Ахметов Б.С., Кыдыралина Л.М. Модель на основе сети Петри для разграничения полномочий пользователей в сети информационно-образовательной среды университета. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей XVIII Междунар. научно-техн. конф. – Пенза: ПДЗ, 2018. – С. 81-84.

УДК 004.056.53

МОДЕЛЬ НА ОСНОВЕ СЕТИ ПЕТРИ ДЛЯ РАЗГРАНИЧЕНИЯ ПОЛНОМОЧИЙ ПОЛЬЗОВАТЕЛЕЙ В СЕТИ ИНФОРМАЦИОННО–ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ УНИВЕРСИТЕТА

Б.С. Ахметов, Л.М. Кыдыралина

MODEL BASED ON PETER‘S NETWORK FOR THE LIMITATION OF THE AUTHORITY OF USERS IN THE NETWORK OF THE INFORMATION AND EDUCATIONAL ENVIRONMENT OF THE UNIVERSITY

B.S. Akhmetov, L.M. Kydyralina

Аннотация. В связи с переходом большинства учебных заведений, и прежде всего крупных университетов, на информационные платформы обучения и системы электронного документооборота возникает задача усиления киберзащищенности информационно-образовательной среды учебного заведения (ИОСУЗ) от несанкционированного доступа к информационным ресурсам. В докладе рассмотрена модель на основе сети Петри для разграничения полномочий пользователей в сети информационно-обра-зовательной среды университета.

Ключевые слова: кибербезопасность, информационно-образова-тельная среда университета, моделирование, сети Петри.

Abstract. In connection with the transition of most educational institutions, first of all large universities, to information training platforms and electronic document management systems, the task arises to strengthen the cybersecurity of the information and educational environment of the educational institution (IEEEI) from unauthorized access to information resources. The report considers a model based on the Petri net for delineating the powers of users in the network of the information and educational environment of the university.

Keywords: cybersecurity, information-educational environment of the university, modeling, Peter’s nets.

Сегодня ИОСУЗ – это многоуровневая иерархическая система, в которой сталкиваются интересы и данные различных пользователей. С точки зрения администраторов информационной безопасности и защиты информации, классическое понятие периметра защиты ИОСУЗ выглядит достаточно размытым. Это, прежде всего, связано с постоянно возрастающим количеством и типом новых устройств, подключаемых к сети ИОСУЗ. В результате анализа моделей систем защиты информации (СЗИ), в частности для ИОСУЗ [1–5], можно сделать вывод о целесообразности применения аппарата вероятностных сетей Петри для оценки защищенности ИОСУЗ от деструктивных вмешательств со стороны компьютерных злоумышленников (КЗЛ). На этапе нахождения вероятностных параметров реализации конкретной киберугрозы (нарушение разграничения полномочий) для ИОСУЗ, будем полагать, что смоделирована работа всех СЗИ. И кроме того выполнен расчет вероятностных параметров смены разметок в соответствующих вероятностных сетях Петри (ВСП) или сетях Петри-Маркова (СПМ) [6]. Реализация угрозы в ИОСУЗ – это порядок передвижений (полушагов) по ВСП или СПМ. Будем полагать, что ВСП или СПМ пребывают в каждом состоянии некоторое случайный отрезок вре-

мени. Рассматриваемому временному отрезку также ставим в соответствие параметр, задающий соответственно величину плотности распределения вероятности. Далее, анализируем передвижения по траекториям ВСП или СПМ за полушаги. А затем проверяем логические условия переключения ВСП или СПМ в следующее состояние. Постоянство состояний ВСП или СПМ определит траекторию исследуемого процесса для рассматриваемой киберугрозы. Аналитически описать процесс можно, применив интегро-дифференциальные уравнения для траекторий передвижений из начальных состояний в конечные [6].

Рассмотрим пример: пусть $h(tr:1(a) \to j(a) = h(tr_1)$ – номер траектории передвижения из состояния $a_{1(a)}$ (индекс с буквой означает номер состояния) в состояние $a_{j(a)}$. Траектория включает в себя серию полушагов. Или из состояния в переход, а затем из перехода в состояние и т.д.:

$$S_{1[h(tr)]}, S_{2[h(tr)]}, \ldots, S_{i[h(tr)]}, \ldots, S_{j[h(tr)]},$$

где i, j – индексы, которые соответствуют номеру состояния (или номеру перехода). Количество траекторий описано величиной $H(tr)$. Тогда величины, задающие вероятность и плотность распределения времени выполнения соответствующего полушага, соответственно $P_{j(a)j(z)}$ и $f_{j(a)j(z)}$. Вероятность и плотность распределения времени передвижения из $a_{1(a)}$ в $a_{j(a)}$ по $h(tr_{1j})$ находим так [6]:

$$P_{h(tr_{1j})} = \prod_{j[h(tr_{1j})]=1}^{J[h(tr_{1j})]} P_{j[h(tr_{1j})]};$$

$$f_{h(tr_{1j})} = f_{1[h(tr_{1j})]} * f_{2[h(tr_{1j})]} * \ldots * f_{i[h(tr_{1j})]} * \ldots * f_{J[h(tr_{1j})]},$$

где $J[h(tr_{1j})]$ – количество позиций и переходов в $h(tr_{1j})$; $*$ – обозначение операции свертки $a_{1(a)}$ по всем возможным $h(tr_{1j})$ из соотношений:

$$P_{1(a)j(a)} = \prod_{h(tr_{1j})=1}^{H(tr_{1j})} P_{h(tr_{1j})}; \tag{1}$$

$$f_{1(a)j(a)} = \frac{\prod_{h(tr_{1j})=1}^{H(tr_{1j})} P_{h(tr_{1j})} \cdot f_{h(tr_{1j})}}{\prod_{h(tr_{1j})=1}^{H(tr_{1j})} P_{h(tr_{1j})}}. \tag{2}$$

В соответствии с [6] можно найти вероятности $\Phi_{i,j(t)}$ реализации анализируемой киберугрозы.

В настоящее время исследования продолжается, в частности, в направлении разработки прикладного программного обеспечения для моделирования вероятностных параметров реализации конкретной киберугрозы для ИОСУЗ.

Библиографический список

1. Rezgui, Y. Information security awareness in higher education: An exploratory study [Text] / Y.Rezgui, M. Adam // Computers & Security 27.7 2010. P. 241-253.

2. Sultan, N. Cloud computing for education: A new dawn? [Text] / N.Sultan // International Journal of Information Management 30.2. pp. 109–116.

3. Ахметов Б.С., Яворский В.В. Моделирование информационной образовательной среды вуза. Караганда: КарГТУ, 2006. С. 251.

4. Schneider, F. Cybersecurity education in universities // IEEE Security & Privacy 11.4 2013. Pp. 3–4.

5. Schuett, M. Information Security Synthesis in Online Universities [Text] / M.Schuett, M. Rahman // arXiv preprint arXiv:1111.1771- 2011.

6. Petrov O., Borowik B., Karpinskyy M., Korchenko O., Lakhno V. Immune and defensive corporate systems with intellectual identification of threats [Text] // Pszczyna:ŚląskaOficynaDrukarska, pp.222. ISBN: 978-83-62674-68-8, 2016.

Ахметов Бахытжан Сражатдинович
Казахский национальный
педагогический университет
имени Абая,
г. Алматы, Казахстан
E-mail: bakhytzhan.akhmetov.54@mail.ru

Akhmetov B.S.
Kazakh National Pedagogical
University named after Abay,
Almaty, Kazakhstan

Кыдыралина Лазат Муктаровна
Казахский национальный
педагогический университет
имени Абая,
г. Алматы, Казахстан
E-mail: Lazat_75@mail.ru

Kydyralina L.M.
Kazakh National Pedagogical
University named after Abay,
Almaty, Kazakhstan