СБОРНИК **НАУЧНЫХ ТРУДОВ НГТУ. – 2020. – № 1–2 (97).** – 26–39

УДК 004.891.1.3 DOI: 10.17212/2307-6879-2020-1-2-26-39

ИССЛЕДОВАНИЕ АНОМАЛЬНЫХ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЯ В ИНФОРМАЦИОННОЙ СРЕДЕ*

Н.Е. КАРПОВА[1], А.С. БАРАНОВ[2], А.А. ЕМЕЛИНА[3], А.Е. КОНОВАЛОВ[4]

[1] *443001, РФ, г. Самара, ул. Молодогвардейская, 244, Самарский государственный технический университет, кандидат технических наук, доцент кафедры «Электронные системы и информационная безопасность». E-mail: esib@samgtu.ru*
[2] *443029, РФ, г. Самара, ул. Солнечная, 53, монтажник ООО «НИЦ "ФОРС"». E-mail: as_baranov@bk.ru*
[3] *443001, РФ, г. Самара, ул. Молодогвардейская, 244, Самарский государственный технический университет, лаборант кафедры «Электронные системы и информационная безопасность». E-mail: alina.lina0723@gmail.ru*
[4] *443099, РФ, г. Самара, ул. Молодогвардейская, 54/59, специалист по защите информации ГБУЗ СО «Самарская стоматологическая поликлиника № 1». E-mail: sahsa199920@mail.ru*

Статья посвящена анализу действий пользователя в компьютерной системе и разработке системы мониторинга аномальных действий пользователя в информационной среде. Для разработки системы был использован математический аппарат нечеткой логики. Основными достоинствами систем мониторинга информационной среды, основанных на теории нечетких множеств, является возможность представлять произвольные значения параметров в виде аналитики заданных величин, возможность учитывать большее количество сценариев развития, возможность использовать данную систему при принятии решений и описании схем анализа потоков информационной среды, а также отслеживать большое количество компьютерных параметров. В ходе исследования было выявлено, что действия злоумышленников отличаются от поведения обычных пользователей. В результате авторы предлагают разработанную систему мониторинга аномальных действий пользователя в информационной среде, которая основана на анализе журналов событий. Работа системы требует накопления информации (файлы аудита, данные о времени входа и продолжительности сессии, данные об удалении файлов и т. д.), на основе которой создается эталон (шаблон) нормального поведения пользователя. В дальнейшем происходит сравнение поведения пользователя с эталоном, и при выявлении аномалий система сигнализирует об отклонениях. Данный алгоритм позволяет отследить большое количество параметров пользователя для определения несанкционированного доступа (НСД).

* Статья получена 26 мая 2020 г.

Ключевые слова: защита информационных систем, поведенческий анализ, нечеткие множества, угрозы, системы мониторинга, аудит, несанкционированный доступ, журналы событий, эталон поведения пользователя

ВВЕДЕНИЕ

Большинство преступлений, связанных с информацией, совершают сотрудники организаций. Особенно важным и актуальным вопросом является мониторинг действий пользователя в информационной среде. Это подтверждает и опрос [10], согласно которому 90 % организаций чувствуют уязвимость перед внутренними угрозами. В качестве механизмов проверки подлинности сотрудников целесообразно разработать средства идентификации пользователей корпоративной системы, применяя методики поведенческого анализа. В ряде научных работ [1, 2, 4, 5, 7] описываются основные методы мониторинга поведения пользователя в сети. Также существуют системы [3, 6, 8, 9], основанные на нейронных сетях, однако на сегодняшний день такие системы имеют очень ограниченный круг пользователей.

В настоящей работе предлагается применение аппарата нечеткой логики для разработки системы мониторинга аномальных действий пользователя в информационной среде.

1. ИССЛЕДОВАНИЕ

В рамках исследования был проведен анализ шести параметров информационной системы: вероятность использования папок, продолжительность сеанса, время входа в сеть и выхода из нее, создание файлов, часто используемые программы, удаление файлов. Данные параметры позволяют осуществлять комплексный мониторинг действий пользователя и своевременно реагировать на аномальные действия в системе, связанные с НСД. Были проанализированы журналы событий за один месяц для 50 учебных компьютеров, расположенных в аудиториях института. Основными пользователями компьютеров являлись студенты учебного заведения.

Было выявлено 13 основных путей перемещения пользователя в системе, а также вероятности прохождения по этим путям. Вероятность (μ) нормального / аномального поведения вычислялась по следующей формуле:

$$\mu = \frac{N}{M}, \qquad (1)$$

где M – общее количество папок, а N – частота посещения конкретных папок. Данные сведения представлены в табл. 1. Для упрощения зададим каждый путь через переменную x_i – порядковый номер пути посещения конкретных папок.

Таблица 1

Перечень основных путей

x_i	μ	Путь
x_1	0,2	"C:\Windows\Logs"
x_2	0,2	"C:\Windows\System32"
x_3	0,3	"C:\Windows\"
x_4	0,3	"C:\Program Files"
x_5	0,6	"C:\Users\1\Documents\Загрузки\"
x_6	0,6	"C:\Documents and Settings\student\Рабочийстол"
x_7	0,6	"C:\Documents and Settings\student\Моидокументы"
x_8	0,7	"C:\Users\1\Documents\"
x_9	0,7	"C:\Documents and Settings\student\"
x_{10}	0,8	"C:\Users\1\"
x_{11}	0,9	"C:\Users\"
x_{12}	0,9	"C:\Documents andSettings\"
x_{13}	1	"C:\ "

Проанализировав таблицу, можно сделать вывод о том, что аномальным поведением пользователя является посещение системных папок, а также папок, не соответствующих учебным задачам, что соответствует условию $\mu \leq 0{,}4$.

Построим функцию и график нечеткого множества, который изображен на рис. 1.

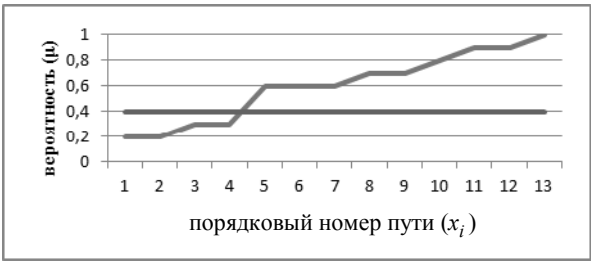

Рис. 1. Графическое представление нечеткого множества функции доступа пользователя к папкам и файлам

$$\mu(x) = \begin{cases} x_1,\ 0,2; \\ x_2,\ 0,2; \\ x_3,\ 0,3; \\ x_4,\ 0,3; \\ x_5,\ 0,6; \\ x_6,\ 0,6; \\ x_7,\ 0,6; \\ x_8,\ 0,7; \\ x_9,\ 0,7; \\ x_{10},\ 0,8; \\ x_{11},\ 0,9; \\ x_{12},\ 0,9; \\ x_{13},\ 1. \end{cases} \quad (2)$$

Следующим признаком является время входа в систему и выхода из нее. Данные промежутки были выбраны исходя из длительности пар и рабочего времени. Самая большая вероятность входа в систему – это первая половина дня. Также мы учитываем обеденное время. Во второй половине дня проходят занятия, однако их меньше, а следовательно, и вероятность работы в системе меньше. В 18:40 заканчивается последняя пара, соответственно после этого времени не должно наблюдаться действий по входу в систему и выходу из нее. В данном параметре системы необходимо сверяться с календарем и определять, будний это день или выходной. В 19:00 система в автоматическом режиме будет блокировать включенные компьютеры.

Временные интервалы представлены в табл. 2. Для упрощения зададим каждый временной интервал через переменную t_i.

Таблица 2

Время входа в систему и выхода из нее

(μ)	Время (мин)
0,8	07.55...13.15 (t_1)
0,4	13.15...13.30 (t_2)
0,8	13.30...15.20 (t_3)
0,6	15.20...18.40 (t_4)
0,2	18.40...07.55 (t_5)

Построим функцию (3) и график нечеткого множества, который изображен на рис. 2.

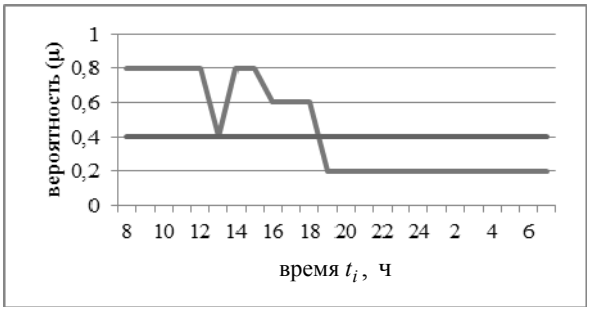

Рис. 2. Графическое представление нечеткого множества функции времени входа в систему и выхода из нее

$$\mu(x) = \begin{cases} t_1,\ 0,8; \\ t_2,\ 0,4; \\ t_3,\ 0,8; \\ t_4,\ 0,6; \\ t_5,\ 0,2. \end{cases} \qquad (3)$$

Поведение, определяемое вероятностью ниже 40 %, можно считать аномальным. Здесь мы можем наблюдать 2 варианта аномального поведения: 1) время работы в обеденное время (t_2) и 2) время сеанса в нерабочее время университета.

Аналогично был произведен анализ следующих четырех параметров, покажем их функции принадлежности и графическое представление.

Третьим параметром является продолжительность работы компьютера.

Приведем функцию (4) и график нечеткого множества (рис. 3).

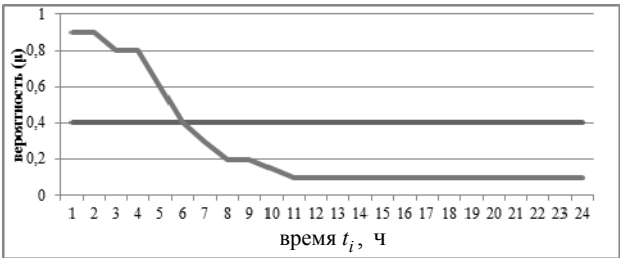

Рис. 3. Графическое представление нечеткого множества функции продолжительности работы компьютера

$$\mu(x) = \begin{cases} t_1,\ 0,9; \\ t_2,\ 0,8; \\ t_3,\ 0,5; \\ t_4,\ 0,4; \\ t_5,\ 0,3; \\ t_6,\ 0,2; \\ t_7,\ 0,15; \\ t_8,\ 0,1. \end{cases} \quad (4)$$

Рассмотрим четвертый параметр, связанный с созданием файлов.

Приведем функцию (5) и график нечеткого множества (рис. 4).

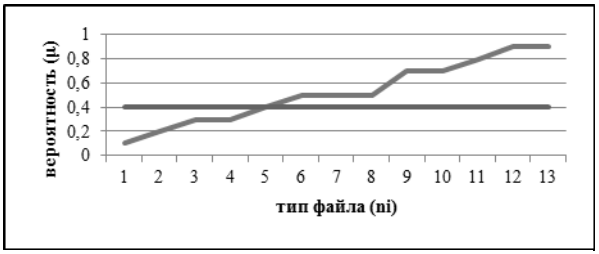

Рис. 4. Графическое представление нечеткого множества функции создания файлов

$$\mu(x) = \begin{cases} n_1,\ 0,1; \\ n_2,\ 0,2; \\ n_3,\ 0,3; \\ n_4,\ 0,3; \\ n_5,\ 0,5; \\ n_6,\ 0,5; \\ n_7,\ 0,5; \\ n_8,\ 0,7; \\ n_9,\ 0,7; \\ n_{10},\ 0,7; \\ n_{11},\ 0,9; \\ n_{12},\ 0,9. \end{cases} \quad (5)$$

Рассмотрим пятый параметр, связанный с часто используемыми программами.

Приведем функцию (6) и график нечеткого множества (рис. 5).

Рис. 5. Графическое представление нечеткого множества функции часто используемых программ

$$\mu(x) = \begin{cases} x_1,\ 0,1; \\ x_2,\ 0,2; \\ x_3,\ 0,3; \\ x_4,\ 0,3; \\ x_5,\ 0,5; \\ x_6,\ 0,5; \\ x_7,\ 0,8; \\ x_8,\ 0,9. \end{cases} \quad (6)$$

Рассмотрим шестой параметр, связанный с удалением файлов.

Приведем функцию (7) и график нечеткого множества (рис. 6).

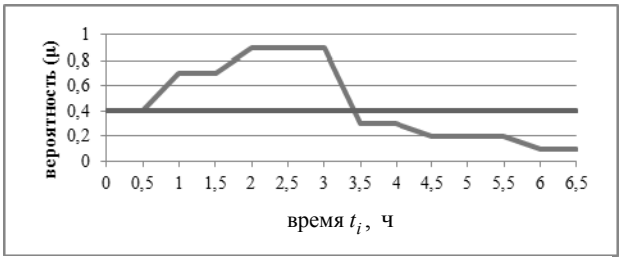

Рис. 6. Графическое представление нечеткого множества функции удаления программы

$$\mu(x) = \begin{cases} x_1,\ 0,4; \\ x_2,\ 0,7; \\ x_3,\ 0,9; \\ x_4,\ 0,3; \\ x_5,\ 0,2; \\ x_6,\ 0,1. \end{cases} \quad (7)$$

На основе проведенного анализа был составлен эталон пользователя информационной среды.

Эталон:

– студент, заходящий в информационную среду только во время пар с продолжительностью работы в системе не более 4,5 часа;

– студент, использующий в своей работе только учебные программы: Visual Studio, IDA Pro, IP Video System designTool, Microsoft Office, NanoCad, Multisim;

– студент, создающий следующие виды файлов: текстовые, графические, .dwg, .jvsg, .mc8;

– студент, удаляющий только те файлы, которые сам создал.

2. СТРУКТУРНАЯ СХЕМА

На основе данных, полученных в проведенном исследовании, была разработана система анализа аномальных действий пользователя в информационной среде. Структурная схема разработки приведена на рис. 7. Работа системы требует накопления данных, на базе которых создается эталон нормального поведения пользователя. Затем в системе происходит сравнение поведения пользователя с эталоном и при выявлении аномалий система сигнализирует об отклонениях.

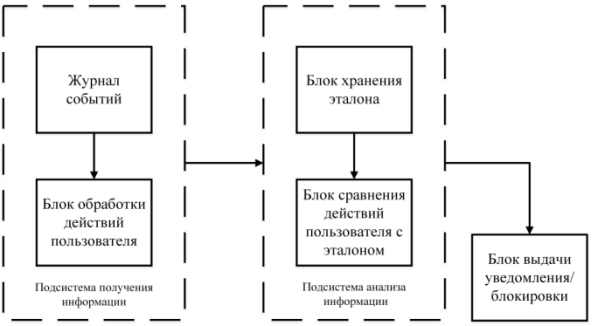

Рис. 7. Структурная схема системы анализа действий пользователя в информационной среде

3. АЛГОРИТМ

Самый первый параметр, который должна проверять программа, – это день входа в сеть. Следующим параметром, который должна отслеживать система, является время входа в сеть. Третьим параметром система должна проверить используемую программу и, если использование данной программы относится к эталонному поведению пользователя, то проверять путь нет необходимости, параметр «вероятность использования папок» в алгоритме пропускается. Если же использование какой-либо программы определяется как аномальное, то необходимо заблокировать пользователя. Так как результатом использования многих программ является создание различного рода файлов, то четвертым параметром, который должна проверять система, является создание файлов. Если информация о данном расширении отсутствует, следующим шагом необходимо выполнить проверку вероятности посещения папки. Пятым параметром, который отслеживает система, является время удаления документов от момента их создания. Затем проверяется параметр длительности нахождения за компьютером. Далее контролируется текущее время.

Если оно выходит за пределы 19:00, то должна произойти автоматическая блокировка. Если нет превышения по времени, то системе необходимо заново пройти весь алгоритм.

На основе разработанной системы и проведенных исследований нами был составлен алгоритм, приведенный на рис. 8.

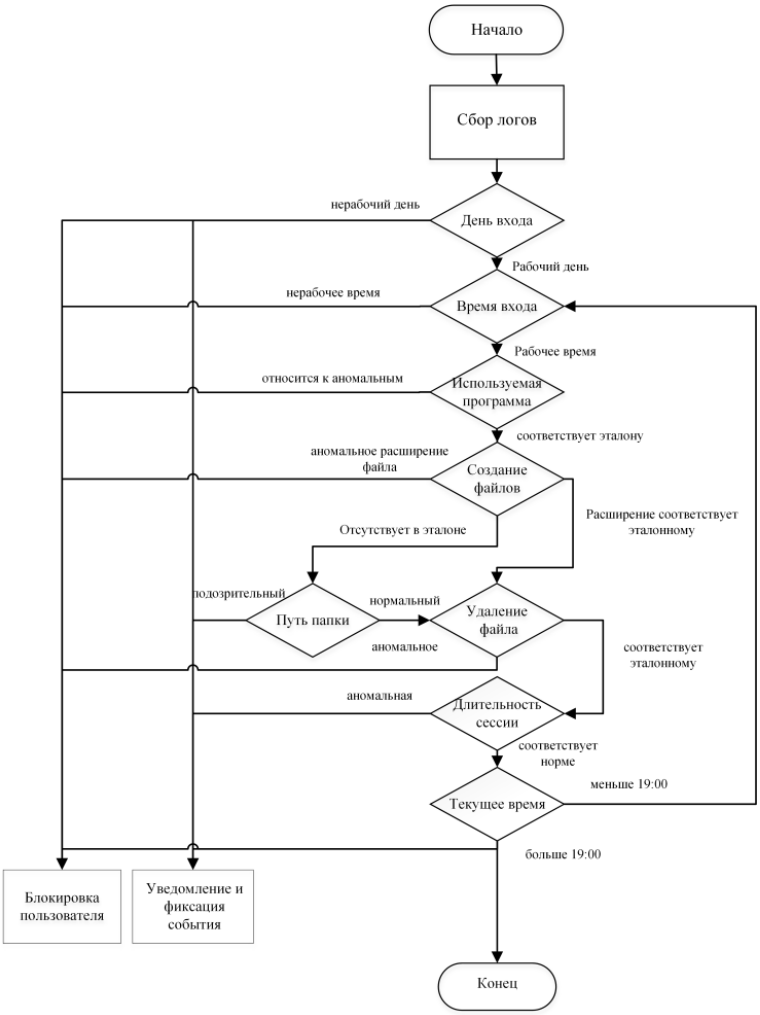

Рис. 8. Алгоритм распознавания аномального действия пользователя

ЗАКЛЮЧЕНИЕ

Авторы настоящей статьи разработали систему анализа аномальных действий пользователя в информационной среде Института автоматики и информационных технологий Самарского государственного технического университета, на основе исследования был создан алгоритм системы мониторинга действий пользователя в компьютерной системе с использованием аппарата нечеткой логики. Система мониторинга разработана на языке C#. Программа была протестирована в учебных аудиториях института.

Система показала себя как стабильно функционирующая, устойчивая. Она четко соблюдает алгоритм и отправляет уведомления, а также блокирует пользователя в случае отклонений от эталонного поведения. На основе проведенных исследований в будущем планируется разработка и обучение нейронной сети по выявлению аномального поведения пользователей в информационных системах, а также возможность внедрения данной нейронной сети в другие корпоративные структуры.

СПИСОК ЛИТЕРАТУРЫ

1. *Аверкин А.Н.* Нечеткие поведенческие модели принятия решений с учетом иррациональности поведения человека // Научные труды Вольного экономического общества России. – 2014. – Т. 186. – С. 153–158.

2. *Баев А.В. Гаценко О.Ю. Самонов А.В.* Программный комплекс управления доступом USB-устройств к автоматизированным рабочим местам // Вопросы кибербезопасности. – 2020. – № 1 (35). – С. 52–61. – URL: http://cyberrus.com/wp-content/uploads/2020/03/52-61-135-20_6.-Baev.pdf (дата обращения: 04.07.2020).

3. *Зуев В.Н., Ефимов А.Ю.* Нейросетевой поведенческий анализ действий пользователя в целях обнаружения вторжений уровня узла // Программные продукты и системы. – 2019. – Т. 32, № 2. – С. 258–262.

4. *Корченко А.Г.* Построение систем защиты информации на нечетких множествах. – Киев: МК-Пресс, 2006. – 320 с.

5. *Лыдин С.* Обзор DATAPK – комплекса оперативного мониторинга и контроля защищенности АСУ ТП // AntiMalware: web-сайт. – 2020. – 15 мая. – URL: https://www.anti-malware.ru/reviews/PAK-DATAPK/ (дата обращения: 04.07.2020).

6. Идентификация пользователей корпоративной системы с помощью поведенческого анализа с использованием модели искусственной нейронной

сети / В.М. Савинова, А.А. Бесхмельницкий, Е.С. Бабина, А.Д. Осадчая // Транспортное дело России. – 2017. – № 5. – С. 65–68.

7. *Савинов А.Н.* Методы, модели и алгоритмы распознавания клавиатурного почерка в ключевых системах: дис. ... канд. техн. наук. – Йошкар-Ола, 2013. – 97 с.

8. Neural networks for systems security / C.M. Lozano, F. Lopez, J. Lopez, L. Pino, G. Ramos // Proceedings of 5th European Congress on Intelligent Techniques and Soft Computing. – Aachen, Germany, 1997. – Vol. 1. – P. 410–414.

9. *Obaidat M.S., Macchairolo D.T.* A multilayer neural network system for computer access security // IEEE Transactions on Systems, Man, and Cybernetics. – 1994. – Vol. 24, N 5. – P. 806–813.

10. *Seals T.* Fear of insider threats hits an all-time high // Infosecurity Magazine. – 2017. – 14 November. – URL: https://www.infosecurity-magazine.com/news/fear-of-insider-threats-hits-an/ (accessed: 04.07.2020).

Карпова Надежда Евгеньевна, кандидат технических наук, доцент кафедры «Электронные системы и информационная безопасность» Самарского государственного технического университета. Основные направления научных исследований – автоматизированные интеллектуальные системы и автоматизированные информационно-измерительные системы. Имеет более 100 публикаций. E-mail: esib@samgtu.ru

Баранов Александр Сергеевич, монтажник ООО «НИЦ “ФОРС”». E-mail: as_baranov@bk.ru

Емелина Алина Анатольевна, лаборант кафедры «Электронные системы и информационная безопасность». E-mail: alina.lina0723@gmail.ru

Коновалов Александр Евгеньевич, специалист по защите информации ГБУЗ СО «Самарская стоматологическая поликлиника № 1». E-mail: sasha199920@mail.ru

DOI: 10.17212/2307-6879-2020-1-2-26-39

Research of abnormal user actions in the information environment*

N.E. Karpova[1], A.S. Baranov[2], A.A. Emelina[3], A.E. Konovalov[4]

[1] *Samara State Technical University, 244 Molodogvardeyskaya Street, Samara, 443100, Russian Federation, candidate of technical sciences, associate professor of the electronic systems and information security department. E-mail: esib@samgtu.ru*
[2] *Samara State Technical University, 53 Solnechnaya Street, Samara, 443029, Russian Federation, installer OOO «NITS "FORS"». E-mail: as_baranov@bk.ru*
[3] *Samara State Technical University, 244 Molodogvardeyskaya Street, Samara, 443100, Russian Federation, laboratory assistant of the electronic systems and information security department. E-mail: alina.lina0723@gmail.ru*
[4] *Samara State Technical University, 54/59 Molodogvardeyskaya Street, Samara, 443099, Russian Federation, Information protection specialist, Samara City Dental Clinic № 1. E-mail: sahsa199920@mail.ru*

The article is devoted to the analysis of user actions in a computer system and the development of a system for monitoring abnormal user actions in the information environment. We used the mathematical apparatus of fuzzy logic for system development. The main advantages of information environment monitoring systems based on fuzzy set theory are the ability to represent arbitrary parameter values in the form of analytics of given values, the ability to take more development scenarios into account, the ability to use this system when making decisions, when describing flow analysis schemes for the information environment, and track a large number of computer parameters. During the research, it was found that the actions of hackers differ from the behavior of ordinary users. As a result, the authors propose a developed system for monitoring abnormal user actions in the information environment, which is based on the analysis of event logs. The operation of the system requires the accumulation of information (audit files, log-in time and session duration data on file deletion, etc.), based on which a standard (template) of normal user behavior is created. Then, the user's behavior is compared with the standard, and when anomalies are detected, the system signals about deviations. This algorithm allows you to track a large number of user parameters to determine unauthorized access.

Keywords: protection of information systems, behavioral analysis, fuzzy sets, threats, monitoring system, audit, unauthorized access, event logs, user behavior standard

REFERENCES

1. Averkin A.N. Nechetkie povedencheskie modeli prinyatiya reshenii c uchetom irratsional'nosti povedeniya cheloveka [Fuzzy behavioral decision-making modelbased on human irrational behavior]. *Nauchnye trudy Vol'nogo ekonomich-*

* *Received 26 May 2020.*

eskogo obshchestva Rossii = Scientific works of the Free Economic Society of Russia, 2014, vol. 186, pp. 153–158.

2. Baev A.V. Gacenko O.Yu. Samonov A.V. Programmnyi kompleks upravleniya dostupom USB-ustroistv k avtomatizirovannym rabochim mestam [The software complex access control USB devices to automated workstations]. *Voprosy kiberbezopasnosti = Cybersecurity Issues*, 2020, no. 1 (35), pp. 52–61. Available at: http://cyberrus.com/wp-content/uploads/2020/03/52-61-135-20_6.-Baev.pdf (accessed 04.07.2020).

3. Zuev V.N., Efimov A.Yu. Neirosetevoi povedencheskii analiz deistvii pol'zovatelya v tselyakh obnaruzheniya vtorzhenii urovnya uzla [Neural network user behavior analysis for detecting host-level intrusion]. *Programmnye produkty i sistemy = Software and Systems*, 2019, vol. 32, no. 2, pp. 258–262.

4. Korchenko A.G. *Postroenie sistem zashchity informatsii na nechetkikh mnozhestvakh* [Building information security systems on fuzzy sets]. Kiev, MK-Press Publ., 2006. 320 p.

5. Lydin S. Obzor DATAPK – kompleksa operativnogo monitoringa i kontrolya zashchishchennosti ASU TP [Overview of DATAPK – a complex of on-line monitoring and security control of automated process control systems]. *AntiMalware*: website, 2020, 15 May. (In Russian). Available at: https://www.anti-malware.ru/reviews/PAK-DATAPK/ (accessed 04.07.2020).

6. Savinova V.M., Beskhmel'nitskii A.A., Babina E.S., Osadchaya A.D. Identifikatsiya pol'zovatelei korporativnoi sistemy s pomoshch'yu povedencheskogo analiza s ispol'zovaniem modeli iskusstvennoi neironnoi seti [Identification of users of a corporate system using behavioral analysis using an artificial neural network model]. *Transportnoe delo Rossii = Transport business of Russia*, 2017, no. 5, pp. 65–68.

7. Savinov A.N. *Metody, modeli i algoritmy raspoznavaniya klaviaturnogo pocherka v klyuchevykh sistemakh*. Diss. kand. tekhn. nauk [Methods, models and algorithms for recognizing keyboard handwriting in key systems. PhD eng. sci. diss.]. Yoshkar-Ola, 2013. 97 p.

8. Lozano C.M., Lopez F., Lopez J., Pino L., Ramos G. Neural networks for systems security. *Proceedings of 5th European Congress on Intelligent Techniques and Soft Computing*, Aachen, Germany, 1997, vol. 1, pp. 410–414.

9. Obaidat M.S., Macchairolo D.T. A multilayer neural network system for computer access security. *IEEE Transactions on Systems, Man, and Cybernetics*, 1994, vol. 24, no. 5, pp. 806–813.

10. Seals T. Fear of insider threats hits an all-time high. *Infosecurity Magazine*, 2017, 14 November. Available at: https://www.infosecurity-magazine.com/news/fear-of-insider-threats-hits-an/ (accessed 04.07.2020).

Для цитирования:

Исследование аномальных действий пользователя в информационной среде / Н.Е. Карпова, А.С. Баранов, А.А. Емелина, А.Е. Коновалов // Сборник научных трудов НГТУ. – 2020 – № 1–2 (97). – С. 26–39. – DOI: 10.17212/2307-6879-2020-1-2-26-39.

For citation:

Karpova N.E., Baranov A.S., Emelina A.A., Konovalov A.E. Issledovanie anomal'nykh deistvii pol'zovatelya v informatsionnoi srede [Research of abnormal user actions in the information environment]. *Sbornik nauchnykh trudov Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta = Transaction of scientific papers of the Novosibirsk state technical university*, 2020, no. 1–2 (97), pp. 26–39. DOI: 10.17212/2307-6879-2020-1-2-26-39.