
10. Appel, M., Konigorski, U., & Walther, M. (2018). A Graph Metric for Model Predictive Control of Petri Nets. IFAC-PapersOnLine, 51(2), pp. 254-259.
11. Gao, Z., Zhao, C., Shang, C., & Tan, C. (2017, October). The optimal control of mine drainage systems based on hybrid Petri nets. In Chinese Automation Congress (CAC), 2017 (pp. 78-83).

ӘДІСТЕМЕЛІК ЖЕЛІЛЕРДІ ҚОЛДАНУДЫ БАСҚАРУ МОДЕЛІ

Б.Т. Ахметов, Д.Т. Курушбаева

Кибер-қорғалған ақпараттық-компьютерлік желіні (IVS) адаптивті басқарудың тұжырымдамалық моделі сипатталған. Петри торларының аппаратын қолдана отырып, пайдаланушылардың қол жеткізу құқығын адаптивті басқару мәселесін шешудің мысалы қарастырылған. Сәйкес үлгі енгізіліп, PIPE v4.3.0 және Petri.Net Simulator пакеттерінде модельдеу жүргізілді. 2.017. Ақпараттандырудың кез-келген нысаны сияқты, АТТ ақпаратты қорғау және киберқауіпсіздік (CRL) мәселелерін шешуді талап етеді. ОВІ IVS типті қауіпсіздік жүйелері мен CIRT құрудағы жалпы бастапқы міндет қорғаныштың нақты объектісін зерттеу, ықтимал зиянкестердің (компьютерлік шабуылдаушы – KZL) және киберқауіптердің модельдерін құру міндеті болып қала береді. Көптеген мамандардың пікірінше, уақытша ұстау изоляторларының әртүрлі қауіпсіздік жүйелерінің функционалды модельдерін Петри нет теориясы тұрғысынан сипаттау мүмкіндігі перспективалы болып көрінеді. Жоғарыда аталған қадамдарды орындау ақырында ақпараттық қауіпсіздік жүйелеріне (SZI) IVS ОВІ сәйкес талаптарды қамтамасыз етеді.

Түйін сөздер: *киберқауіпсіздік, ақпараттық қауіпсіздік, Petri net, киберқауіпсіздік.*

ADAPTIVE NETWORK ACCESS MANAGEMENT MODEL

B. Akhmetov, D. Kurushbaeva

The conceptual model of adaptive control of a cyber-protected information-computer network (IVS) is described. An example of solving the problem of adaptive management of user access rights using the apparatus of Petri nets is considered. The corresponding model was implemented and simulation was performed in the PIPE v4.3.0 and Petri.Net Simulator packages. 2.017. Like any object of informatization, an ITT requires solving problems of protecting information and cybersecurity (CRL). The general initial task in constructing effective security systems and CIRTs of the OBI IVS remains the task of examining a specific object of protection, forming models of a potential intruder (computer attacker – KZL) and cyber threats. In the opinion of a large number of specialists, the possibility of describing functional models of various security systems of temporary detention facilities in terms of Petri net theory seems quite promising. The implementation of the above steps will ultimately provide adequate requirements for information security systems (SZI) IVS OBI.

Key words: *cybersecurity, information security, Petri net, cyberthreat.*